

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	9
Synopsis	42
Введение	72
ГЛАВА 1. Обзор литературы	79
1.1 Протоколы квантовой коммуникации	79
1.1.1 Протоколы квантовой коммуникации на дискретных переменных	80
1.1.2 Протокол BB84	81
1.1.3 Протокол B92	84
1.1.4 Протокол квантовой коммуникации с использованием недоверенного приемного узла	92
1.1.5 Протокол квантовой коммуникации с использованием полей близнецов	99
1.1.6 Протокол квантовой коммуникации на боковых частотах модулированного излучения	108
1.2 Когерентное детектирование	108
1.2.1 Гомодинное детектирование	109
1.2.2 Гетеродинное детектирование	110
1.2.3 90-градусный оптический гибрид	112
1.3 Протоколы квантового распределения ключа на непрерывных переменных	113
1.3.1 Протокол квантового распределения ключа с использованием модуляции Гаусса	115
1.3.2 Протокол квантового распределения ключа с использованием модуляции Гаусса и локальным осциллятором, сгенерированным на приемной стороне . .	120

1.4	Фазовый шум в системах квантового распределения ключа	125
1.4.1	Методы борьбы с фазовым шумом в системах квантового распределения ключа	126
1.5	Известные атаки злоумышленника на источники лазерного излучения	128
1.5.1	Атака "засевом" лазерным излучением	129
1.5.2	Атака на мощность локального осциллятора в системах квантового распределения ключа на непрерывных переменных	130
1.5.3	Выводы по главе	131
ГЛАВА 2. Система квантового распределения ключа на боковых частотах с применением обратной связи . . .		133
2.1	Система квантового распределения ключа на боковых частотах .	133
2.2	Метод оптической инжекции	136
2.2.1	Математическая модель оптической инжекции	137
2.3	Определение частотного диапазона фазовой синхронизации двух когерентных источников излучения	138
2.4	Изменение длины волны излучения локального осциллятора под действием внешнего излучения.	139
2.5	Математическая модель гетеродинного детектирования для системы КРК на боковых частотах с применением обратной связи.	141
2.6	Оптическая схема эксперимента для системы квантового распределения ключа на боковых частотах с применением метода оптической инжекции	142
2.7	Описание экспериментальной установки	143
2.8	Полученные экспериментальные результаты	144
2.9	Выводы по главе	147

ГЛАВА 3. Система квантового распределения ключа на боковых частотах с применением двух независимых источников когерентного излучения на непрерывных переменных	149
3.1 Метод гетеродинного детектирования сигналов для системы квантового распределения ключа на боковых частотах	150
3.2 Протокол квантового распределения ключа на боковых частотах с гетеродинном методом детектирования сигналов	151
3.3 Оптическая схема системы квантового распределения ключа на боковых частотах с применением гетеродинного детектирования	151
3.4 Математическая модель системы квантового распределения ключа на боковых частотах с применением гетеродинного детектирования	153
3.5 Алгоритм подстройки поляризационных искажений для системы квантового распределения ключа на боковых частотах с применением гетеродинного детектирования	155
3.6 Описание экспериментальной установки	157
3.7 Описание полученных результатов	158
3.8 Выводы по главе	159
ГЛАВА 4. Атака оптической накачкой на источник когерентного излучения	162
4.1 Атака оптической накачкой на лазер с распределенной обратной связью	162
4.2 Изменение Ватт-Амперной характеристики лазера с распределенной обратной связью при атаке на других длинах волн	164
4.3 Изменение формы импульса при атаке на лазер с распределенной обратной связью, работающем в режиме переключения усиления	167
4.4 Определение минимально необходимой изоляции лазерного источника для предотвращения атаки оптической накачкой	170

4.5	Оценка возможности проведения атаки на существующие системы квантового распределения ключей	171
4.6	Выводы по главе	173
ГЛАВА 5. Исследование источника когерентного излучения на основе оптической инжекции на устойчивость к лазерному засеиванию мощным излучением		175
5.1	Введение	175
5.2	Теоретическое описание метода оптической синхронизации	177
5.2.1	Полупроводниковые источники света с инжекционной синхронизацией	177
5.2.2	Статистика интерференции фазово-рандомизированного классического света	179
5.3	Проведение эксперимента	181
5.3.1	Источник света на испытаниях	181
5.3.2	Экспериментальная установка	184
5.4	Результаты экспериментов	188
5.4.1	Характеристики источника КРК	188
5.4.2	Длина волны источника равна длине волны источника	191
5.4.3	Атака в зависимости от длины волны	196
5.5	Выводы по главе	198
Заключение		200
Список литературы		202
Тексты публикаций		219

Реферат

Общая характеристика диссертации

Актуальность темы

Квантовое распределения ключа (КРК) - актуальная технология, появившаяся 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 сдвиг 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 (КРК-НП). 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 вычитываются, что позволяет уменьшить шум системы, и отсутствие охлаждения до температур порядка -40° градусов Цельсия. Все это позволяет упростить конечную систему. К преимуществам КРК-НП можно отнести большую скорость выработки секретного ключа по сравнению с системами КРК на дискретных переменных, в которых применяются детекторы одиночных фотонов.

Среди сложностей систем КРК-НП выделяется способ передачи сильного лазерного излучения или локального осциллятора (ЛО) на приемную сторону и его разделения с квантовым сигналом. В первых системах КРК-НП 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 интерференционная 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 кан-

лов 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 уязвимость 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 воздействиям 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 2×2 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 информации 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 учиты-

вается 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 когерентного 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 являться система квантового распределения ключа на непрерывных переменных с применением гетеродинного детектирования с независимым ЛО. Суть данной системы заключается в том, что на приемнике и передатчике установлены 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 теоретических 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 поглощается активной средой лазера передатчика так, что поглощенное излучение выступает в роли оптической накачки, которая работает как дополнение к электрической накачке 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 длине 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 преимуществ 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

Разработать систему гетеродинного приема сигналов в квантовой системе коммуникаций на боковых частотах с локальным осциллятором на стороне получателя с применением оптической инжекции и исследовать устойчивость к атакам на техническую реализацию источников лазерного излучения в этой системе.

Задачи

Задача 1

Реализация обратной связи в виде оптической инжекции для системы КРК

на боковых частотах с гетеродинным методом детектирования и применением непрерывных переменных.

Задача 2

Применение гетеродинного приема сигналов в системах КРК, и гетеродинное детектирование мультиплексированного сигнала на одной несущей

Задача 3

Исследовать атаку оптической накачкой на источники излучения, которые могут являться локальным осциллятором для систем квантового распределения ключа на непрерывных переменных

Задача 4

Исследовать влияние мощного оптического излучения на источник излучения на основе оптической инжекции

Основные положения, выносимые на защиту

1. Использование метода оптической инжекции для реализации обратной связи в системе квантовой коммуникации на боковых частотах на непрерывных переменных с дискретной модуляцией и локальным осциллятором, реализованным на стороне получателя, позволяет стабилизировать длину волны источника излучения на передающей стороне, что приводит к возможности передачи по волоконно-оптическому каналу фазово-кодированных сигналов и их гетеродинный прием.
2. Для квантовых коммуникаций на основе когерентного детектирования гетеродинным методом регистрации многомодовых квантовых состояний с фазовым кодированием на основе двух независимых источников лазерного излучения с применением частотного мультиплексирования на одной

несущей частоте и разработан алгоритм контроля поляризации входящего сигнала на основе метода быстрого преобразования Фурье.

3. Засеивание 1.6 мВт оптической мощности в непрерывном режиме излучения на длине волны 1310 нм в резонатор лазера с распределенной обратной связью (Agilecom WSLS-934010C4124-82) с рабочей длиной волны 1550 нм увеличивает среднее число фотонов на длине волны 1550 нм на 21%, увеличивает энергию выходного импульса на 10% и увеличивает дифференциальную квантовую эффективность атакуемого лазера на 2%.
4. Засеивание излучением нарушителя мощностью в 800 мВт в непрерывном на длине волны 1549.7 нм в ведомый лазер (Agilecom WSLS-934010C4124-82) в источнике на основе оптической инжекции повышает стандартное отклонение амплитуды выходных импульсов ведомого лазера на 3%, повышает стандартное отклонение их энергии на 3% и увеличивает среднюю излучаемую мощность на 8%

Научная новизна

Впервые реализована система обратной связи с помощью оптической инжекции для системы квантового распределения ключей на боковых частотах и передан просеянный ключ. Реализован гетеродинный метод детектирования сигналов с двумя независимыми источниками излучения для системы квантового распределения ключей на боковых частотах и разработан алгоритм контроля поляризации для этой системы. Впервые продемонстрирован новый тип атаки на техническую реализацию - атака оптической накачкой на источник излучения в системах квантового распределения ключей, которая позволяет увеличить излучаемое среднее число фотонов в обход существующих методов защиты. Определено экспериментально влияние мощного лазерного излучения на источник когерентного излучения на основе оптической инжекции, увеличивающее энергию излучаемых импульсов и ее разброс, увеличивает выходную

мощность атакуемого источника, что в совокупности приводит к снижению скорости выработки секретного ключа.

Теоретическая и практическая значимость

Теоретическая значимость работы определяется тем, что в рамках ее были переданы фазово-кодированные состояния в системе квантового распределения ключей на боковых частотах на непрерывных переменных с гетеродинным методом детектирования сигналов и были стабилизированы длины волн информационного лазера и лазера локального осциллятора. Также в рамках работы был совершен обмен фазово-кодированными состояниями в системе квантового распределения ключей на боковых частотах на непрерывных переменных с гетеродинным методом детектирования сигналов и двумя независимыми источниками излучения информационного сигнала и локального осциллятора, в рамках передачи таких состояний отработан алгоритм подстройки поляризации информационного излучения. Увеличена выходная средняя мощность и энергия импульсов лазера с распределенной обратной связью, используемого в системах квантового распределения ключей, с помощью оптической накачки на длине волны 1310 нм. Увеличена средняя выходная мощность и среднеквадратическое отклонение амплитуды выходных импульсов, излучаемых источником когерентного излучения на основе оптической инжекции, с помощью мощного лазерного излучения злоумышленника, приводящее к созданию дополнительной уязвимости по доступу к секретному ключу. Практическая значимость работы заключается в том, что проведенные экспериментальные исследования по реализации гетеродинного метода детектирования сигналов показывают работоспособность данного подхода для создания систем квантового распределения ключей с применением такого способа регистрации сигналов. Исследованные же методы воздействия злоумышленника на источники излучения в системах квантового распределения ключей позволяет усовершенствовать

модель нарушителя, повысив устойчивость конечных систем квантового распределения ключей к атакам на техническую реализацию.

Достоверность

Достоверность полученных результатов основана на использовании современных методов научного исследования и сравнении полученных результатов с данными научно-технической литературы. При проведении исследований применялись утвержденные методики и аттестованное оборудование. Обработка экспериментальных данных осуществлялась при помощи пакета прикладного программного обеспечения Origin и Питон. Материалы опубликованы в 9 печатных работах, а также были представлены на 10 международных и российских конференциях.

Внедрение результатов работы

Результаты диссертационной работы внедрены в проекты, выполняемые в рамках Дорожной карты по направлению "Квантовые коммуникации таких как "Разработка и создание системы квантовой коммуникации на непрерывных переменных в котором внедрены результаты, полученные по реализации гетеродинного метода детектирования для системы квантового распределения ключей на боковых частотах и "Создание Пилотного участка Магистральной Квантовой сети в рамках которого внедрены исследования устойчивости источника лазерного излучения к атаке оптической накачкой

Апробация результатов работы

1. КМУ X 'Применение гетеродинного метода анализа сигналов для реализации протокола квантовой коммуникации с топологией 'звезды'
2. ФЭКС-2021 'Применение гетеродинного метода анализа сигналов для реализации протокола квантовой коммуникации с топологией 'звезды'
3. ППС LI 'Когерентный прием в системах квантовой коммуникации на боковых частотах с недоверенным приёмным узлом'
4. XI КМУ 'Многопользовательские квантовые сети городского масштаба на основе пассивных оптических сетей'
5. 20th International Conference Laser Optics ICLO 2022 'Continuous variable measurement-device-independent quantum communication scheme based on subcarrier waves'
6. XII КМУ 'Система квантовой коммуникации на непрерывных переменных с недоверенным приемным узлом'
7. LII научная и учебно-методическая конференция ППС 'Частотное мультиплексирование для системы квантового распределения ключа на боковых частотах'
8. Всероссийская научная конференция с международным участием 'Невская фотоника-2023' (09.10.2023 - 13.10.2023), 'Гетеродинное детектирование для системы квантового распределения ключа на боковых частотах с двумя независимыми источниками излучения'
9. 22th International Conference Laser Optics ICLO 2024 'Laser-pumping attack on QKD sources', 1-5 июля 2024 г.
10. 22th International Conference Laser Optics ICLO 2024, 'Secure laser source for QKD systems', 1-5 июля 2024 г.
11. QCrypt 2024, 2-6.09.24, 'Optical pumping attack to laser source in Quantum key distribution system'

Личный вклад автора

Аспирантом лично разработаны оптические схемы систем квантового распределения ключей на боковых частотах с гетеродинным методом детектирования сигналов и с применением метода оптической инжекции, а также исследовано влияние оптической накачки на лазер с распределенной обратной связью и изучено влияние мощного оптического излучения на источники излучения на основе оптической инжекции. Аспирантом были проведены экспериментальные работы по изучению работы разработанных систем и самостоятельно обработаны экспериментальные результаты.

Структура и объем диссертации

Публикации

Основные результаты по теме диссертации изложены в 9 публикациях. Из них 9 изданы в журналах, рекомендованных ВАК, 9 опубликованы 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. Goncharov R.K., Fadeev M.A., Zinovev A.V., Nasedkin B.A., Kiselev A., Egorov V.I. Coherent detection schemes for subcarrier wave continuous variable quantum key distribution // Journal of the Optical Society of America B: Optical Physics – 2021, Vol. 38, No. 6
2. Pervushin B.E., Fadeev M.A., Zinovev A.V., Goncharov R.K., Santev A.A., Ivanova A.E., Samsonov E.O. Quantum random number generator using

vacuum fluctuations // Наносистемы: Физика, химия, математика = Nanosystems: Physics, Chemistry, Mathematics - 2021, Vol. 12, No. 2, pp. 156–160

3. Fadeev M.A., Goncharov R., Smirnov S., Chistiakov V. Continuous variable measurement-device-independent quantum communication scheme based on subcarrier waves // Proceedings - International Conference Laser Optics 2022, ICLO 2022
4. Boltanskii M.V., Maksimova E.I., Fadeev M.A., Shakhovoy R.A. Influence of optical feedback on an optical pulse shape of a semiconductor laser // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Физико-математические науки = St.Petersburg State Polytechnical University Journal. Physics and Mathematics, 2024, Vol. 17, No. 3.1, pp. 224–228
5. Latypov I.Z., Chistyakov V.V., Fadeev M.A., Sulimov D.V., Khalturinsky A.K., Kynev S.M., Egorov V.I. Hybrid quantum communication protocol for fiber and atmosphere channel // Наносистемы: Физика, химия, математика = Nanosystems: Physics, Chemistry, Mathematics, 2024, Vol. 15, No. 5, pp. 654 – 657
6. Fadeev M.A., Ponosova A.A., Huang A., Shakhovoy R., Makarov V. Secure laser source for QKD systems // Proceedings - International Conference Laser Optics 2024, ICLO 2024, 2024, pp. 571
7. Fadeev M.A., Ponosova A.A., Shakhovoy R., Makarov V. Laser-pumping attack on QKD sources // Proceedings - International Conference Laser Optics 2024, ICLO 2024, 2024, pp. 562
8. Фадеев М.А., Морозова П.А., Смирнов С.В., Иванова А.Е., Кынев С.М., Чистяков В.В., Гетеродинное детектирование для системы квантового распределения ключа на боковых частотах // Известия высших учебных заведений. Радиофизика, 2024. том 67 издание 9, с.784–792
9. M. A. Fadeev, A.Ponosova, Q.Peng, H.Anqi, R. Shakhovoy, and V.Makarov, ‘Optical-pumping attack on a quantum key distribution laser source’, Opt. Express, 2025.

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 [1–4], так и непрерывных переменных [5–9]. Проводится описание и анализ особенностей методов когерентного детектирования [10], используемых в системах квантового распределения ключа. Освещается вопрос наличия фазовых шумов в системах квантового распределения ключа. Демонстрируются примеры методов компенсации фазовых шумов, таких как применение пилотных импульсов [11] и создание обратной связи [12]. Показаны известные атаки злоумышленника на оборудование в составе систем КРК [13–15]. Описывается атака "засевом" лазерным излучением на лазер передатчика, ее влияние и возможные методы защиты [16–18]. Другим рассматриваемым аспектом является 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 [19–22].

Во второй главе исследуется метод оптической инжекции [23; 24] для реализации обратной связи в системе квантового распределения ключа на боковых частотах [25–27]. Метод оптической инжекции заключается в том, что существует пара лазеров: ведущий и ведомый. Излучение ведущего лазера вводится в резонатор ведомого. Инжекция дополнительных фотонов в резонатор лазера-ведомого уменьшает время релаксационных колебаний излучения, что ускоряет процесс генерации излучения и уменьшает негативные эффекты. Такой подход позволяет улучшить характеристики излучения ведомого лазера в частности:

- сужение спектральной линии выходного излучения

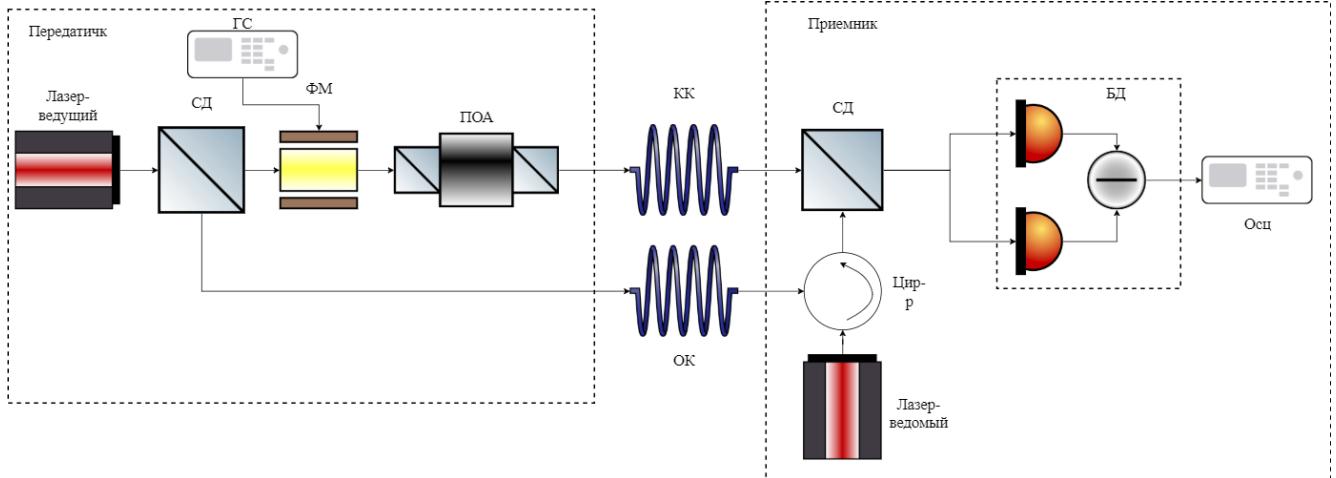


Рисунок 1 — Схема эксперимента системы КРК с применением оптической инжекции. СД - светоделитель, ФМ - фазовый модулятор, ГС - генератор сигналов, ПОА - перестраиваемый оптический аттенюатор, КК - квантовый канал, ОК - открытый канал, Цир-р - циркулятор, БД - балансный детектор, Осц - осциллограф.

- уменьшение нелинейностей и подавление релаксационных колебаний
- уменьшение чирпа выходных импульсов и увеличение стабильности их амплитуды

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 связи будет стабилизация промежуточной частоты и уменьшение фазовых шумов. Для реализации данного метода используется отдельный канал и циркулятор для разделения 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 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, $\omega - \Omega$ - 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, $\omega - \Omega$ - 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 - $\omega - f$ - центральная частота лазера Алисы минус частота ЛО, $(\omega - \Omega) - f$ - нижняя боковая частота минус частота ЛО и $(\omega + \Omega) - f$ - 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 передатчика. 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 $(\omega + \Omega) - f$, 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 фазы сигнала.

Полученная последовательность бит является сырым ключом. Полученный ключ просеивается. В полученном просеянном ключе оценивается квантовый коэффициент ошибок по битам (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 отсутствует 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.

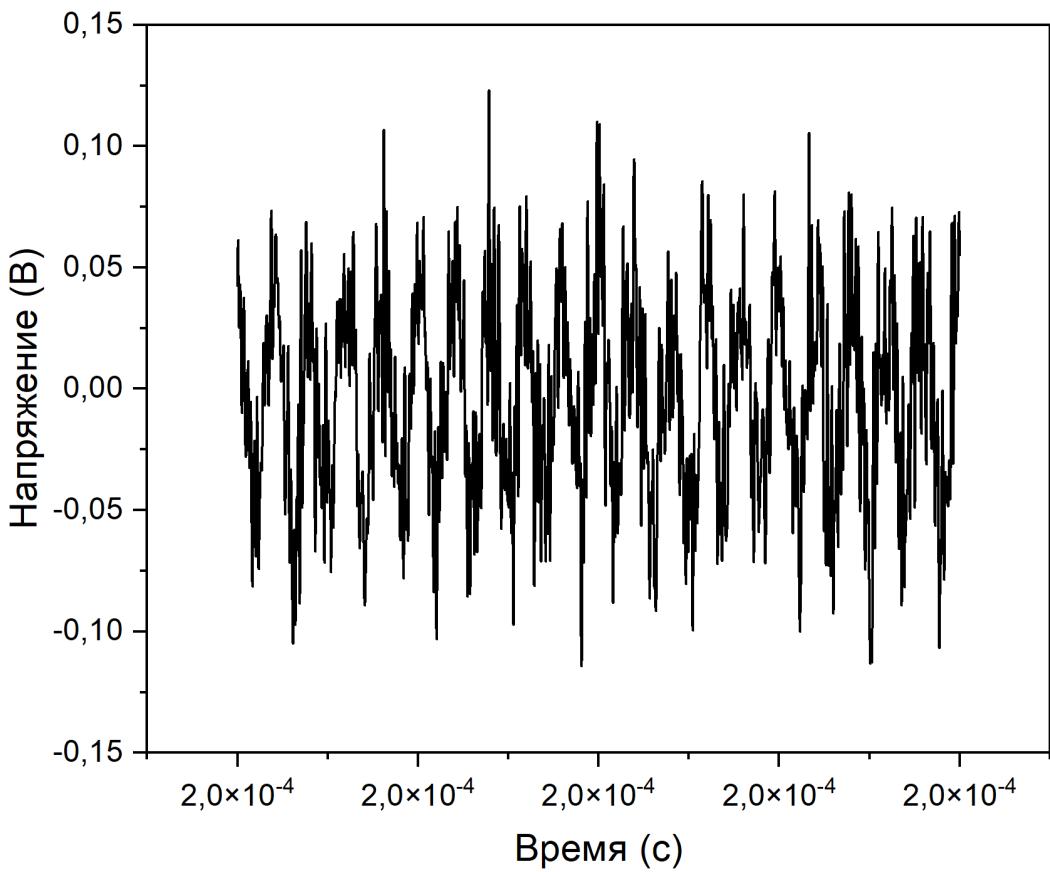


Рисунок 2 — Зашумленный сигнал на выходе балансного детектора

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. 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 мультиплексирования 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.

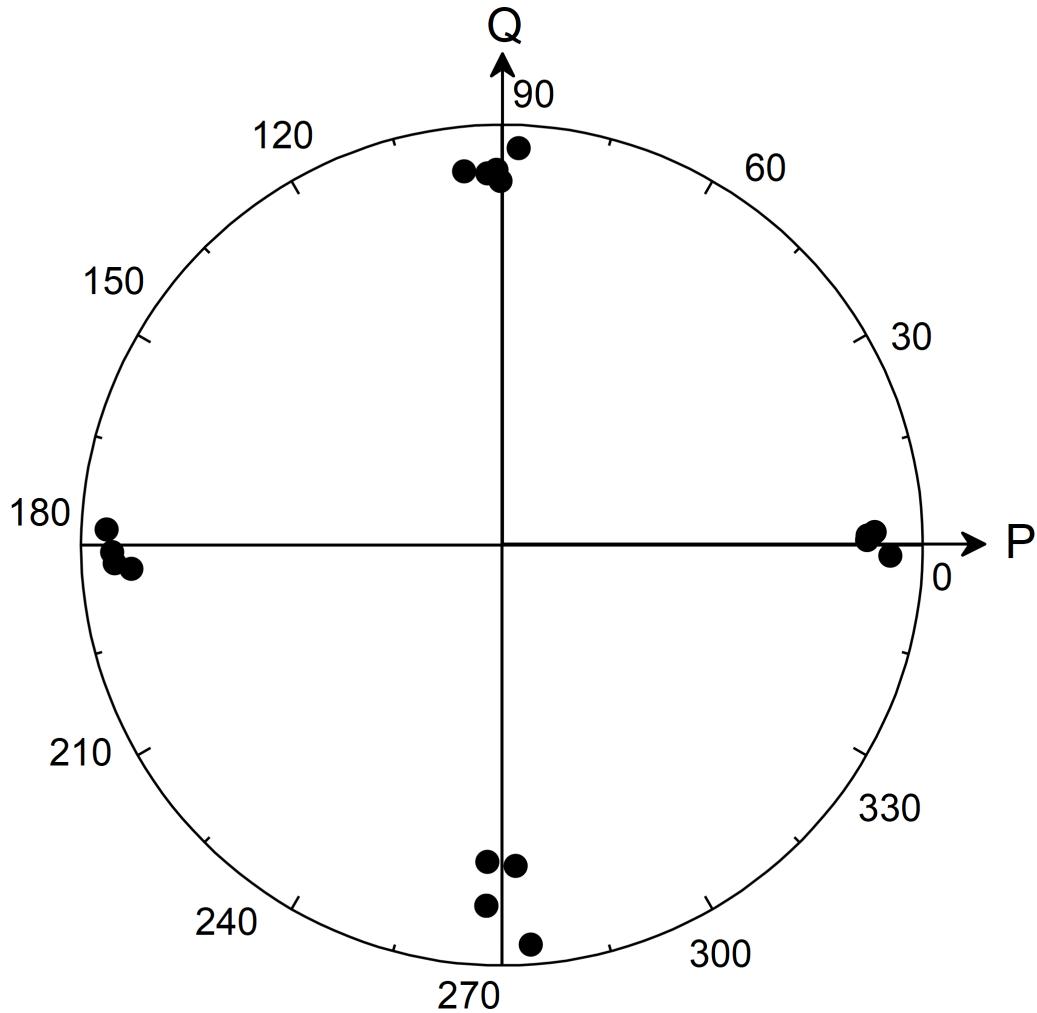


Рисунок 3 — Полученные значения фазы после цифровой обработки

В третьей главе рассматривается схема применения гетеродинного метода детектирования [28–30] сигналов с двумя независимыми источниками сигналов [8; 20] 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 [27; 31].

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 формирует когерентное излучение. Это излучение, пройдя необходимые пассив-

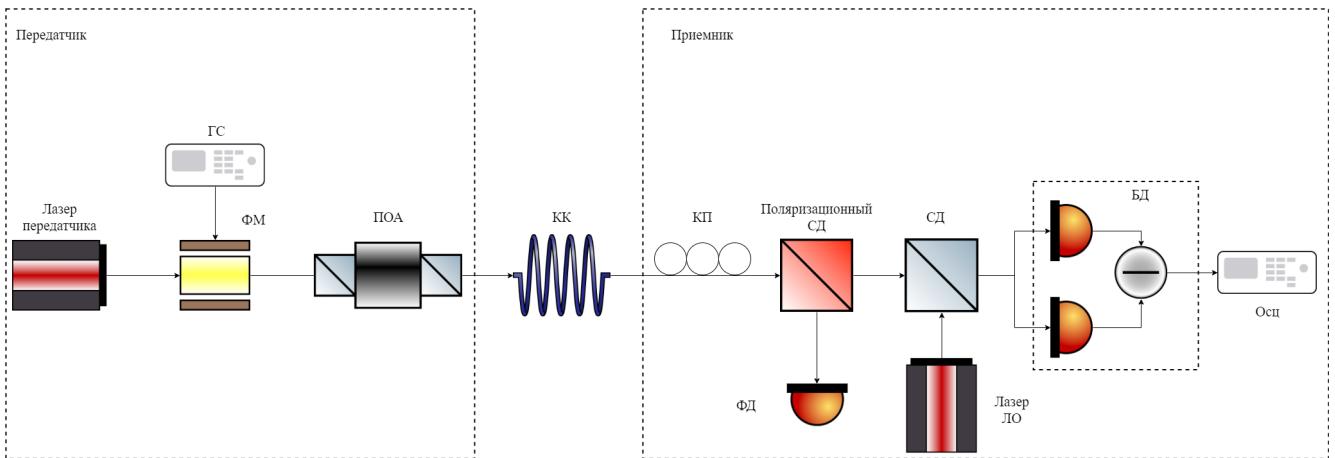


Рисунок 4 — Схема системы квантового распределения ключа на боковых частотах с независимым локальным осциллятором. СД - светоделитель, ФМ - фазовый модулятор, ГС - генератор сигналов, ПОА - перестраиваемый оптический аттенюатор, КК - квантовый канал, БД - балансный детектор, Осц - осциллограф.

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 сдвиг, который соответствует битам информации. Для примера в данной работе используется квадратурно-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 передатчика. 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 обогащается дополнительными гармониками. Эти гармоники появляются из-за того, что частоты ЛО и лазера Алисы не совпадают. Эти спектральные компоненты 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 увеличения 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 применяться 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

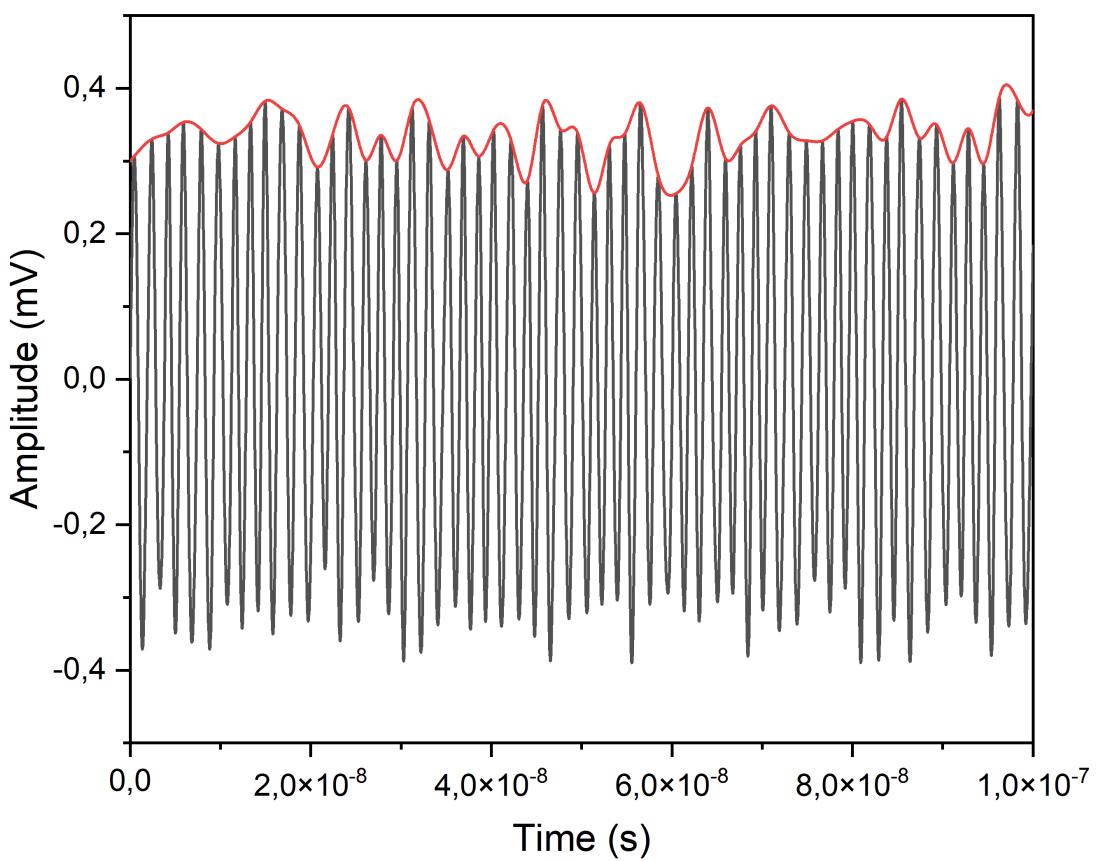


Рисунок 5 — Сигнал на выходе балансного детектора после гетеродинного приема.

его и поляризации квантовых состояний для эффективной интерференции на приемнике. В рамках данной работы предлагается алгоритм контроля поляризации на основе Быстрого Преобразования Фурье. Суть данного алгоритма заключается в том, что при использовании поляризационного светофильтра 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

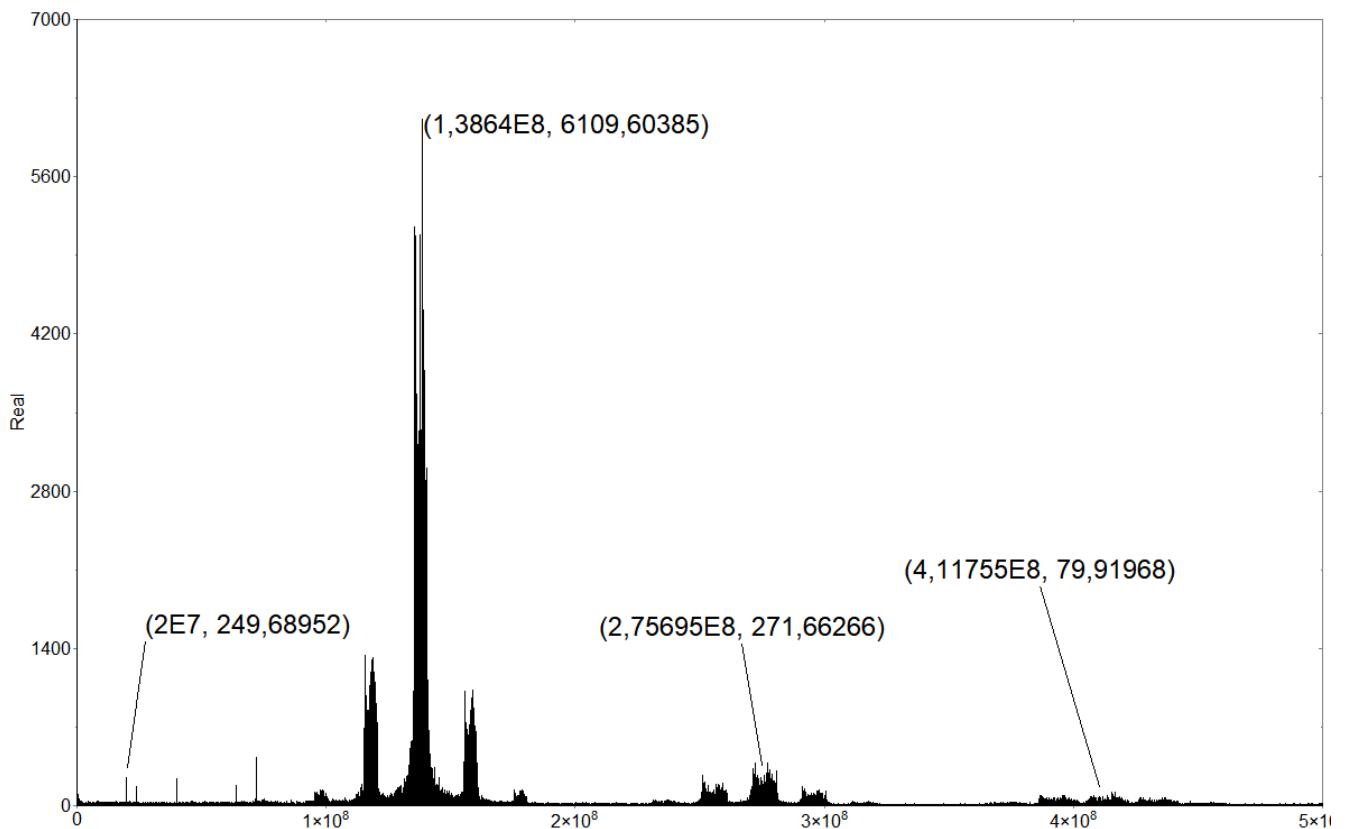


Рисунок 6 — Спектр сигнала с искаженной поляризацией

4. Дальнейший поворот поляризации сигнала до максимума гармоники на частоте модуляции

В результате его работы возможна как подстройка поляризации за счет применения активного контроля поляризации, который будет использовать результат БПФ как обратную связь для подстройки поляризации. На рисунке 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 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

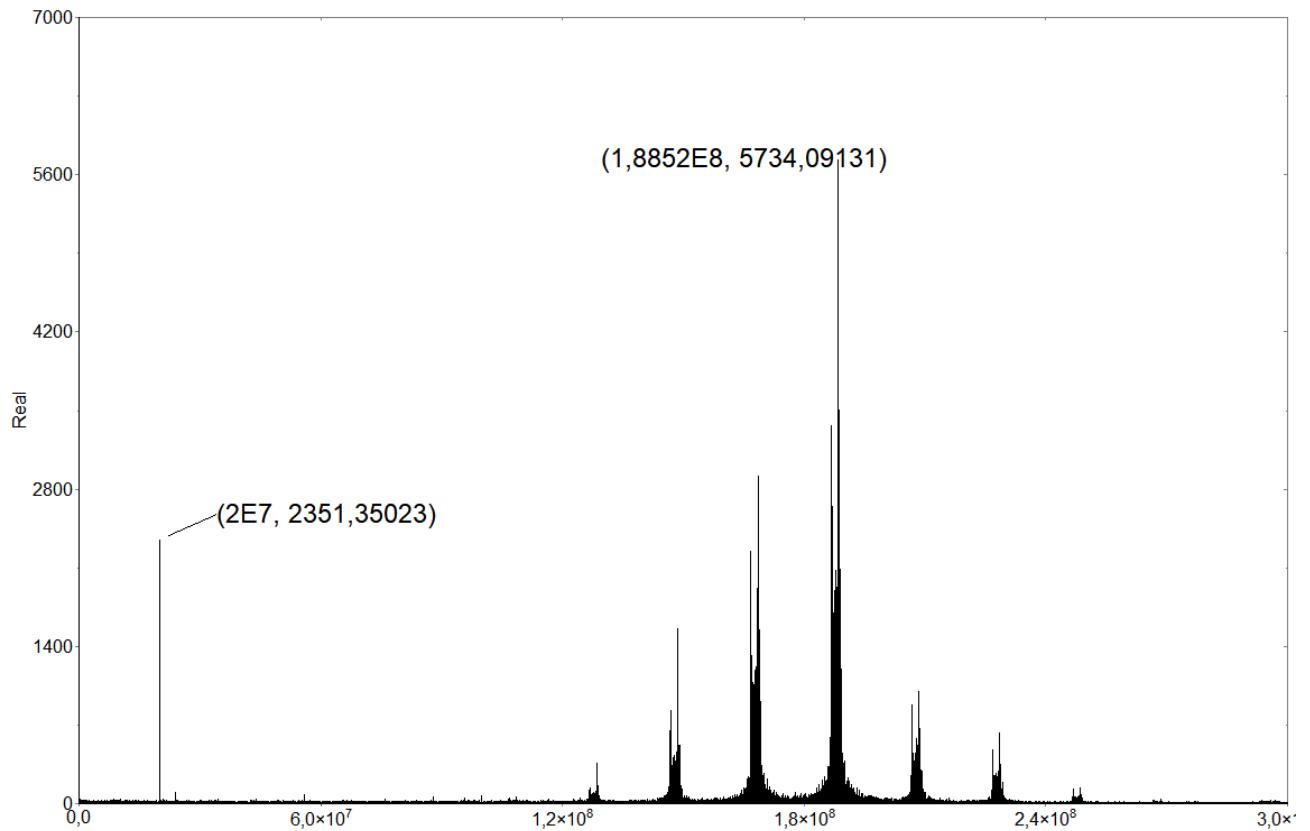


Рисунок 7 — Спектр сигнала с искаженной поляризацией

двух независимых источников когерентного излучения позволяет не использовать системы обратной связи, которые требуют дополнительного оптического канала и открывают дополнительные возможности для злоумышленника. Генерация локального осциллятора на стороне приемника позволяет 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 случай-

ный фазовый шум из-за случайности процесса генерации лазерного излучения в двух независимых источниках. Данная проблема решается анализом фазы промежуточной 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 посвящена 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 [32; 33]. Данный тип атаки схож с атакой оптическим "засевом" (Laser Seeding) [16; 17] тем, что Ева инжектирует свое излучение в резонатор лазера на передатчике 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 [34–36]. 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 требуется 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 подключается 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 передатчика, 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 [37]. Это приводит к тому, что создается дополнительная инверсия населенности, приводящая к смещению Ватт-Амперной характеристики лазера при неизменном токе накачки. В результате этого калибркованный источник излучения на стороне передатчи-

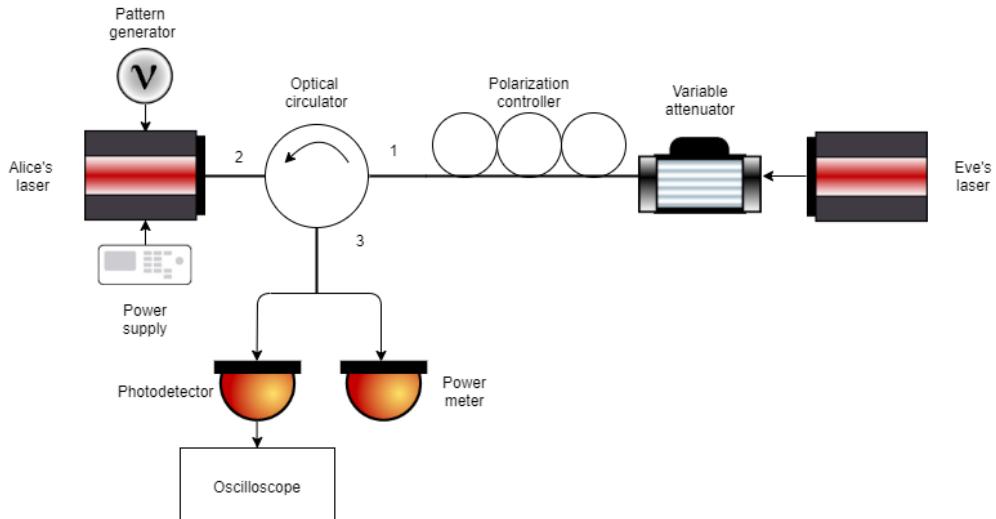


Рисунок 8 — Схема эксперимента по засеванию лазера. Alice's Laser - Лазер Алисы, Pattern generator - генератор последовательности импульсов, Power Supply - лабораторный блок питания, optical circulator - оптический циркулятор, polarization controller - контроллер поляризации, varriable attenuator - перестраиваемый аттенюатор, Eve's laser - лазер злоумышленника, Photodetector - фотоприемник, power meter - измеритель мощности, Oscilloscope - осциллограф.

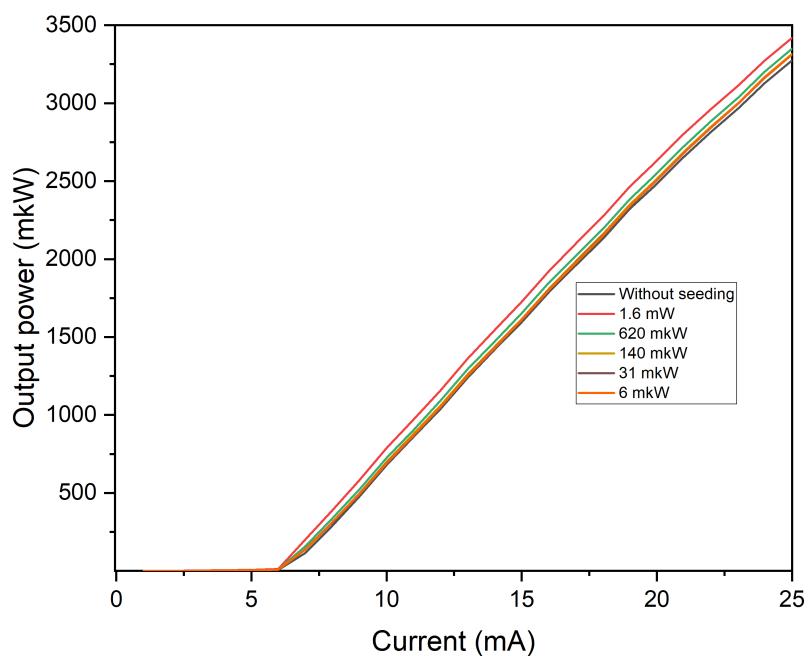


Рисунок 9 — Изменение Ватт-Амперных характеристик под различными мощностями накачки на длине волны 1310 нм. Output power - выходная мощность в микроваттах, current - ток в миллиамперах

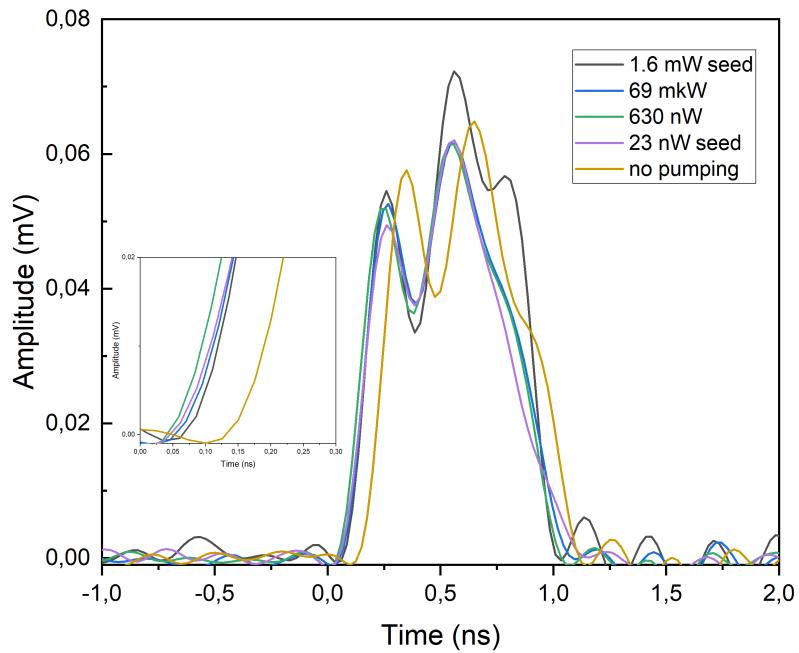


Рисунок 10 — Изменение формы импульса под действием внешней оптической накачки на разных мощностях на длине волны 1310 нм. Amplitude - амплитуда в милливольтах, Time - время в наносекундах, seed - засевание, pumping - накачка.

ка начинает излучать 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 расщеплением числа фотонов. Этот же эффект проявляется в изменении формы импульса. Оптическая накачка [38–40] увеличивает площадь импульса и, соответственно, его энергию, повышая как и среднее число фотонов в сигнальных импульсах, так и среднее число фотонов в состояния-ловушках в протоколе BB84 с состояниями-ловушками [24].

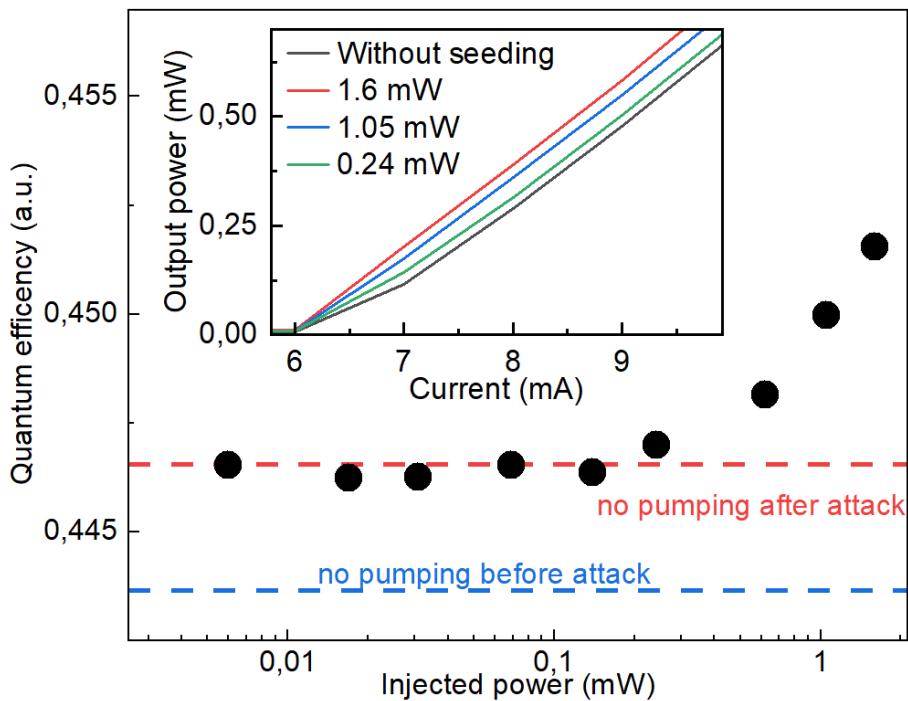


Рисунок 11 — Изменение квантовой эффективности под действием внешнего излучения на длине волны 1310 нм. Quantum efficiency - квантовая эффективность в относительных единицах, Output power - выходная мощность в милливаттах, Injected power - введенная мощность в милливаттах, current - ток в миллиамперах, 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 эффективности на 1%, продемонстрировано на графике 11 и увеличения выходной мощности на 4%. Была рассчитана минимально необходимая мощность для эффективной атаки злоумышленника на типичную оптическую схему передатчика, реализующую протокол BB84.

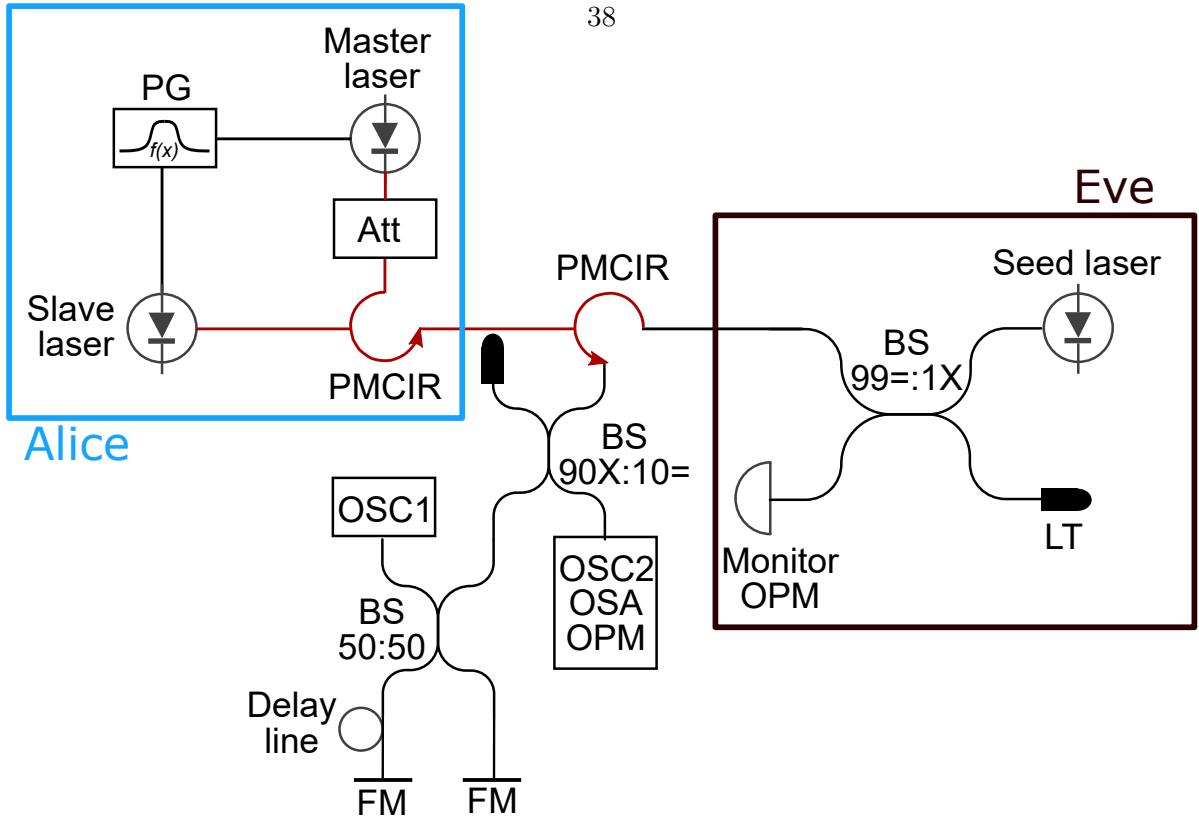


Рисунок 12 – Оптическая схема установки лазерного засеивания источника на основе оптической инжекции.

Исследования, проводимые в [шестой главе](#), посвящены 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 [41–43]. 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 теоретическому максимуму в 0.5.

Однако, для таких источников не были исследованы методы воздействия такие как атака "засевом" лазера [44]. 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 WSL934010C4124-42 со встроенным изолятором, который использовался в качестве ведущего лазера для генерации опорного излучения. Второй же лазер представлял собой лазер Agilecom WSL934010C4124-82, аналогичный первому, но уже без встроенного изолятора. Это нужно для того, чтобы максимизировать количество излучения, 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 эрбийевый 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 также 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 измерений приведены на рисунке 13. Данные результаты показывают, что Ева способна увеличивать нестабильность выходной мощности для увеличения среднего числа фотонов в импульсе. Длительность импульса так же изменяется под действием внешнего излучения, изображенном на рисунке 14. Под внешним воздействием дрожание импульса возрастает на 2%.

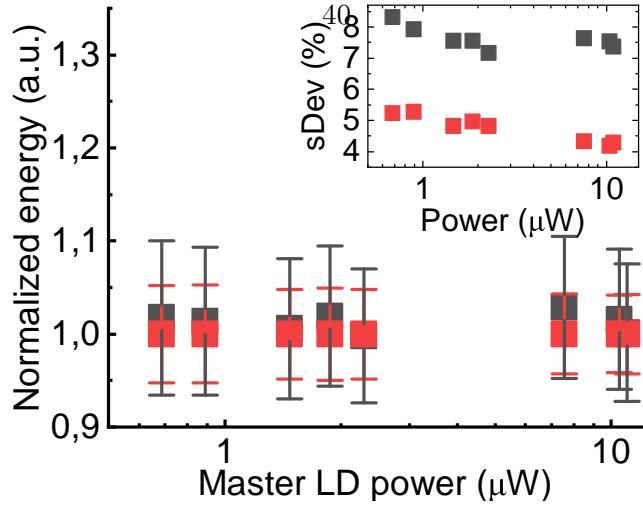


Рисунок 13 — Изменение энергии импульса источника под действием внешнего излучения и без него в зависимости от мощности лазера-мастера.

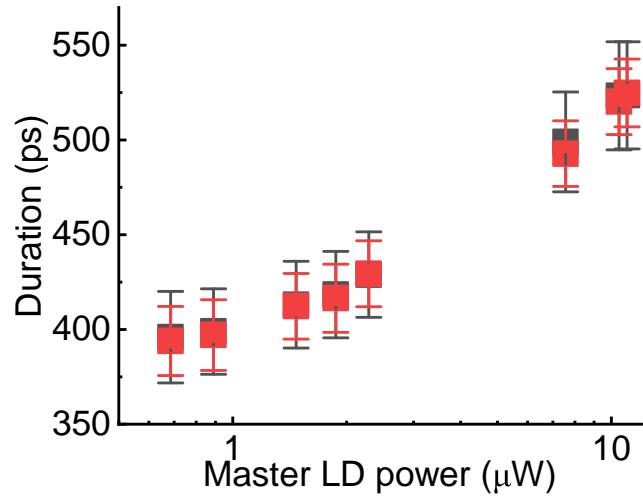


Рисунок 14 — Изменение длительности импульса под действием внешнего излучения

Существующие работы показывают [45], что даже незначительные отклонения в длительности импульса существенно снижают дальность распределения секретного ключа.

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

аттенюации используется формула

$$\alpha = P_a - P_{req} - \beta \quad (2)$$

, 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.

Synopsis

General thesis summary

Relevance

Quantum key distribution (QKD) is a relevant technology emerging from quantum information science theory that allows a symmetric bit sequence to be distributed using quantum techniques to two or more users to use this sequence as a key for symmetric data encryption while simultaneously detecting unauthorized access by illegitimate users. The use of quantum states of light in the key distribution allows to achieve a level of secrecy unavailable to classical encryption protocols. Such quantum states can be represented as single photons. Their quantum properties do not allow an attacker to copy their states or read them without modification and without introducing errors. Such quantum states can be transmitted both through fiber-optic communication lines (FOCL), atmospheric channels and in outer space by means of satellites. The principle of operation of these systems is as follows. On the transmitter side (Alice) quantum states are formed. For this purpose coherent laser radiation is used, attenuated to single photons with the help of attenuator. A change in the polarization or phase shift of the photon is introduced into the prepared quants of light. The state thus prepared is transmitted through a communication channel to the receiver (Bob). At the receiver side, the photon state is re-measured independently of Alice. In the case of Bob's correlation, the received single photon is detected by a single photon detector. Due to the properties of the single photon in the form of impossibility of cloning, impossibility of measurement without destruction and its indivisibility it is possible to trace the impact of the intruder, as his actions will lead to the appearance of errors in the received bit sequence. This is how the control of unauthorized access is ensured.

A separate class are systems of quantum key distribution on continuous variables (CV-QKD). In such systems quantum state, prepared and transmitted by Alice, on the receiving side interacts with strong laser radiation. And the result of this interaction is registered by a balance detector. The main differences of this detector from the detector of single photons is the use of two classical photodetectors, connected in such a way that their photocurrents are mutually subtracted, which reduces the noise of the system, and the lack of cooling to temperatures of about -40° degrees Celsius. All of this allows for simplification of the final system. To the advantages of the FACS can be attributed a greater speed of secret key generation compared to the FAC systems on discrete variables, which use single photon detectors.

Among the complexities of the CV-QKD systems is the method of transmission of strong laser radiation or local oscillator (LO) to the receiving side and its separation from the quantum signal. In the first Gaussian modulated CV-QKD systems, the Local Oscillator and quantum states were generated at the transmitter, combined and transmitted together in a quantum channel. At the receiving end, the local oscillator and the quantum signal are separated, the LO is delayed by a special delay line and reconnected at the beam splitter for interaction. The result of this interaction is an interference pattern whose intensity distribution depends on the state encoded by Alice. The resulting field is registered by a balance detector, at the output of which a voltage level is formed, which is further subjected to post-processing. Transmission of the local oscillator through the channel limits the range of operation of this type of system and limits the speed of key generation, because for the best operation of the system requires LO as much power as possible. The second problem is the ability of an attacker to manipulate the local oscillator to create information leakage channels. As an alternative, it is proposed to use a local oscillator generated at the receiving side. Such a solution will increase the range of key transmission, the speed of its generation and close the vulnerability to an attack on LO. One of the promising approaches to the realization of quantum communication systems on continuous variables is the system of quantum communication on side frequencies of modulated radiation. The basis of this method is the transfer of the

quantum channel to side frequencies, which appear as a result of modulation of optical radiation by an alternating electric field. This increases the stability of the transmitted signal to external influences and provides a high spectral efficiency, as well as provides indicators for the ratio of the rate of key generation to the distance between the receiver and transmitter units, comparable to other systems of quantum communication. This method is also suitable for realizing continuous variable protocols with coherent detection methods. In particular, this paper considers a heterodyne method in which the quantum states prepared by Alice are transmitted over a fiber link to the receiver, in it they fall on a 2x2 beam splitter with a 50:50 splitting ratio and are mixed on it with a powerful local oscillator, which is detuned in frequency from the transmitting laser by an amount that exceeds the frequency of the state change. The result of the interference is detected by a balance detector. The output of the balance detector produces a signal at an intermediate frequency from the entire spectrum of the signal transmitted by Alice. Extraction of information requires filtering using low pass filter and demodulation of the received signal to generate a raw key.

One of the challenges in implementing heterodyne detection method for key distribution is the need to compensate for phase noise. Various methods are used for this purpose. The first of these methods is the transmission of a 'pilot tone', during detection of which the phase noise contributed by the channel is measured. The measured value is then taken into account in the post-processing of the states. The second is the implementation of feedback in various forms. Within the scope of this paper, an optical feedback method is proposed for a quantum key distribution system at side frequencies on continuous variables. The essence of this method is the injection of laser radiation from the master laser, which is the transmitter laser, into the slave laser, which is used as a local oscillator in the receiver. This method allows stabilizing the LO wavelength and reducing phase noise due to the fact that both sources are coherent radiation generators with random phase. The optical injection method requires an additional channel to transmit the feedback generation. Such a channel increases system complexity and fiber optic link (FOCL) requirements, which is particularly critical in urban links where the allocation of an additional fiber

or channel in multiplexed networks is difficult. The solution to this problem may be a system of quantum key distribution on continuous variables using heterodyne detection with independent LO. The essence of this system is that the receiver and transmitter are equipped with wavelength stabilized lasers with a spectral line width of less than 10 kHz. This approach allows to avoid constant adjustment of the laser wavelengths and to reduce the phase noise associated with the independence of the radiation sources. However, the phase noise does not disappear, so it still needs to be compensated. In the case of implementing such a signal detection method for a quantum key distribution protocol at side frequencies, the carrier frequency can be used for this purpose by measuring its phase and making adjustments in post-processing.

The differences between real QKD systems and the models used for theoretical proofs can be exploited by an attacker to carry out different types of attacks on the equipment comprising the system. It has been shown in earlier works that laser radiation sources based on semiconductor crystals can be vulnerable to 'seeding' by an attacker's external radiation at a wavelength close to that used by the transmitter. This attack results in a change in the shape of the emitted pulse and an increase in output power, and in some cases a change in wavelength can also be observed. These effects result in an increase in the average number of photons emitted by the transmitter, which opens up the possibility of a photon number splitting attack for the attacker. However, 'seeding' attacks by laser radiation at other wavelengths have not been considered in the literature. This type of attack is more dangerous because passive fiber optic elements that introduce additional attenuation, such as isolators or DWDM filters, are used to protect against it. However, there are works that demonstrate that the amount of attenuation in such elements can be reduced when the incident wavelength of the radiation is significantly changed. For example, an insulator with an operating wavelength of 1550 nm introduces 50 dB of back-pass loss, when this value is 20 dB when exposed to radiation at a wavelength of 1310 nm. And in the case of the DWDM filter, it contributes virtually no attenuation at 1310 nm. Thus, it is much easier for an attacker to perform a 'seeding' attack with laser radiation, since the attenuation introduced at this wavelength is less.

This type of attack is called an 'optical pumping attack'. Its essence is that the attacker probes the laser with a wavelength different from the operating wavelength. This radiation is absorbed by the active medium of the transmitter laser so that the absorbed radiation acts as an optical pump, which works as a complement to the electrical pump of the semiconductor laser. In this case, the Watt-Ampere characteristic of the laser and its quantum efficiency changes. This leads to the fact that the energy of the emitted pulses increases while the pump current remains unchanged. In the framework of this work, this type of attack is first labelled, the lower limit of the necessary radiation power at the wavelength of 1310 nm to change the characteristics of the laser under study is determined, and the effect of optical pumping on the laser characteristics is measured.

In quantum distribution systems, laser radiation sources based on optical injection are used. Such sources are constructed in the following way: two lasers are used – a master and a slave laser connected by a circulator. Radiation of the slave laser allows reducing the jitter of emitted pulses, stabilizing the output power and narrowing the spectral line. However, such sources have not been investigated for robustness to external radiation. Previously shown work on laser 'seeding' has been carried out only for single radiation sources. A source based on optical injection has several advantages relative to a single source: the presence of isolation from the quantum channel due to the optical circulator and the presence of external radiation from the leading laser. This work studies the effect of high-power laser radiation on the duration, jitter, and amplitude of the emitted pulses, and demonstrates a lower bound on the radiation power required to modify the operation of this system.

The goal

To develop a system of heterodyne detection of signals in a quantum communication system at side frequencies with a local oscillator on the receiver side using optical injection and to investigate the resistance to attacks on the technical

implementation of laser radiation sources in this system. In order to achieve the goal in the framework of the thesis, the following objectives have been established:

Objectives

Objective 1: development of QKD system with feedback

Implementation of optical injection feedback for sideband QKD system with heterodyne detection method and continuous variables

Objective 2: research of heterodyne detectinon for SCW-QKD with two independent sources

Application of heterodyne signal detection in QKD systems with two independent sources of laser radiaton and development of polartzation maitaining algorithm.

Objective 3: experimental design

Study the optical pumping attack on radiation sources that can be local oscillators for continuous variable quantum key distribution systems.

Objective 4: research of influence of high power radiation to optical injection locked source.

To investigate the effect of high-power optical radiation on a radiation source based on optical injection.

Research methods

In the framework of this thesis, the following research methods were used (an analysis of practical cases, an overview of the latest practices, etc.)

Assertions that are presented for defense

1. The use of optical injection method for the implementation of feedback in the system of quantum communication at side frequencies on continuous variables with discrete modulation and local oscillator implemented on the receiver side allows stabilising the wavelength of the radiation source on the transmitting side, which leads to the possibility of transmission of phase-encoded signals and their heterodyne reception through the fiber-optic channel.
2. For quantum communications on the basis of coherent detection by heterodyne method of registration of multimode quantum states with phase coding on the basis of two independent sources of laser radiation with the use of frequency multiplexing on one carrier frequency and developed an algorithm to control the polarization of the incoming signal on the basis of fast Fourier transform method.
3. Seeding 1.6 mW of continuous mode optical power at 1310 nm into the resonator of a distributed feedback laser (Agilecom WSLS-934010C4124-82) with an operating wavelength of 1550 nm increases the average number of photons at 1550 nm by 21%, increases the output pulse energy by 10%, and increases the differential quantum efficiency of the attacked laser by 2%.
4. Seeding 800 mW of intruder radiation continuously at 1549.7 nm into a slave laser (Agilecom WSLS-934010C4124-82) in an optical injection based source increases the standard deviation of the amplitude of the output pulses of the slave laser by 3%, increases the standard deviation of their energy by 3%, and increases the average radiated power by 8%.

The novelty of research

An optical injection feedback system for a quantum key distribution system at side frequencies is implemented for the first time and the sifted key is transmitted.

A heterodyne signal detection method with two independent radiation sources is implemented for a quantum key distribution system at side frequencies and a polarization control algorithm is developed for this system. For the first time a new type of attack on the technical implementation - optical pumping attack on the radiation source in quantum key distribution systems, which allows to increase the emitted average number of photons bypassing the existing protection methods, is demonstrated. The influence of high-power laser radiation on the source of coherent radiation based on optical injection has been determined experimentally, which increases the energy of emitted pulses and its spread, increases the output power of the attacked source, which together leads to a decrease in the rate of secret key generation.

Theoretical and practical significance

The theoretical significance of the work is determined by the fact that within the framework of it phase-encoded states in the system of quantum key distribution at side frequencies on continuous variables with heterodyne method of signal detection were transferred and the wavelengths of information laser and local oscillator laser were stabilized. Also within the framework of the work the exchange of phase-encoded states in the system of quantum distribution of keys at side frequencies on continuous variables with heterodyne method of signal detection and two independent sources of radiation of information signal and local oscillator was made, within the framework of transfer of such states the algorithm of adjustment of polarization of information radiation was worked out. The average output power and pulse energy of a distributed feedback laser used in quantum key distribution systems are increased by optical pumping at a wavelength of 1310 nm. The average output power and standard deviation of the amplitude of the output pulses emitted by a coherent radiation source based on optical injection with the help of high-power laser radiation of an intruder, leading to the creation of additional vulnerability on access to the secret key, is increased. Practical significance of the work lies in the

fact that the conducted experimental studies on the implementation of heterodyne method of signal detection show the operability of this approach to create systems of quantum key distribution using this method of signal registration. Researched methods of the attacker's influence on the sources of radiation in the systems of quantum key distribution allows to improve the model of the intruder, increasing the resistance of the final systems of quantum key distribution to attacks on the technical implementation

Validity

The reliability of the obtained results is based on the use of modern methods of scientific research and comparison of the obtained results with the data of scientific and technical literature. The approved methods and certified equipment were used in the research. Experimental data processing was carried out with the help of Origin and Python application software package. The materials were published in 9 printed papers and presented at 10 international and Russian conferences.

Implementation of research results

(specify the degree of implementation; technologies, new universal measurement methods, educational technologies, etc.)

Approbation of research results

Key research results were presented and discussed at the following conferences:

1. CYS X 'Application of the heterodyne signal analysis method for implementing a quantum communication protocol with a star topology'
2. IWQO-2021 'Application of the heterodyne signal analysis method for implementing a quantum communication protocol with a star topology'
3. PPS LI 'Coherent reception in quantum communication systems at side frequencies with an untrusted receiving node'
4. XI CYS 'Multi-user city-scale quantum networks based on passive optical networks'
5. 20th International Conference Laser Optics ICLO 2022 'Continuous variable measurement-device-independent quantum communication scheme based on subcarrier waves'
6. XII CYS 'Quantum communication system on continuous variables with an untrusted receiving node'
7. LII scientific and educational-methodological conference of the teaching staff 'Frequency multiplexing for a quantum key distribution system on side frequencies'
8. All-Russian scientific conference with international participation 'Nevskaya Photonics-2023' (09.10.2023 - 13.10.2023), 'Heterodyne detection for a quantum key distribution system at side frequencies with two independent radiation sources'
9. 22nd International Conference Laser Optics ICLO 2024 'Laser-pumping attack on QKD sources', 1-5 July 2024
10. 22nd International Conference Laser Optics ICLO 2024, 'Secure laser source for QKD systems', 1-5 July 2024
11. QCrypt 2024, 2-6 September 2024, 'Optical pumping attack to laser source in Quantum key distribution system'

Translated with DeepL.com (free version)

Personal contribution of the author

(the author's participation in all the stages of research, such as data collection or execution of experiments, approbation of the obtained results, design of experimental panels and plants (key elements of experimental plants), processing and interpretation of experimental data, publication of research papers, etc.)

Thesis structure and number of pages

Publications

Key results of research are described in nine publications. Four of them are published in journals recommended by the Higher Attestation Commission and one is published in a journal indexed by Scopus. One certificate of state registration of a computer program has also been obtained.

Publications in international journals indexed by Scopus:

- 1.
- 2.
- 3.

Publications in journals from the list of the Russian Higher Attestation Commission:

- 1.
- 2.
- 3.

Publications in other journals:

- 1.
- 2.
- 3.

Основное содержание работы

In the introduction the relevance of the research conducted within the framework of the thesis work is justified, the purpose of the research is defined, the tasks of the work are set, the scientific novelty of the work, its theoretical and practical significance, as well as the possibility of implementation of its results are indicated.

In the

In the first chapter is given a review of the state of science and technology on the subject of quantum key distribution. Quantum communication protocols using both discrete [1–4] and continuous variable [5–9] are considered. The features of coherent detection methods [10] used in quantum key distribution systems are described and analyzed. The issue of phase noise in quantum key distribution systems is highlighted. Examples of methods to compensate for phase noise are demonstrated, such as applying pilot pulses [11] and creating feedback [12]. Known attacker's attacks on equipment within QKD systems are shown [13–15]. The laser seeding attack on the transmitter laser, its impact and possible defense methods are described [16–18]. Another aspect under consideration is an attack on the power of the local oscillator transmitted in the channel for quantum key distribution systems on continuous variables, the principle of its implementation, the result of the attack and methods to counteract it [19–22].

In the second chapter, we investigate the optical injection method [23;24] for creating feedback in the quantum key distribution system at side frequencies [25–27]. The optical injection method is that there is a pair of lasers: a master laser and a slave laser. The radiation from the master laser is injected into the resonator of the slave laser. Injection of additional photons into the resonator of the slave laser reduces

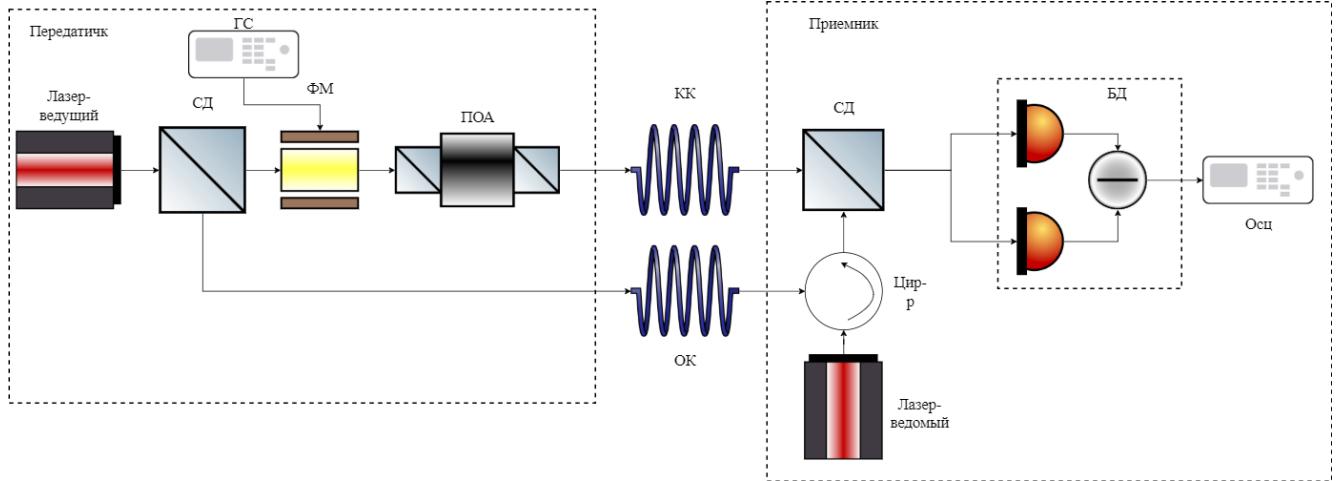


Figure 1 – Schematic diagram of the QKD system experiment using optical injection. SD - beam splitter, FM - phase modulator, GS - signal generator, POA - tunable optical attenuator, QC - quantum channel, OC - open channel, Qir-r - circulator, BD - balance detector, Osz - oscilloscope

the relaxation oscillation time of the radiation, which accelerates the radiation generation process and reduces negative effects. This approach improves the emission characteristics of the slave laser in particular:

- narrowing of the spectral line of the output radiation
- Reduction of nonlinearities and suppression of relaxation oscillations
- Reducing the output pulse chirp and increasing amplitude stability

This approach allows synchronizing the frequencies of the master and slave lasers, and as a consequence, reducing their relative phase noise, achieving phase synchronism. This effect allows optical injection to be used as a feedback implementation for the local oscillator in a QRC system at side frequencies using continuous variables. The result of the feedback application will be stabilization of the intermediate frequency and reduction of phase noise. To implement this method, a separate channel and circulator is used to separate the radiation of the master and slave laser. This method can be applied to a quantum key distribution system at side frequencies. This system, the optical scheme of which is shown in Figure 1, works as follows. At the transmitter side, the radiation generated by the laser is split into two parts. The first part of the radiation goes to an Alice phase modulator, where phase modulation by an alternating electrical signal takes place, in which phase shifts are introduced to encode the information. Quadrature Phase Shift Keying or

Quadrature Phase Shift Keying (QPSK) modulation can be used as encoding. This digital modulation method introduces phase shifts corresponding to values of 45° , 135° , 225° and 315° . These phase shift values are assigned bit values 00, 01, 10, 11. As a result, three harmonics of the signal appear in the spectrum: ω - the centre frequency of the laser, $\omega - \Omega$ - the lower side frequency and $\omega + \Omega$ - the upper side frequency, where Ω is the modulation frequency. The radiation after modulation is described by Eq:

$$F_s(t) = A_0 * \sin(\omega_0 t + \varphi_0) + \frac{A_0 * m}{2} * (\sin((\omega_0 + \Omega)t + (\varphi_0 + \varphi(t))) - \frac{A_0 * m}{2} * (\sin((\omega_0 - \Omega)t + (\varphi_0 - \varphi(t)))), \quad (3)$$

where A_0 is the amplitude of the original radiation, ω is the centre frequency of the laser, $\omega - \Omega$ is the lower side frequency and $\omega + \Omega$ is the upper side frequency, Ω is the modulation frequency, φ_0 is the phase of the original radiation, $\varphi(t)$ is the phase of the modulating radiation, t is the time, m is the modulation index. Modulation index is the value of the ratio of power at side frequencies to the power in the whole spectrum. The modulation index is proportional to the amplitude of the modulating electrical signal. The obtained spectrum falls on a variable optical attenuator, the attenuation of which is adjusted in such a way that at the side frequencies there is a power corresponding to a given average number of photons, when the carrier can remain classical. The prepared quantum states are transmitted into the quantum channel. The second part of the radiation passes through a separate fiber channel to the receiver side, where it enters the fiber circulator so that the radiation enters the slave laser resonator. The incoming radiation from the quantum channel enters the first input of a fiber beam splitter with two inputs and two outputs and a 50:50 splitting ratio. The second input of the beam splitter is a local oscillator, which is the radiation generated by a separate laser on the receiving side. Due to the presence of feedback in the form of optical injection, the wavelength of the laser on the receiving side is synchronized with the wavelength of the Alice laser. As a result, the LO and quantum states interfere at the beam splitter. As a result of this interference, additional harmonics at an intermediate frequency appear at the output of the beam splitter. These harmonics are $\omega - f$ - the central frequency

of the Alice laser minus the LO frequency, $(\omega - \Omega) - f$ - the lower side frequency minus the LO frequency and $(\omega + \Omega) - f$ - the upper side frequency minus the LO frequency, where Ω - the modulation frequency, ω - the Alice laser frequency, f - the LO frequency.

The result of this interference is detected by a balance detector. This device is two classical photodiodes connected so that their currents are subtracted. This connection reduces the intrinsic noise of the detector. After that, the received current is passed to a low-pass filter to filter out the constant component. The resulting signal is amplified by an amplifier stage and sent to the ADC. As a result, only one signal is formed at the output of the balance detector at the frequency coinciding with the modulation frequency on the transmitter side. The reason for this is that the wavelengths of the LO and the transmitter laser coincide due to feedback in the form of optical injection. Thus, only the $(\omega + \Omega)$ component f remains at the detector output, and the rest is converted to a constant component, which is filtered out. The received oscillation at the output of the balance detector carries phase information encoded by Alice. This signal is processed by digital signal processing techniques to extract the phase value of the signal.

The resulting bit sequence is the raw key. The received key is sifted. In the obtained sifted key, the quantum bit error rate (QBER) is estimated by first opening a part of the key. And the last step is secrecy amplification using HASH functions. To the pluses of this method of realisation of the QKD can be attributed the simplicity of the system, due to the fact that there is no active selection of the basis in the form of a modulator of any type. The presence of feedback in the form of optical injection allows to solve several problems: stabilisation of the LO wavelength, which also simplifies the final system, and reduces phase noise associated with the randomness of the phase of laser radiation generated by different sources. The use of heterodyne method of reception allows to use any type of modulation, which allows to flexibly adjust the protocol for different tasks and leaves the future for increasing the speed of key generation.

The disadvantages of this system include the need for an additional fibre-optic communication channel for feedback, which is partially offset by the fact that real

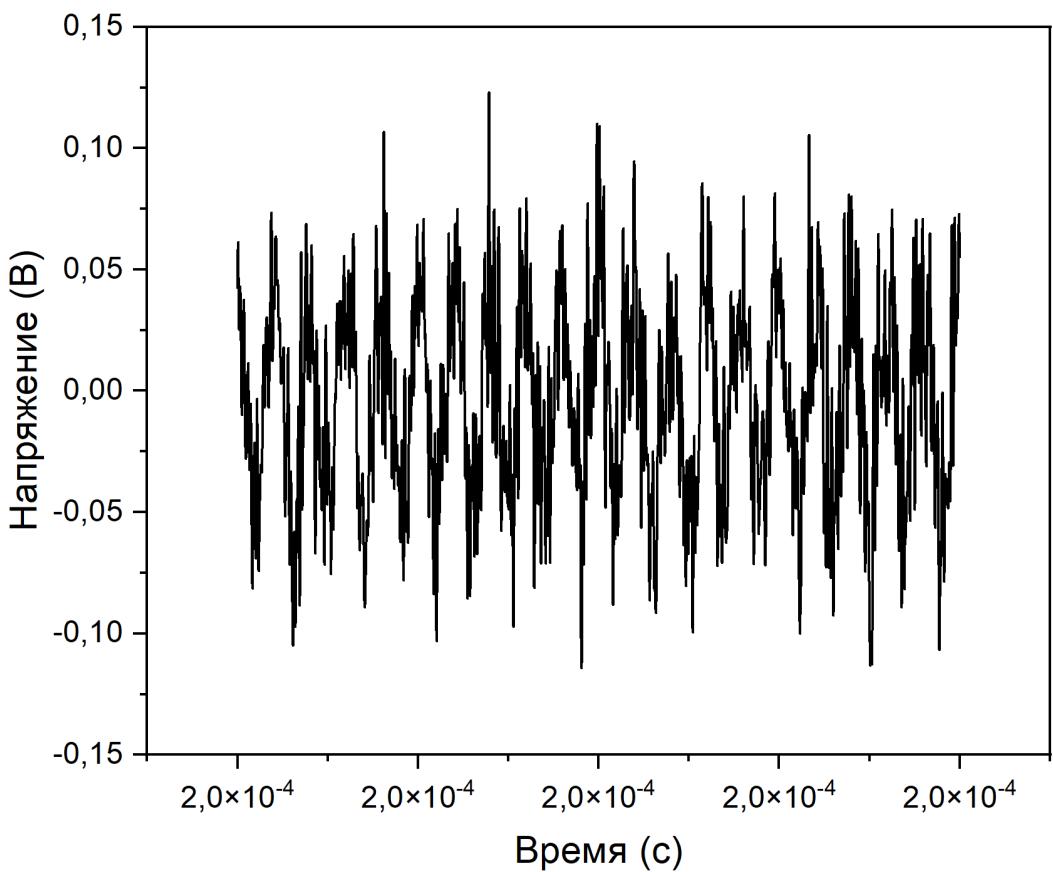


Figure 2 — Noisy signal at the output of a balanced detector

QKD systems are embedded into existing data transmission systems that work with multiplexing technology and the optical injection signal can be embedded into already used channels, as it has no requirements to the level of third-party noise. The second drawback, however, is the vulnerability to laser seeding attack, which requires further study and countermeasures.

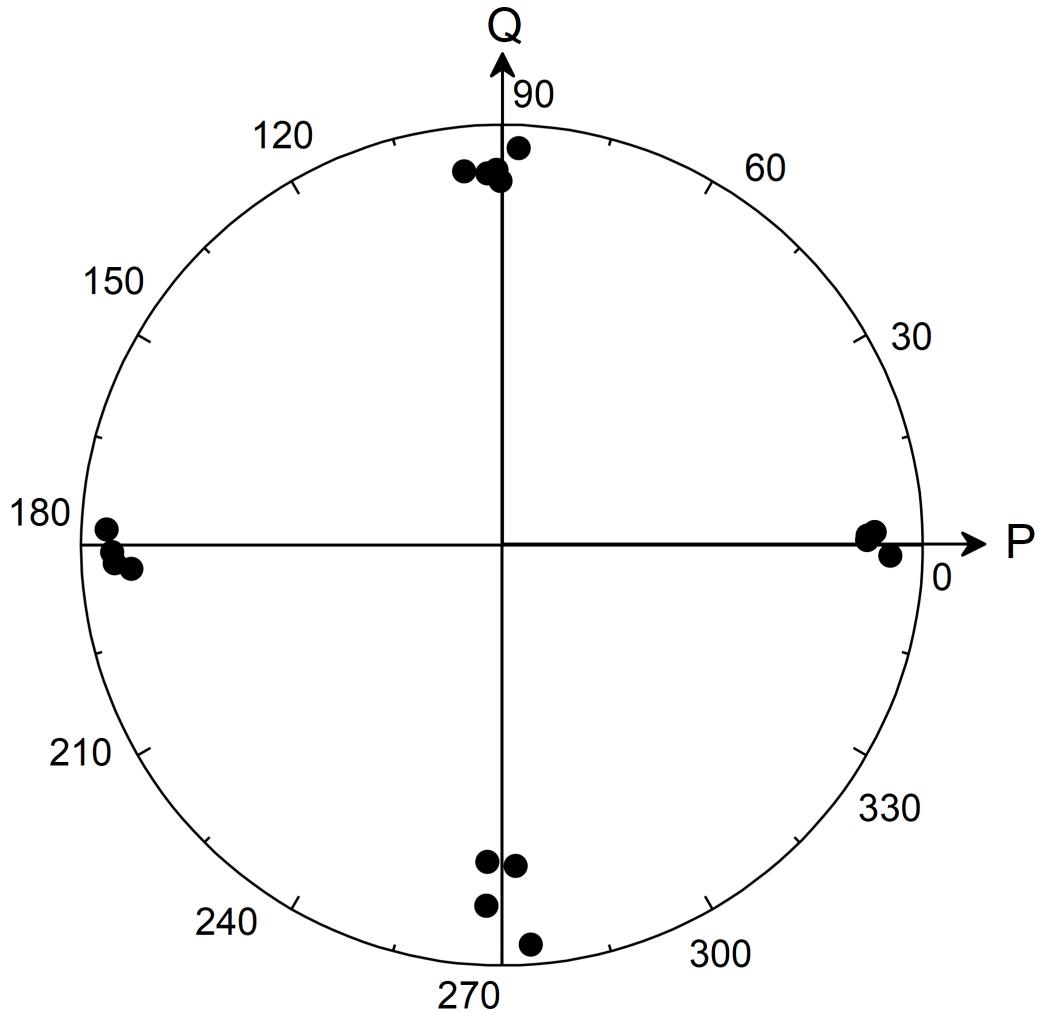


Figure 3 — Phase values obtained after digitalisation

In the third chapter, a scheme for applying the heterodyne detection method to detect [28–30] signals with two independent signal sources [8; 20] for a quantum communication protocol at side frequencies is discussed. A feature of this system is the transfer of quantum states of light to side frequencies that appear in the emission spectrum. The basic implementation of this protocol involves the use of discrete variables and single photon detectors based on avalanche photodiodes for signal registration. However, it is possible to adapt this protocol to use coherent detection methods [27; 31].

In this paper we propose the use of heterodyne signal detection method for a quantum communication system at side frequencies. This system works as follows. A laser on the transmitting side generates coherent radiation. This radiation, having passed through the necessary passive elements in the form of optical isolators, reaches the crystal of the phase modulator. An alternating voltage at the modulation

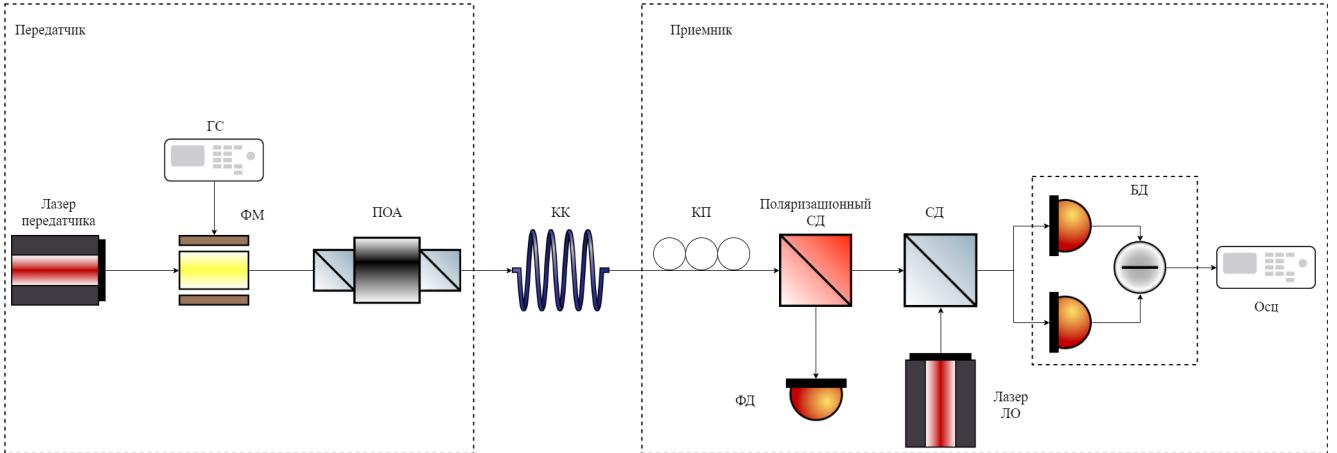


Figure 4 — Scheme of a quantum key distribution system at side frequencies with an independent local oscillator. SD - beam splitter, FM - phase modulator, GS - signal generator, POA - tunable optical attenuator, QC - quantum channel, BD - balance detector, Osz - oscilloscope

frequency is transmitted to the electrical input of the phase modulator. A phase shift is introduced into this voltage, which corresponds to bits of information. Quadrature phase-shift keying or quadrature phase-shift keying (QPSK) is used as an example in this paper. The phase shift values in this case are 45° , 135° , 225° and 315° and the following information bits 00, 01, 10, 11 correspond to these phase shifts. As a result of this modulation, three harmonics appear in the spectrum of radiation after the phase modulator, two of which encode information from the transmitter. The prepared radiation is attenuated by a variable attenuator to achieve a power level at side frequencies less than 1 photon on average. The quantum states thus obtained are transmitted via a fiber optic communication line to the receiving side.

The transmitted signal from Alice, after passing through the fiber optic link, reaches the polarization controller to compensate for the distortions introduced by the passage through the fiber. After that, the polarization beam splitter is installed and only the desired polarization is selected and the radiation with the desired polarization is allowed to pass through. The quantum states are then mixed with the LO generated by a separate laser on a beam splitter with two inputs and two outputs and a 50:50 splitting ratio. These signals interfere and as a result of this interference, the emission spectrum is enriched with additional harmonics. These harmonics appear because the frequencies of the LO and the Alice laser do not

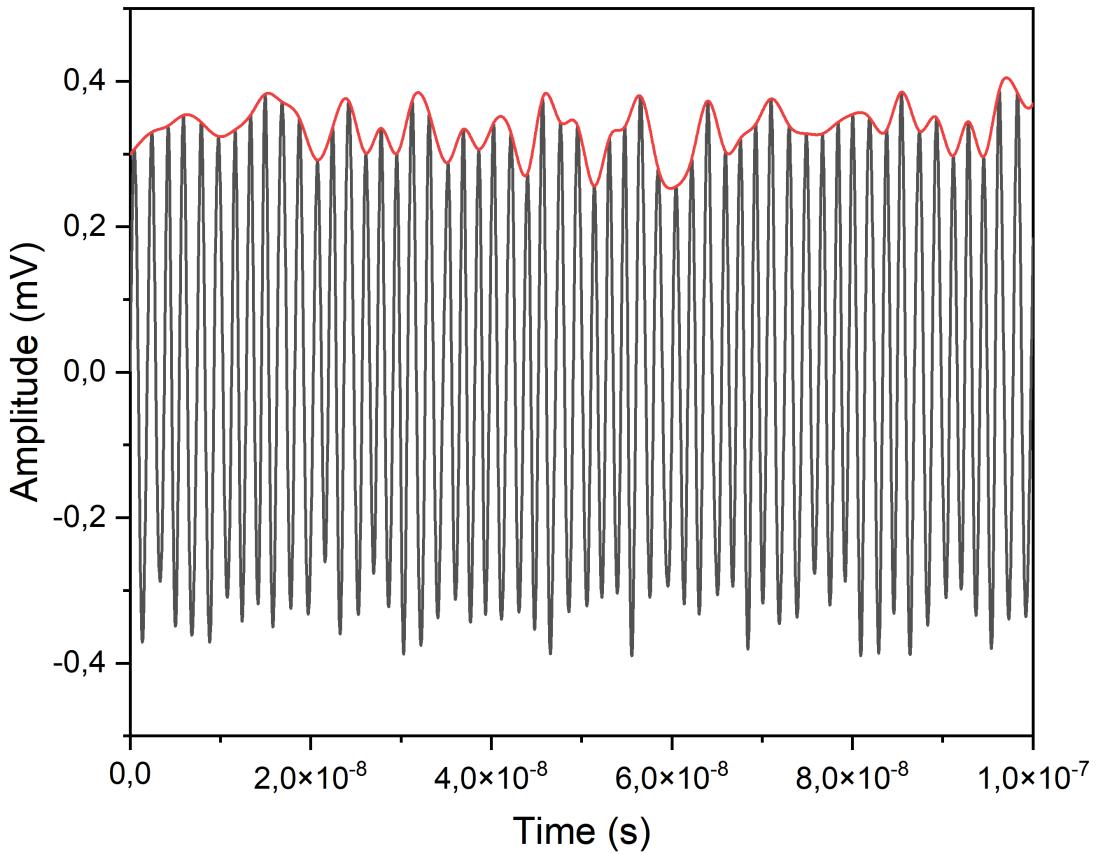


Figure 5 — The signal at the output of the balanced detector after heterodyne reception

match. These spectral components are at different frequencies - total, difference and Raman. But given the limited bandwidth of the balance detector, we can observe at its output only harmonics at difference frequencies that fall into it. Total and other combinational frequencies do not fall into the bandwidth of the DB and are registered as a constant component, which loses all the information encoded in their phases. Whereas the harmonic oscillations at the difference intermediate frequency pass the amplifying stage unchanged and retain the information encoded in the phase of Alice's emission. In this way, the spectrum is transferred from the optical domain to the radio frequency domain, where amplification and signal processing are simplified.

A balance detector is a device that consists of two photodetectors connected so that

their photocurrents are mutually subtracted. The received signal is then filtered to eliminate the influence of the constant component of the photocurrent. After that the received signal goes to the amplifier stage to increase its amplitude. The presence of the amplifier stage limits the bandwidth of the entire device. Typical bandwidths can vary from 100 MHz to 1.2 GHz. This limits the range of received frequencies and the raw key generation rate.

The received signal after amplification must be digitised by an ADC for further processing. As processing can be applied various methods of digital signal processing, such as Fast Fourier Transform or Hilbert Transform. As a result of this processing, phase values are generated from the harmonic signal received after the ADC, which correspond to given bit values from which a bit sequence called raw key is formed. However, using LO at the receiver side requires tweaking its polarisation and the polarisation of the quantum states for effective interference at the receiver. In this work, a polarisation control algorithm based on Fast Fourier Transform is proposed. The essence of this algorithm is that when a polarisation beam splitter is used, the modulation frequency that carries the information from the transmitter is doubled. This appearance of the doubled frequency can be tracked in the frequency domain. The following algorithm is used for this purpose

1. Apply FFT to the received signal
2. Analyse the spectral composition of the signal
3. Rotating the polarisation of the signal until the harmonic is eliminated at twice the modulation frequency.
4. Further rotation of the signal polarisation to the harmonic maximum at the modulation frequency

As a result of its operation, it is possible to adjust the polarisation by using active polarisation control, which will use the FFT result as feedback to adjust the polarisation. Figure ?? shows the spectrum of an information signal with distorted polarisation. The information about the presence of a doubled modulation frequency is fed to the polarisation controller and it starts its operation until the true modulation frequency is maximal and the doubled modulation frequency disappears. The result of the algorithm is shown in Figure ?? . The spectrum of the signal at

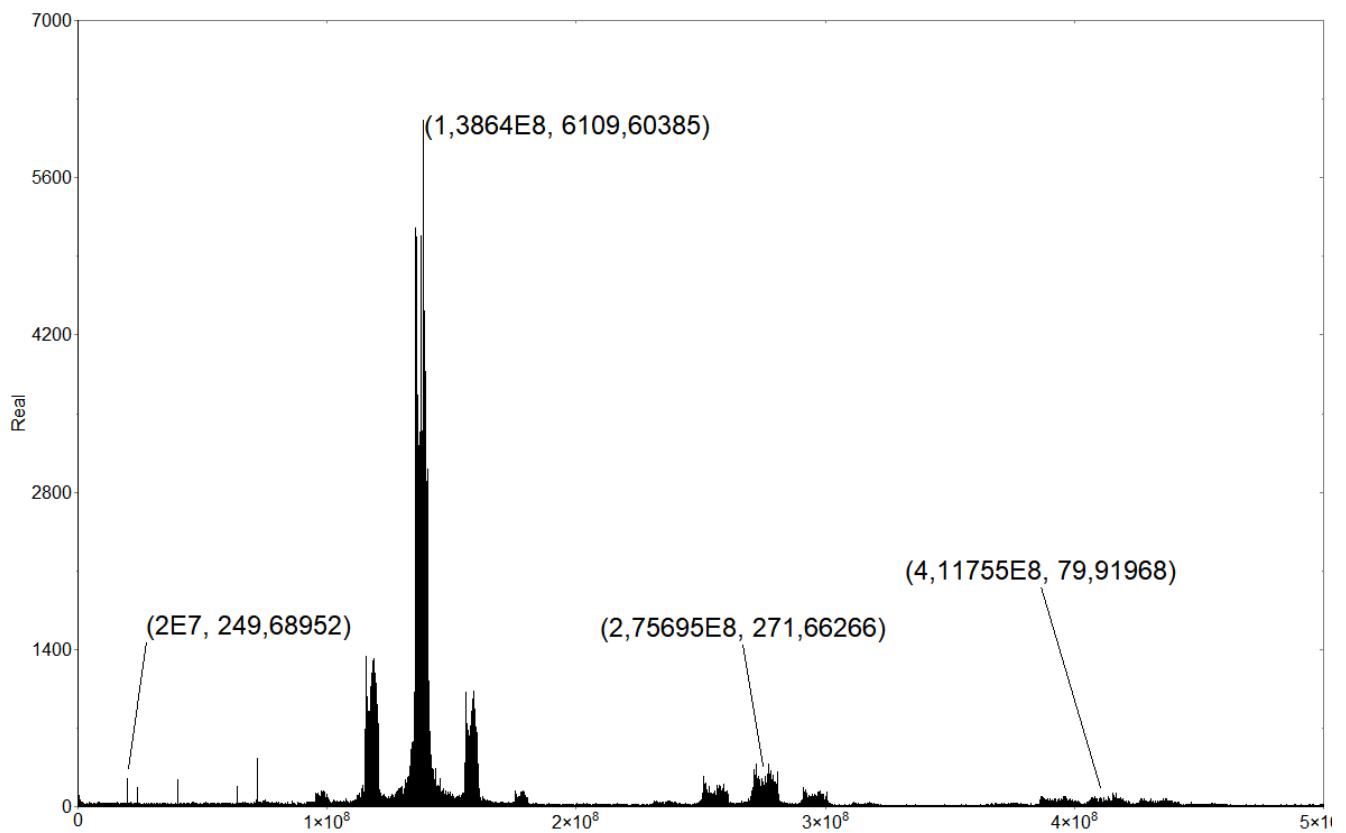


Figure 6 — Spectrum of ruined polarisation

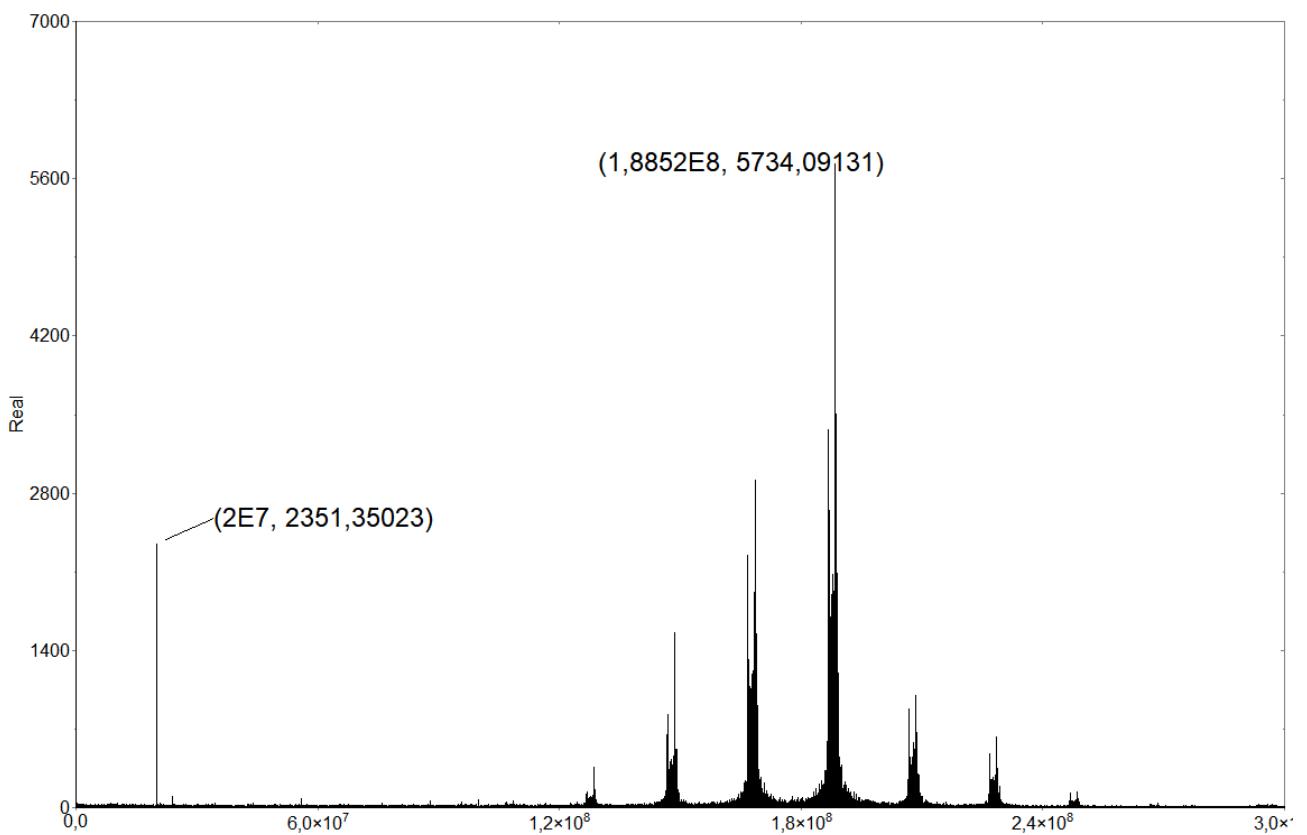


Figure 7 — Spectrum of a signal with distorted polarisation

normal polarisation contains no harmonic at the doubled frequency and the harmonic at the modulation frequency is maximal.

To the advantages of this method can be attributed flexibility in the choice of protocol, as the transfer of information to the intermediate frequency allows you to analyse almost any modulation without the need to introduce additional elements, for example, phase modulator to select the basis. The use of two independent sources of coherent radiation allows not to use feedback systems, which require an additional optical channel and open additional opportunities for an intruder. Generation of a local oscillator on the receiver side allows to increase its power, compared to protocols in which LO is transmitted over a quantum channel, which allows to reduce noise associated with scattering in the FOCL and increase the signal-to-noise ratio, which positively affects the bit rate.

From the disadvantages of the same can be highlighted the need to adjust the frequency, as two independent oscillators need periodic frequency adjustment. This problem is solved by the peculiarity of the protocol of quantum communication at side frequencies due to the fact that in the spectrum there is a powerful carrier, which is also knocked down with the local oscillator and is transferred to an intermediate frequency. By analyzing this frequency after FFT processing, it is possible to adjust the LO frequency so that all signals fall within the bandwidth of the balanced detector. Another disadvantage is the random phase noise due to the randomness of the laser generation process in two independent sources. This problem is solved by analyzing the phase of the intermediate frequency between the local oscillator and the optical carrier obtained after Alice phase modulation. This signal will contain the phase noise of both the LO and the transmitter laser, which can be accounted for in post-processing by pre-processing with digital methods.

Chapter Four is devoted to the study of the effect of the intruder radiation at a wavelength of 1310 nm on the source of coherent radiation based on a semiconductor laser diode with distributed feedback. This vulnerability in its technical implementation is called optical pumping attack [32; 33]. This type of attack is similar to the Laser Seeding attack [16; 17] in that Eve injects its radiation into the laser resonator on the transmitter to alter its characteristics. However, there is a significant difference. In the case of a seeding attack, the attacker uses the same or close wavelength to the operating wavelength of the laser under attack. Whereas in the case of an optical pumping attack, Eve uses a laser wavelength that differs by 50 nanometers or more from the operating wavelength of Alice's laser. This feature makes it possible to more effectively circumvent countermeasures using passive fibre-optic elements in the form of isolators [34–36]. Their isolation coefficient has a spectral dependence, which leads to the fact that the insertion isolation at 1310 nm wavelength is significantly smaller than at 1550 nm wavelength. As a result, the attacker requires less probing power to achieve the desired effect.

This attack is constructed as follows. The attacker installs a fibre circulator with three ports into the break in the fibre optic link. Eve's probing laser is plugged into the first port. The second port is plugged into the fibre optic link towards the sender side and the third port is plugged into the receiver side. In this way the intruder's radiation will enter the optical circuitry of the transmitter, and Alice's radiation will pass through the fibre towards the receiver without any problems. The intruder's radiation undergoes attenuation as it passes through the optical circuitry of the transmitter, so it is necessary to have sufficient probing power to make changes to the laser characteristics. The passed radiation enters the laser crystal and is absorbed in it [37]. This causes an additional population inversion to be created, resulting in a shift in the Watt-Ampere characteristic of the laser while the pump current is unchanged. This causes the calibrated radiation source on the transmitter side to start emitting more power than originally intended. As a result, this causes the output average photon number to increase, generating a larger number of multiphoton states, which opens up the possibility of realising a photon number splitting attack. The same effect is manifested in the change of the

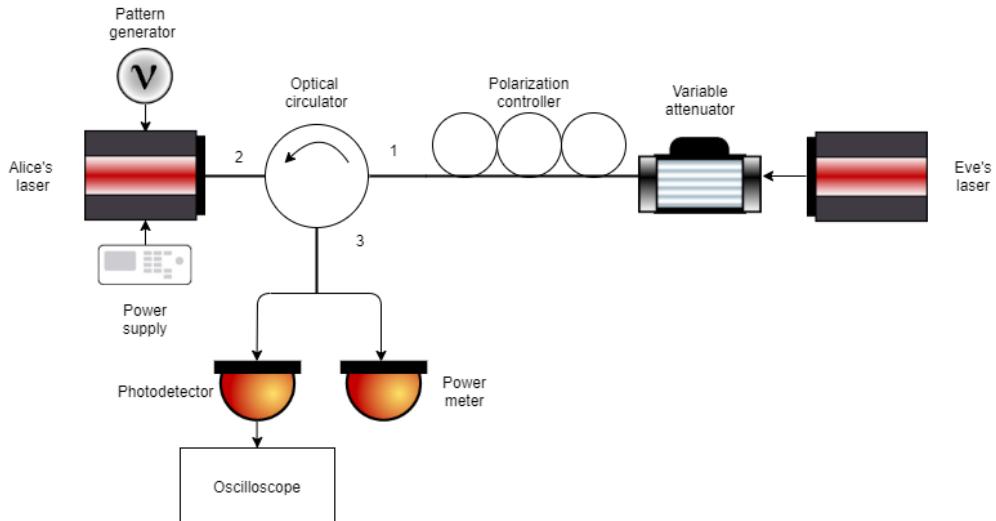


Figure 8 — Schematic of the laser seeding experiment. Alice's Laser - Alice's Laser, Pattern generator - pulse sequence generator, Power Supply - laboratory power supply, optical circulator - optical circulator, polarisation controller - polarization controller, varriable attenuator - tunable attenuator, Eve's laser - intruder laser, Photodetector - photodetector, power meter - power meter, Oscilloscope - oscilloscope

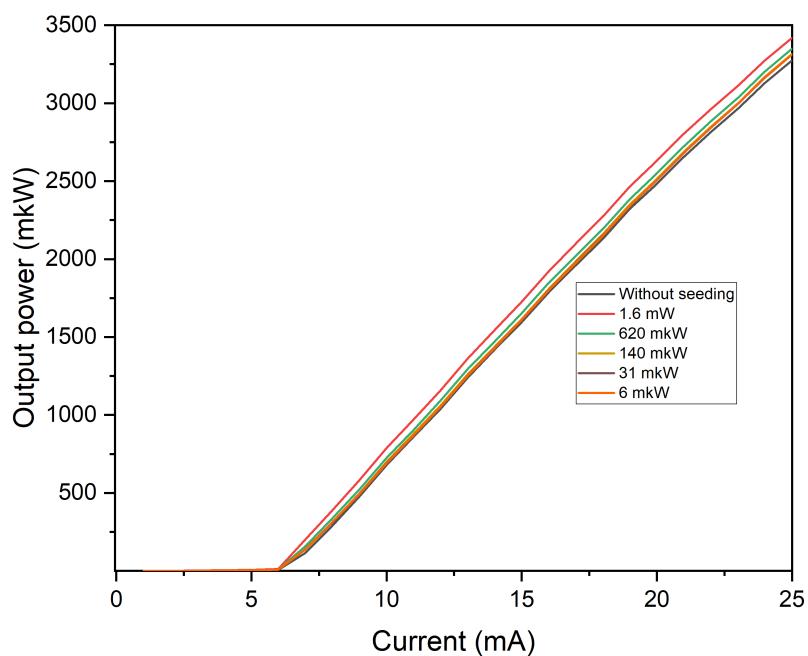


Figure 9 — Variation of Watt Ampere characteristics under different pump powers at 1310 nm wavelength. Output power is output power in microwatts, current is current in milliamperes

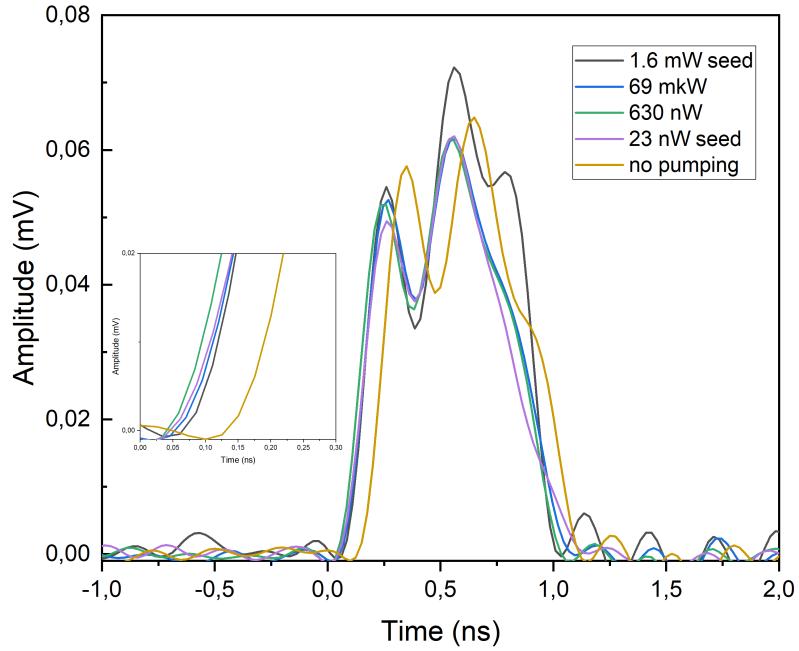


Figure 10 — Change of pulse shape under the action of external optical pumping at different powers at the wavelength of 1310 nm. Amplitude is amplitude in millivolts, Time is time in nanoseconds, seed is seeding, and pumping is pumping

pulse shape. Optical pumping [38–40] increases the pulse area and, consequently, its energy, increasing both the average number of photons in signal pulses and the average number of photons in decoy states in the BB84 protocol with decoy states [24].

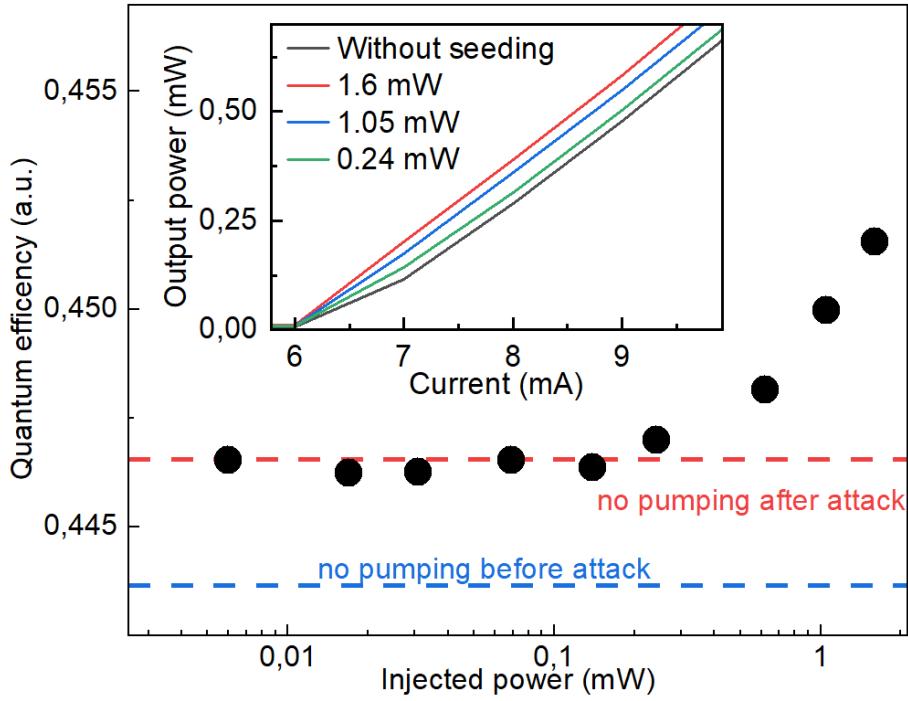


Figure 11 — Change in quantum efficiency due to external radiation at 1310 nm wavelength. Quantum efficiency - quantum efficiency in relative units, Output power - output power in milliwatts, Injected power - injected power in milliwatts, current - current in milliamperes, blue dashed line - value of quantum efficiency before attack, red dashed line - value of quantum efficiency after attack.

In the framework of this work, we show the implementation of an optical pumping attack at a wavelength of 1310 nm, which leads to an increase in the laser output power at constant pump currents, an increase in the pulse area, and an increase in the quantum efficiency of the laser. These effects create conditions for other types of attacks on the QRC system. In the case of this work it was shown that a probing power of $200 \mu\text{W}$ is sufficient to increase the quantum efficiency by 1%, demonstrated in the graph 11 and to increase the output power by 4%. The minimum power required for an attacker to effectively attack a typical optical transmitter circuit implementing the BB84 protocol was calculated.

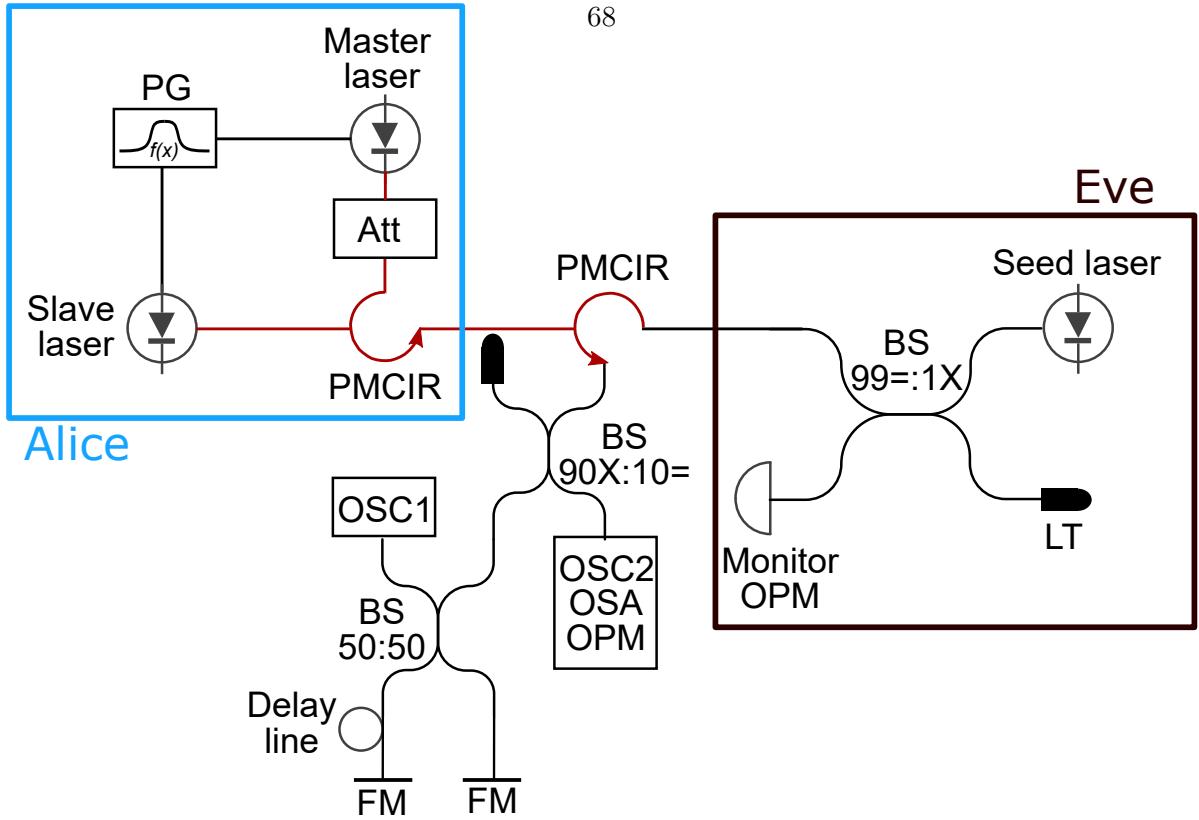


Figure 12 — Optical schematic diagram of laser source seeding setup based on optical injection

The research conducted in the chapter six is devoted to the study of the effect of high-power coherent radiation on a laser source based on optical injection. Such sources are actively used in quantum communication systems implementing a protocol with an untrusted receiver node [41–43]. Such sources have improved output signal amplitude stability, temporal wavelength stability, and reduced output pulse chirp by reducing the influence of transients during generation. These features allow us to obtain a Hong-Ou-Mandel interference prominence close to the theoretical maximum of 0.5.

However, such sources have not been investigated methods of influence such as attack 'seeding' laser [44]. For this purpose, an optical circuit was assembled to investigate the effect of high-power laser irradiation in the power range from 180 to 900 mW.

Two distributed feedback semiconductor lasers were assembled as the source. The first laser was an Agilecom WSL934010C4124-42 laser with an integrated isolator, which was used as the master laser to generate the reference radiation. The

second laser, however, was an Agilecom WSL5-934010C4124-82 laser, similar to the first laser, but without an integrated insulator. This is to maximize the amount of radiation injected into the resonator of the slave laser. The two lasers are connected to each other via an optical circulator. Its first port is connected to the master laser, the radiation from which enters the second port of the circulator where the slave laser is connected. In this way, the study from the master laser enters the resonator of the slave laser. The radiation from the slave laser enters the second port of the circulator and passes to the third port of the circulator. A Gooch&Housego AA1406-193300 laser and an erbium fiber amplifier were used as a source of high-power laser radiation. To introduce its radiation, an additional circulator was used, the first port of which was connected to the amplifier output, the second to the third port of the first circulator. A Michelson fiber interferometer was assembled to investigate the interference of the received pulses.

In the course of this work, the characteristics of the output pulses under the influence of external radiation were investigated. The following parameters were studied: amplitude of output pulses and their stability expressed in the measurement of standard deviation, duration of pulses and their standard deviation, as well as the correlation of the phase of the received pulses using a fiber Michelson interferometer. During exposure, the standard deviation of the energy of the output pulses was varied between 2 and 3.5 per cent at an attack laser power of 900 mW and by varying the master laser power. The results of these measurements are shown in Figure 13. These results show that Eve is able to increase the output power instability to increase the average number of photons per pulse. The pulse duration is also altered by external radiation, shown in Figure 14 the external influence increases the pulse jitter by 2%. Existing work shows [45] that even small deviations in pulse duration significantly reduce the distribution range of the secret key.

To develop a countermeasure, it is necessary to calculate the necessary isolation factor for the worst case scenario, when the attacker uses the maximum available power. In continuous mode, this value is 2 watts. This value needs to be attenuated to less than -35 dBm. By using a fibre optic circulator as part of the circuit, the isolation value is already 50 dB. To calculate the required attenuation value, the

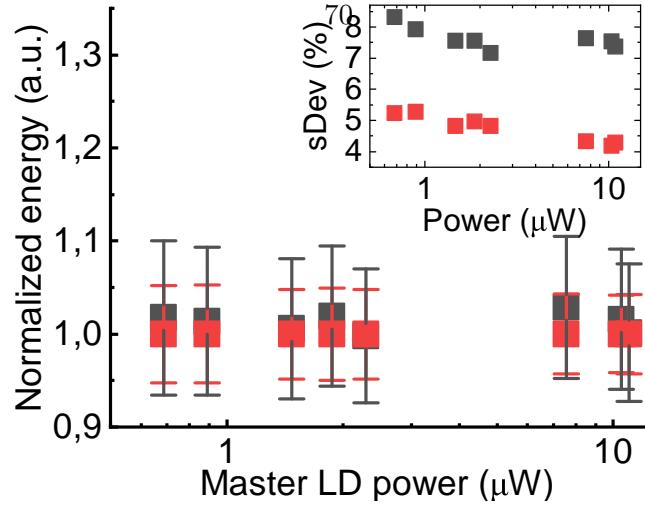


Figure 13 — Change in source pulse energy with and without external radiation as a function of master laser power

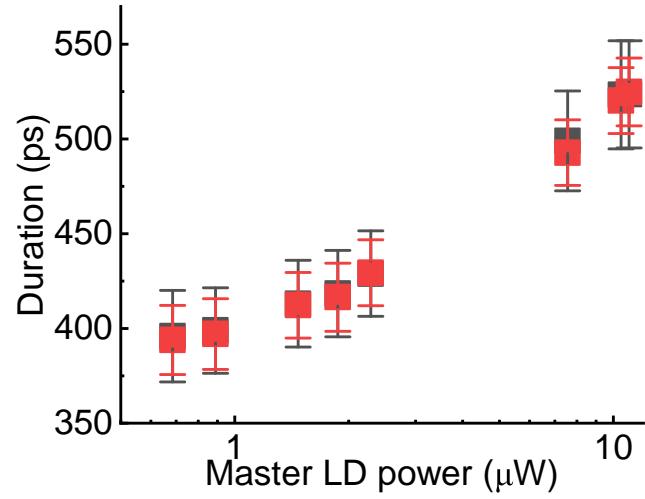


Figure 14 — Change in pulse duration due to external radiation

following formula is used

$$\alpha = P_a - P_{req} - \beta. \quad (4)$$

, where α is the amount of isolation to be introduced, P_a is the amount of probing power in dBm, P_{req} is the power to which the input radiation needs to be attenuated, β is the amount of isolation that is already implemented in the circuit, in dB. Let's substitute in 4 the values of 33 dBm of power, which corresponds to 2 watts of power and 50 dB of isolation. The resulting isolation value required to attenuate 2 watts to -35 dBm is 18 dB. To ensure the safety of this source, it is sufficient to install a fiber isolator with a typical isolation value of 30 dB. This will cover the entire allowable range of sensing power.

The obtained results demonstrate the resistance of the proposed source of coherent radiation to external influences. To change its characteristics, an intruder needs to operate at powers close to those that trigger a spark in fibre-optic communication lines, which carries an increased risk of being detected. And protocols based on the protocol using an untrusted receiver node are not only secure from attacks of an intruder on receiver nodes in the form of single photon detectors, but also from attacks on single photon sources.

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 доступа.

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 классическим 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 отсутствие 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 интерферционная 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 уязвимость 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 воздействиям 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 2×2 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 информации 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 когерентного 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 являться система квантового распределения ключа на непрерывных переменных с применением гетеродинного детектирования с независимым ЛО. Суть данной системы заключается в том, что на приемнике и передатчике установлены 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 теоретических 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, отличной от рабочей. При этом это излучение поглощается активной средой лазера передатчика так, что поглощенное излучение выступает в роли оптической накачки, которая работает как дополнение к электрической накачке 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 длине 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. Засевивание 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 передатчик и приемник, не будучи обнаруженным. Это преимущество вкупе с использованием шифрование методом одноразового блокнота, для которого доказана абсолютная стойкость, 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 двухмерном Гильбертовом пространстве как два базовых вектора

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (1.1)$$

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

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

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 $|1\rangle$ соответственно. Для векторов, соответствующим значениям фазовым набегам $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ получаются следующие вектора:

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

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

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

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

Полученные векторы описывают дискретные состояния, 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, посвященная протоколу квантовой коммуникации, была опубликована в 1984 году, ее авторы Чарльз Беннет и Жиль Брассард [46]. 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 не полностью 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 ($n \leq 1/2$), 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 злоумышленник 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 осуществлена 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 злоумышленник, не знающий ключа, 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 [2]. В 1.1.2 рассматривался протокол, который использует четыре попарно ортогональных, которые находятся в одном базисе, состояния для кодирования квантовых состояний. В случае же протокола B92 предлагается использование всего двух неортогональных состояний из двух базисов. Благодаря этому протокол B92 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 злоумышленником, 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 злоумышленником), 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 темнового счета, которые можно обнаружить и исправить.)
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-

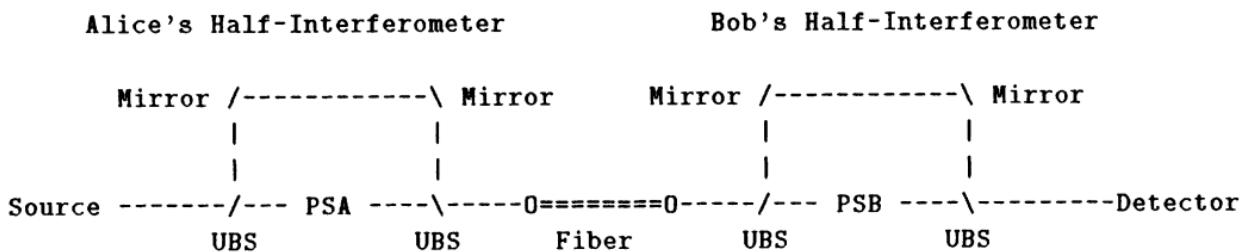


Рисунок 1.1 — Интерферометрическое квантовое распределение ключей с использованием двух неортогональных низкоинтенсивных когерентных состояний. Источник слева поставляет когерентный импульс (волнообразная форма -W-) с интенсивностью ожидаемых фотонов M) 1 в полуинтерферометр Алисы, где несимметричные 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 конструктивная 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. В сигнальный импульс вносится фазовый сдвиг (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

разделить 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 конструктивная интерференция, 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 δt 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 злоумышленник ("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. Ева 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 P_0 и P_1 , 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 злоумышленник 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 пересыпая 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 P_0 , 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 (ν), но и любых двух некоординированных смешанных состояний P_0 и P которые охватывают не пересекающиеся подпространства гильбертова пространства, позволяя Бобу найти два оператора P_0 и P , таких что P_0 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 некогерентных 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 приемного 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) [?; 47], как простое решение для устранения всех (существующих и еще не обнаруженных) каналов утечки информации, связанных с детектором [48], 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) [49] и Готтесмана-Ло-Люткенхауса-Прескилла (GLLP). [50] 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 это не 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) [1] 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 состоянию. Давайте теперь подробно оценим производительность протокола выше. Для простоты рассматривается улучшенный анализ данных, при котором Алиса и Боб оценивают данные, отправленные в двух разных базисах [51]. В частности, используется линейный базис в каче-

стве базиса генерации ключей, в то время как диагональный базис используется только для тестирования.

Для обозначений введем $Q_{rect}^{n,m}$, $Q_{diag}^{n,m}$, $e_{rect}^{n,m}$, $e_{diag}^{n,m}$ - обозначают, соответственно, усиление и QBER сигнальных состояний, отправленных Алисой и Бобом, где n и m обозначают количество фотонов, отправленных законными пользователями, а $rect$ 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, 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, получаем, что $e_{rect}^{n,m}$ 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 ключей протокола квантовой криптографии (в части коррекции ошибок).

(B) Диагональный базис. Чтобы определить количество необходимой амплитудации конфиденциальности, рассматривается 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, находим, что $e_{diag}^{1,1} = 0$. (Это происходит потому, что когда два идентичных однофотонных входят в 50:50 светоделитель, эффект Хонга-Оу-Манделя [52] 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 выходном плече, оба фотона всегда достигнут одного и того же детектора внутри ретранслятора.)

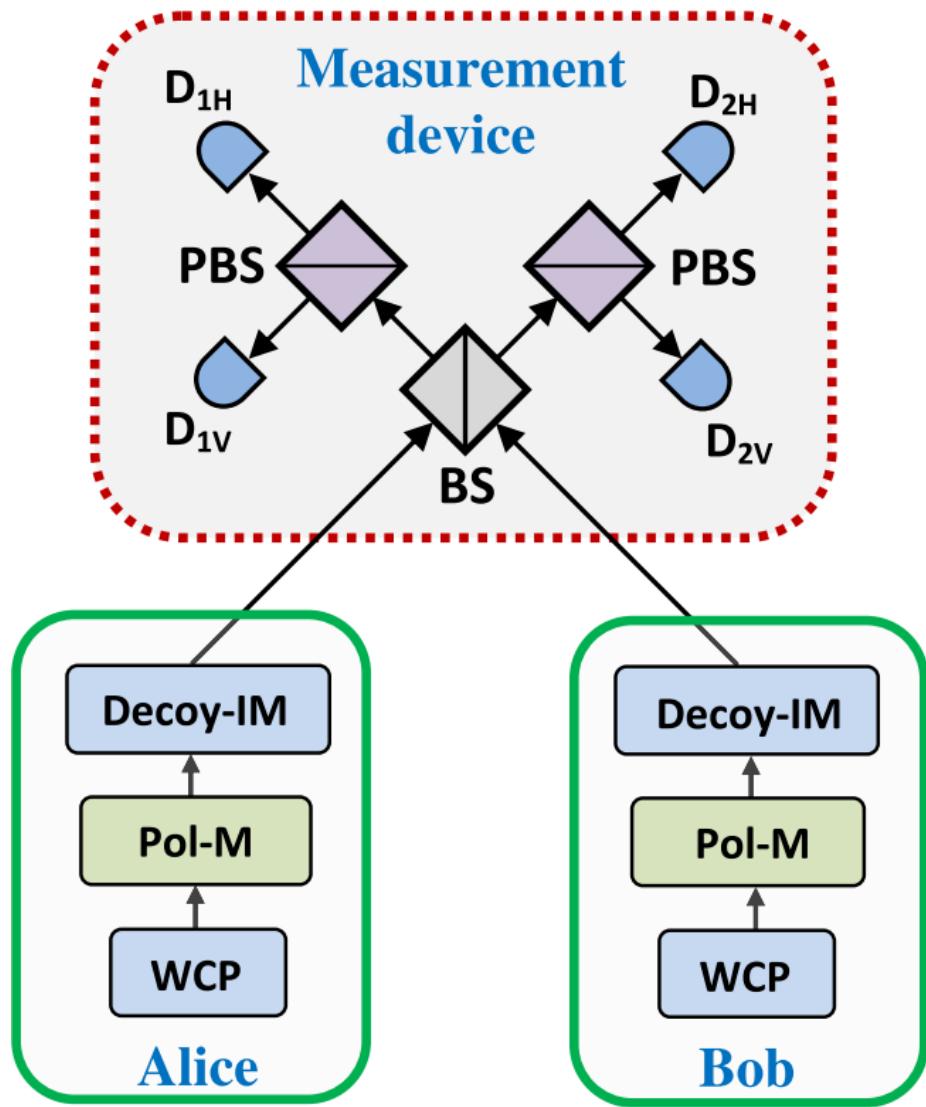


Рисунок 1.2 — Базовая схема протокола MDI-QKD. Алиса и Боб подготавливают фазово случайные слабые когерентные импульсы (СКИ) в разных поляризационных состояниях BB84, которые выбираются независимо и случайным образом для каждого сигнала с помощью модулятора поляризации (Pol-M). Состояния - ловушки генерируются 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} и D_{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 злоумышленника, в то время как измерительное устройство может быть ненадежным.

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).

(С) 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 учитываются недостатки, такие как смещение базиса и темные отсчеты, скорость генерации ключей в реалистичной настройке будет определяться как

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

, где Q_{rect} и E_{rect} обозначают, соответственно, усиление и QBER в прямоугольном базисе (то есть $Q_{rect} = \sum_{n,m} Q_{rect}^{n,m}$ и $E_{rect} = \sum_{n,m} \frac{Q_{rect}^{n,m} e_{rect}^{n,m}}{Q_{rect}}$, $f(E_{rect}) > 1$ 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, предполагается, 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. Для целей моделирования рассматриваются неэффективные и шумные пороговые детекторы и используем экспериментальные параметры из [54] за исключением того, что [54] рассматривает канал свободного пространства, тогда как здесь рассматривается канал на основе оптоволокна с потерей 0,2 дБ/км. Более того, для простоты предполагается, 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, используется протокол коррекции ошибок с функцией неэффективности $f(E_{rect}) = 1,16$ [55]. Полученная нижняя граница секретной скорости ключа проиллюстрирована на

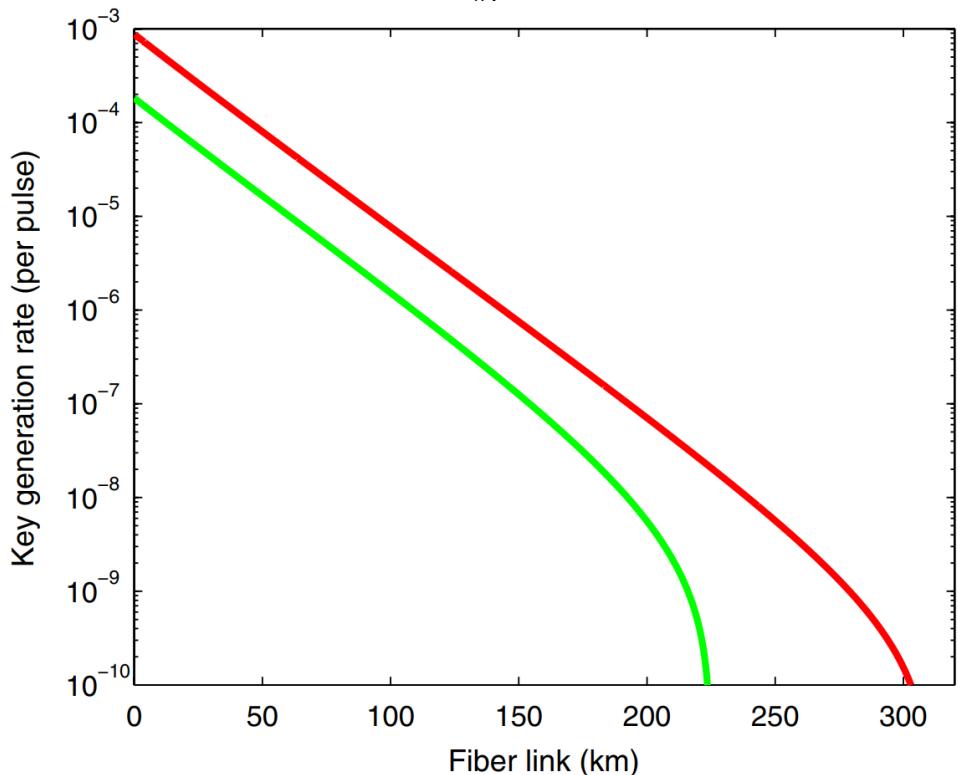


Рисунок 1.3 — Нижняя граница секретной скорости ключа R , заданная уравнением 1.1.4, в логарифмической шкале для установки MDI-QKD с использованием слабых когерентных импульсов, показанной на рисунке 1.1.4 (зеленая кривая). В целях моделирования рассматриваются следующие экспериментальные параметры: 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 $6,02 \times 10^(-6)$. (Для простоты рассматривается упрощенную модель смещения, помещая унитарное вращение в одну из входных ветвей светофильтра 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 параметрического преобразования с понижением частоты (PDC), расположенным посередине между Алисой и Бобом [53]. На красной кривой предполагается, 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

рисунке 1.6. Наши расчеты и результаты моделирования показывают, что скорость генерации ключей существенно сравнима с доказательством безопасности [53] для протоколов квантовой криптографии на основе запутанных пар. Наша схема может выдерживать высокие оптические потери более 40 дБ или 200 км ВОЛС, 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. 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 [52]. Обратите внимание, что физика, лежащая в основе этого протокола, основана на явлении группировки фотонов в одну группу двух неразличимых фотонов на 50:50 светоделителе. Здесь проводится 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 рисунке 1.6. 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 [50; 56], чтобы количественно оценить количество зависимого от базиса недостатка [57]. В-третьих, заметим, что в практических приложениях потребуется только конечное количество фальшивых состояний. Это аналогично стандартным протоколам квантовой криптографии с конечными

фальшивыми состояниями [58], которые широко используются в экспериментах [59]. 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 [60]. 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 [57].

В заключение, предлагается идея квантовой криптографии с недоверенным промежуточным узлом (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 квантовой криптографии с недоверенным промежуточным узлом. 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, считается 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) [61], которое улучшает масштабирование ключе-

вой 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 [54] и Пирандола-Лауренца-Оттавиани-Бьянки (PLOB) [55]. 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) [62]. 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 [62], 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 экспериментальная демонстрация КРК с полями-близнецами через протокол SNS (SNSTFQKD) по катушкам оптического волокна. Протокол.- Рассмотрим схему протокола SNSTFQKD [53], показанную на рисунке 1.4. Здесь реализуется протокол с помощью практического метода четырех интенсивностей [64], 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 ве-

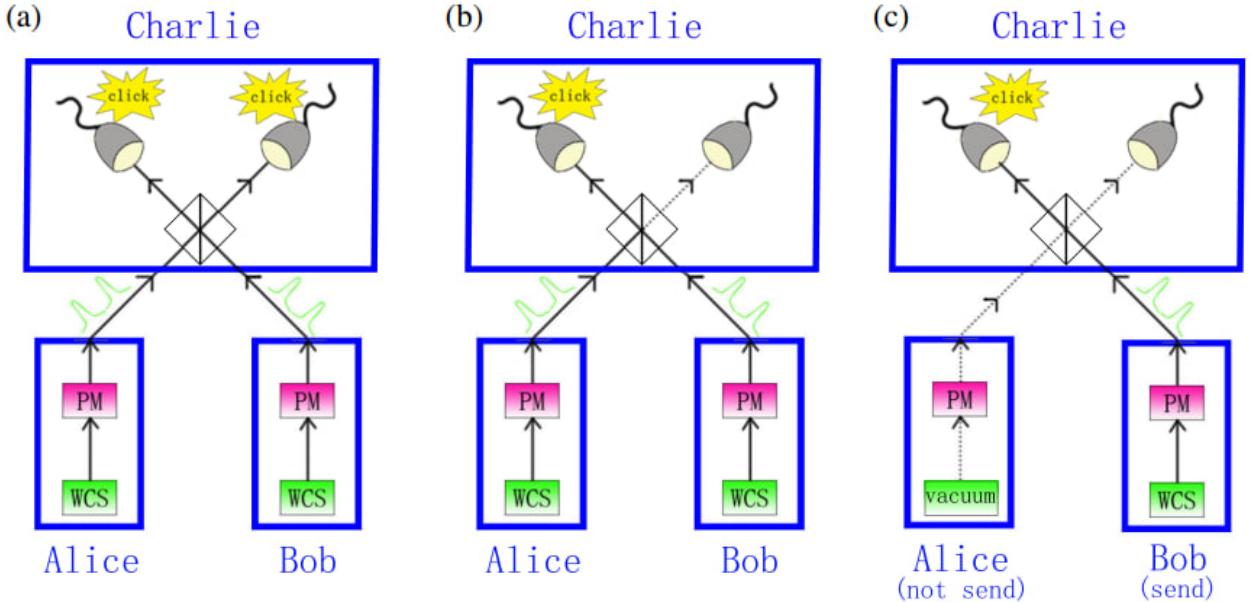


Рисунок 1.4 — Схемы трех различных протоколов. (а) MDIQKD с состояниями-ловушками, где пары импульсов с когерентным состоянием в кодировке BB84 рассылаются, а эффективные события предвещаются двукратным срабатыванием. Скорость передачи ключей линейно зависит от пропускания канала. (б) Оригинальное состояние приманки TFQKD [63], в котором сдвоенные поля когерентных состояний со случайными фазовыми сдвигами посыпаются 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. (с) SNSTFQKD (Sending - not sending TFQKD) с состояниями ловушками [58]. 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

роятностями 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 получить высокую скорость генерации секретного ключа, 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(а). 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 (AM). В эксперименте устанавливается базовый период 5 мкс, в течение которого в первые 3 мкс посыпается 100 сигнальных импульсов с шириной импульса 2 нс и интервалом 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 интерфери-

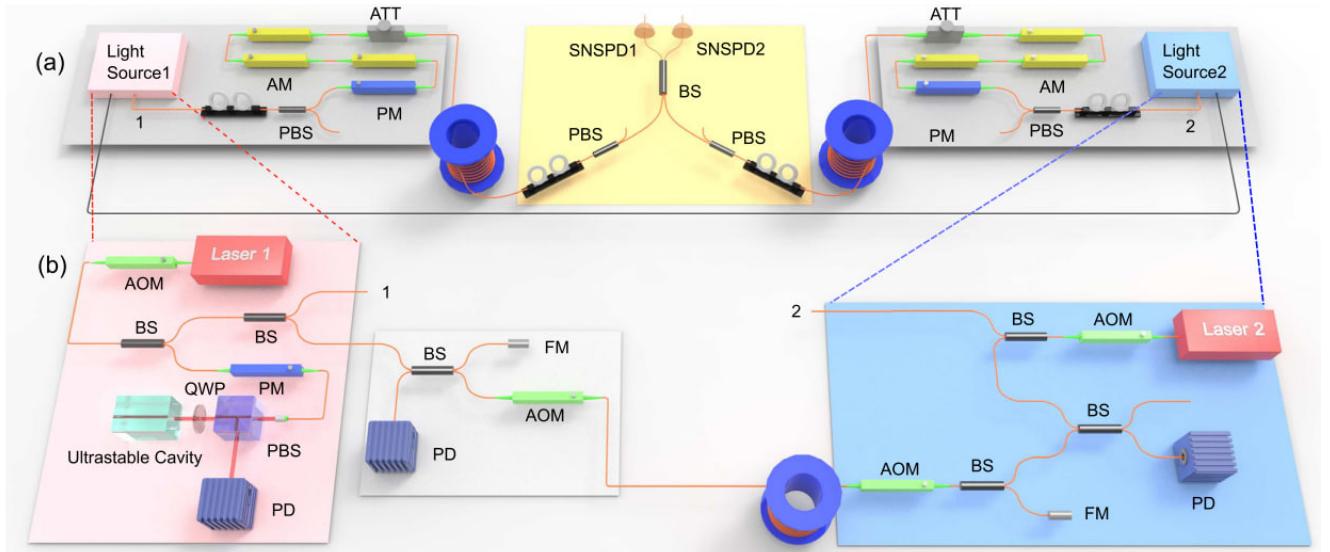


Рисунок 1.5 — (а) Схема нашей экспериментальной установки. В качестве источников Алиса и Боб используют непрерывный лазер с частотной синхронизацией. Эти лазеры затем модулируются фазовым модулятором (ФМ) и тремя амплитудными модуляторами (АМ) для рандомизации фазы, кодирования и модуляции интенсивности обманки. Затем импульсы ослабляются аттенюатором (ATT) и отправляются по оптоволоконным катушкам к Чарли. На измерительной станции Чарли 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). (б) Система частотной синхронизации для лазеров Алисы и Боба. Длина волокна между Алисой и Бобом установлена равной общей длине сигнального волокна. АОМ: акустооптический модулятор, FM: зеркало Фарадея, PD: фотодиод. QWP: четвертьвольновая пластина.

рут. 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

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

, 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. Чтобы справиться с разницей фаз, вызванной разницей длин волн, используется метод частотной синхронизации, 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 (АОМ) 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, разница фаз компенсируется с помощью постобработки. Определив оценочную относительную фазу между волокнами Алисы и Боба как $\Delta\varphi_T$, вычисляется квантовый коэффициент битовых ошибок в базисе X для обнаружений, лежащих в диапазоне

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

где $\theta_A(\theta_B)$ - случайная фаза, которой Алиса (Боб) модулирует сигнал, а Λ - заданный диапазон. Тогда вычислить безопасную ключевую скорость с эффектом

конечного размера данных по следующей формуле:

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

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 $\epsilon = 10^{-10}$, что соответствует общей вероятности отказа $2 * 10^{-9}$. Скорость передачи ключей была бы еще выше, если бы мы учитывали только статистические флуктуации. Здесь предполагается, что эффективность исправления ошибок составляет $f = 1.1$. В работе протестирован SNSTFQKD с общим расстоянием между Алисой и Бобом от 0 до 300 км. Во всех экспериментах с различными длинами волокон общее количество импульсов, посыпаемых Алисой и Бобом, установлено на уровне $7.2 * 10^{11}$. Достоверные детектирования составляют $6.5 * 10^9$, $2.3 * 10^9$, $2.3 * 10^9$, $7.6 * 10^8$ 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 экспериментально проверяется SNSTFQKD при вероятности темнового 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 генерации ключей уже превышает скорость MDI-QKD на расстоянии 108 км. Далее снижается вероятность темнового счета примерно до 10^{-7} (эквивалентно 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 $1.96 * 10^{-6}$, что выше границы PLOB, равной $8.64 * 10^{-7}$ на импульс. Моделирование показывает, что SNSTFQKD преодолевает эту границу на расстоянии 267 км, а расстояние

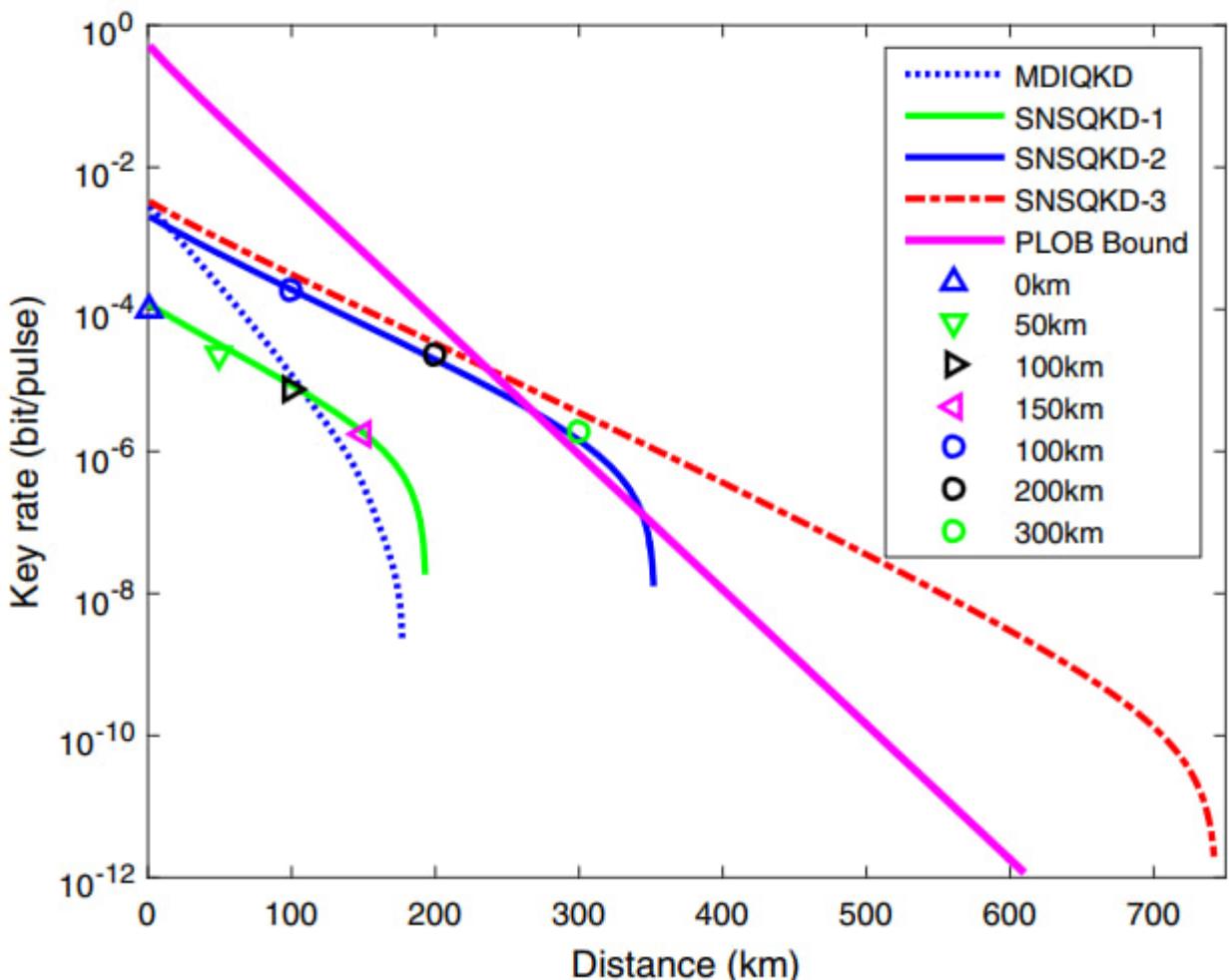


Рисунок 1.6 — Безопасные ключевые скорости и результаты моделирования SNSTFQKD. Треугольники показывают экспериментальные результаты для первого экспериментального теста, а сплошная зеленая кривая - результаты моделирования эксперимента, а сплошная зеленая кривая представляет результаты моделирования с вероятностью темнового 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 результаты для второго теста, а сплошная синяя кривая представляет моделирование с вероятностью темнового счета около 10^{-7} и базовой ошибкой X-базиса около 2 процентов. Общее количество 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.

передачи может превышать 350 км при экспериментальных параметрах. Наконец, моделируется безопасная скорость выработки ключей, предполагая, что всего будет отправлено 10^{14} импульсов (с $2.6 \cdot 10^5$ достоверными срабатываниями, накопленными на расстоянии 720 км), а вероятность темнового 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 разрабатывается технология фазовой синхронизации 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 синхронизации, 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 ожидается, 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) [10]. 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 большая 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 метод 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 детектирования, 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 когерентного 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.

Интенсивность в случае гомодинного детектирования будет описываться следующим выражением

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

, 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

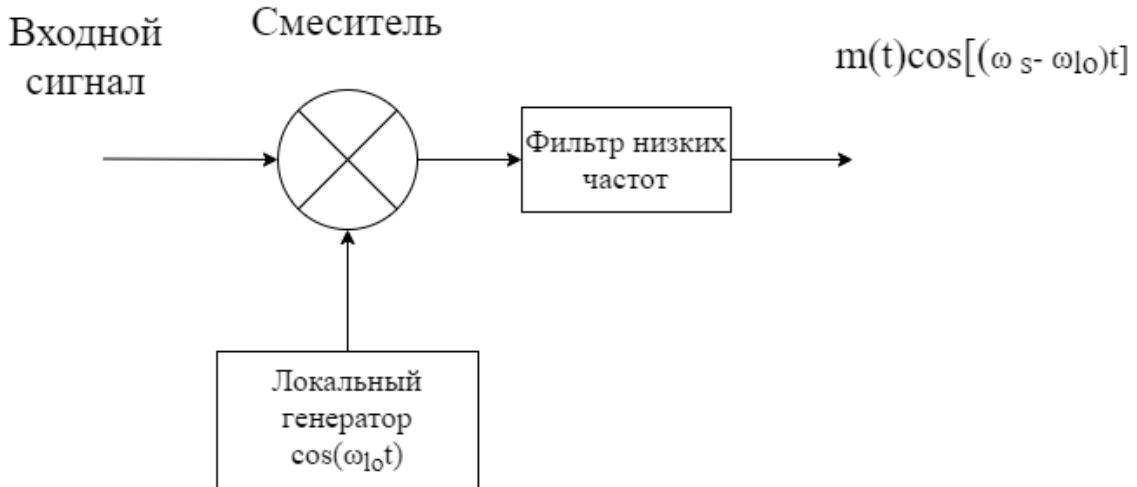


Рисунок 1.7 — Структурная схема гомодинного приема

информационного сигнала и ЛО. Но так как в случае гомодинного детектирования частоты излучения равны, то результат детектирования приводится к виду

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

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 когерентного детектирования является гетеродинное детектирование. Данный метод нашел свое широкое распространение в радиотехнике 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

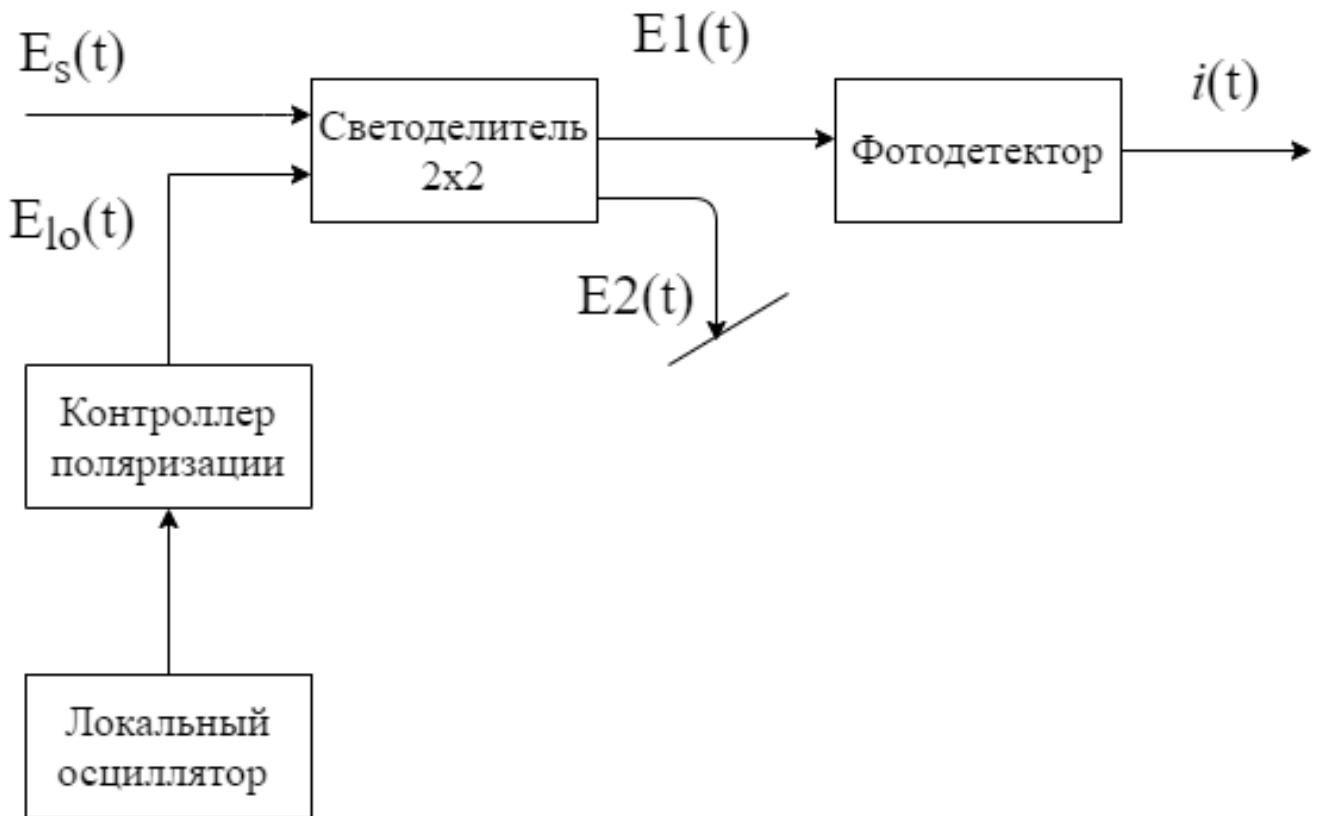


Рисунок 1.8 — Структурная схема гетеродинного оптического приемника

разности частот ЛО и входного сигнала. Данный метод описывается следующим образом:

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

, 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

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

В выражении 1.2.2 присутствует разностная частота $\omega_1 - \omega_2$, которая содержит себе информацию от входного сигнала о его амплитуде и фазе. Благодаря этому, возможно извлекать информацию из сложных типов модуляции, таких как квадратурно-амплитудная, при этом не прибегая к дополнительным техническим приспособлениям. Данный метод детектирования сигналов является

самым гибким для регистрации любых типов модуляции, 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 потеряны 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 классических 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 уровень 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, в КРК-НП [65] квантовые состояния кодируются в непрерывных переменных (НП) лазерного излучения, 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 [66] 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 [67], 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. Независимо от этого Хиллери [68] 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 [69] и основывалась на проверке корреляций типа ЭПР для обнаружения подслушивающего устройства. В 2000 году Серф и другие [70] предложили первый полностью непрерыв-

ный 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 секретности (УС) близко к теоретическим границам [71]. Другой протокол КРК-НП, основанный на гауссовой модуляции сжатых пучков, был предложен Готтесманом и Прескиллом [72]. 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 гауссовой квадратурной модуляцией и показали его защищенность от индивидуальных атак [73], прибегнув к НП-версии теоремы об отсутствии клонирования [74]. 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 [75]. 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 [76]. В 2004 году для протоколов с когерентным состоянием было предложено использование гетеродинного обнаружения [77]; 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 Наваскуэсом и другими [78] и Гарсией-Патроном и Серфом [79]. Коллективные гауссовые атаки были полностью охарактеризованы Пирандолой и другими [80], которые позже вывели мощности секретных ключей для КРК-НП [55; 81]. Безопасность от коллективных атак была расширена на общие атаки Реннером и Цираком [82] 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, в том числе с доверенным шумом [83–85]. Следующим развитием стало изучение эффектов конечного размера и полностью композитных доказательств. Стоит также упомянуть о существовании других направлений исследований, в которых при вычислении скорости секретного ключа учитываются ограничения реалистичного подслушивающего устройства [86; 87]. В следующих разделах, помимо стандартных односторонних гауссовских протоколов (основанных на когерентных или сжатых состояниях), 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, здесь явно не обсуждаются протоколы, основанные на использовании негауссовых операций, таких как вычитание фотонов [88], квантовый катализ [89] или квантовые ножницы [90].

1.3.1 Протокол квантового распределения ключа с использованием модуляции 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 протоколом 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 зарегистрировал сигналы с помощью гомодинным детектированием). 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 u для этого кода. Чтобы восстановить u , Алисе нужно просто исправить x , то есть декодировать в код смежного класса, 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 модуляцией Гаусса

Как и в случае КРК на дискретных переменных, протоколы КРК-НП "приготовление и измерение" в целом проще реализовать на практике [9]. Далее подробно описывается реализация протокола GG02 [73], принцип и безопасность которого были рассмотрены в разделах 2 и 3 соответственно, с помощью волоконной оптики. Этот протокол особенно интересен с практической точки зрения [91], 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 волн, 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 (или локальный осциллятор), 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.

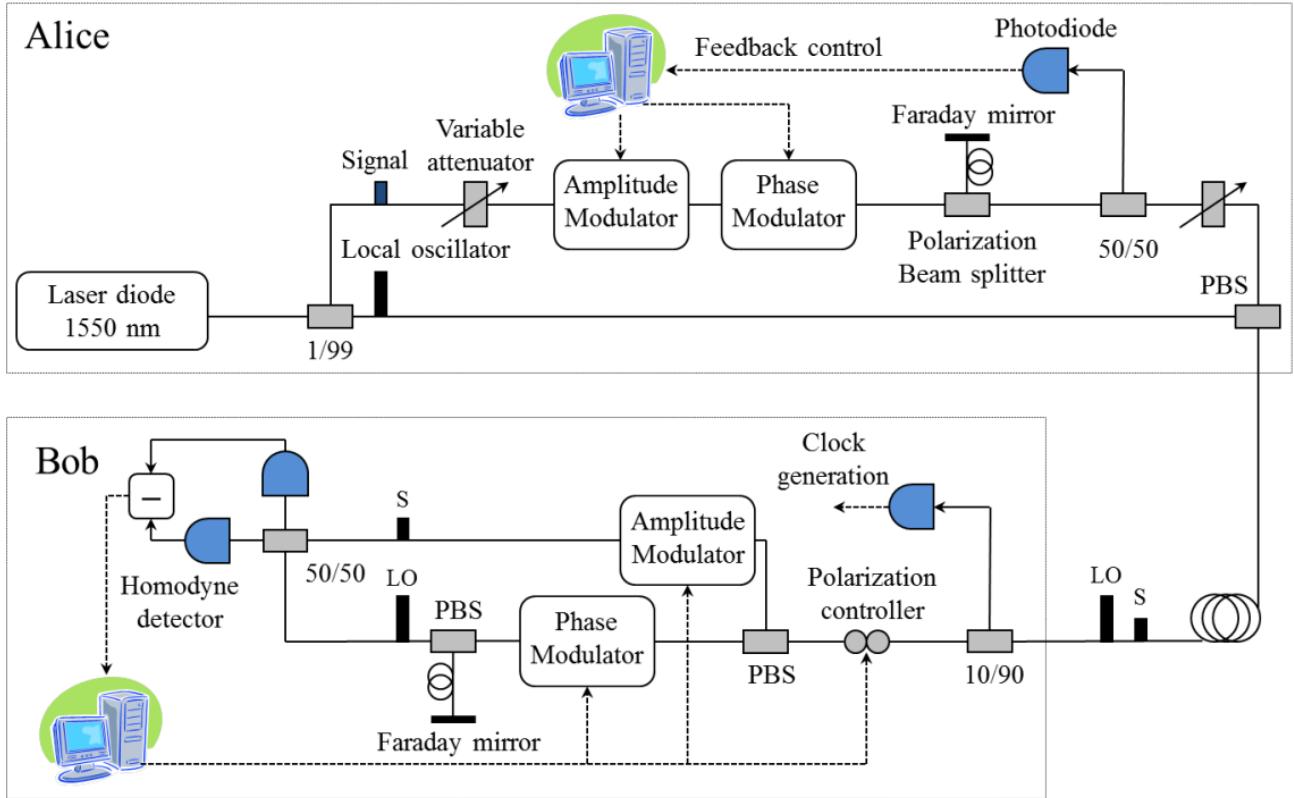


Рисунок 1.9 — Оптическая схема волоконной системы КПК-НП с гомодинным детектированием. Laser diode - лазерный диод, signal - сигнал, Local oscillator - локальный осциллятор, Variable attenuator - переменный аттенюатор, Amplitude modulator - амплитудный модулятор, Phase modulator - фазовый модулятор, 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.

На месте Боба два сигнала демультиплексируются с помощью линии задержки и поляризационного делителя луча и накладываются во времени для интерференции на ограниченный шумами сбалансированный 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, которая была развернута по проложенным оптическим волокнам и объединяла различные технологии КРК. 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. Эти реализации, а также некоторые другие, 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 извлечения секретного ключа на практике. Для оптической установки на рисунке 1.9 соответствующими экспериментальными параметрами являются дисперсия модуляции Алисы V_A , коэффициент пропускания канала Т 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 гомодинного детектирования. 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 модуляции Гаусса и локальным осциллятором, сгенерированным на приемной стороне

Как протоколы КРК на дискретных переменных (КРК-ДП), основанные на обнаружении одиночных фотонов [1; 3], так и протоколы КРК на непрерывных переменных (КРК-НП), основанные на когерентном детектировании [66; 68; 73] были продемонстрированы как жизнеспособные решения на практике. Одним из известных протоколов КРК-НП является протокол когерентного состояния с гауссовой модуляцией (ГМКС) [73], который был продемонстрирован на 80-километровой оптоволоконной линии связи [92]. 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 внут-

ренная функция фильтрации делает КРК-НП привлекательным решением для безопасного распределения ключей по зашумленному каналу, таком как освещенное волокно в обычной оптоволоконной оптической сети [93] или оптической линии связи в свободном пространстве [94]. 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 [73; 92; 94] 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 [15; 18; 19]. 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. 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. 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 [95], оптическая фазовая автоподстройка частоты [18], и оптическая инжекционная фазовая подстройка частоты [96], были разработаны для классической когерентной связи, но эти методы не под-

ходят 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 решается вышеупомянутая давно нерешенная проблема, 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) [8], основанной на протоколе когерентного состояния с гауссовской модуляцией. У отправителя, Алисы, в качестве оптического носителя использовался непрерывный лазер (CW) с узкой шириной линии ≈ 100 Гц, работающий на длине волны 1550 нм. Когерентные состояния готовились путем модуляции непрерывного лазера с помощью синфазно-амплитудного (IQ) модулятора, управляемого 16-битным цифро-аналоговым преобразователем (ЦАП) с двумя каналами, работающими с частотой дискретизации 1 ГВыб/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 аттенюатор (VOA) для регулировки дисперсии модуляции теплового-

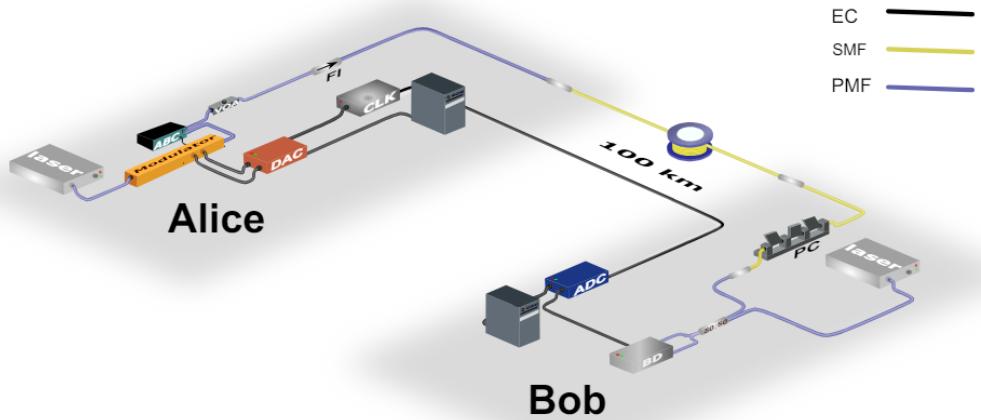


Рисунок 1.10 — Станция Алисы состоит из непрерывного (CW) лазера, работающего на длине волны 1550 нм, синфазного и квадратурного (IQ) модулятора с автоматическим регулятором смещения (ABC) для получения когерентных состояний на боковых частотах. Для управления IQ-модулятором использовался цифро-аналоговый 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 непрерывным 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 ГВыб/с.

го 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 непрерывный 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 светоделиителе, 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 ГВыб/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, проводились измерения "спина к спине" (B2B), в которых Алиса и Боб были соединены через короткий волоконный патч-корд, а VOA был тонко настроен 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 практическая конфигурация системы (ЛЛО КРК-НП) сталкивается с ограничениями по дальности передачи из-за фазового фазового шума лазеров. В данной работе демонстрируется 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, построенные 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

$$\zeta = \zeta_{RIN} + \zeta_{mod} + \zeta_{quant} + \zeta_{Ramman} + \zeta_{RPN} + K \quad (1.15)$$

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 протокола на когерентных состояниях, избыточный шум, связанный с ОФШ на приемной стороне определяется как

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

, 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 скорости выработки секретного ключа 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 [11]. Их суть заключается в том, что к квантовым состояниям мультиплексируется дополнительный классический сигнал, который является опорным для измерения фазового шума при прохождении квантового канала. После прохождения этими сигналами 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) [97]. В этом случае, два лазера сбиваются на фотоприемнике. Их разностная частота подстраивается так, чтобы она сравнялась с опорной частотой генератора, отно-

сительно 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, недостатки 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 атак 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 [98–101]. В результате этой атаки злоумышленник имеет возможность "навязывать" секретный ключ легитимным пользователям [102]. 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 [14; 103; 104]. Но существует и атака на источник излучения из состава системы квантового распределения ключей – атака "засевом" лазерным излучением [16; 17]. Одним из главных условий секретности распределенного ключа в системах КРК является предположение, что интенсивность квантовых 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 посыпает его в оптическую схему Алисы. В результате мощность, претерпевшая затухание из-за прохождения оптических элементов, попадает в резонатор лазера Алисы. Инжектированные таким образом носители увеличивают выходную мощность вынужденного излучения Алисы. Под действием излучения увеличивается и энергия импульса, и непрерывная мощность. В результате этого увеличивается 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 излу-

чением, а не непрерывным как в других работах. Интерференционная картина импульсов злоумышленника и Алисы будут скоррелированы 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 предотвращения.

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

Существующие системы квантового распределения ключей на непрерывных переменных используют один лазер для генерации квантовых состояний и локального осциллятора. 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 естественного затухания. Другой же недостаток данного подхода - уязвимость ЛО ко внешнему воздействию злоумышленника. В работе [19; 21] описывается атака на ЛО в системе КРК-НП. 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 осциллятора. 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 ($0 \leq \alpha \leq 1$) на часть ν ($0 \leq \nu \leq 1$) импульсов локального осциллятора для изменения их формы. Тактовая частота, формируемая для гомодинного детектирования, зависящая от этих импульсов, сдвигается на величину δ .
2. Ева вводит светоделитель в квантовый канал и для части μ ($0 \leq \mu \leq 1$) 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, выполненных 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. Рассмотрены подходы по созданию систем КРК на дискретных переменных по топологии "точка-точка" как и с недоверенным приемным узлом. Как альтернатива протоколам на дискретных переменных рассмотрены протоколы на непрерывных переменных. Продемонстрированы различные подходы к реализации локального осциллятора в системах КРК-НП. Показаны этапы протокола выработки битовых последовательностей для протоколов на дискретных

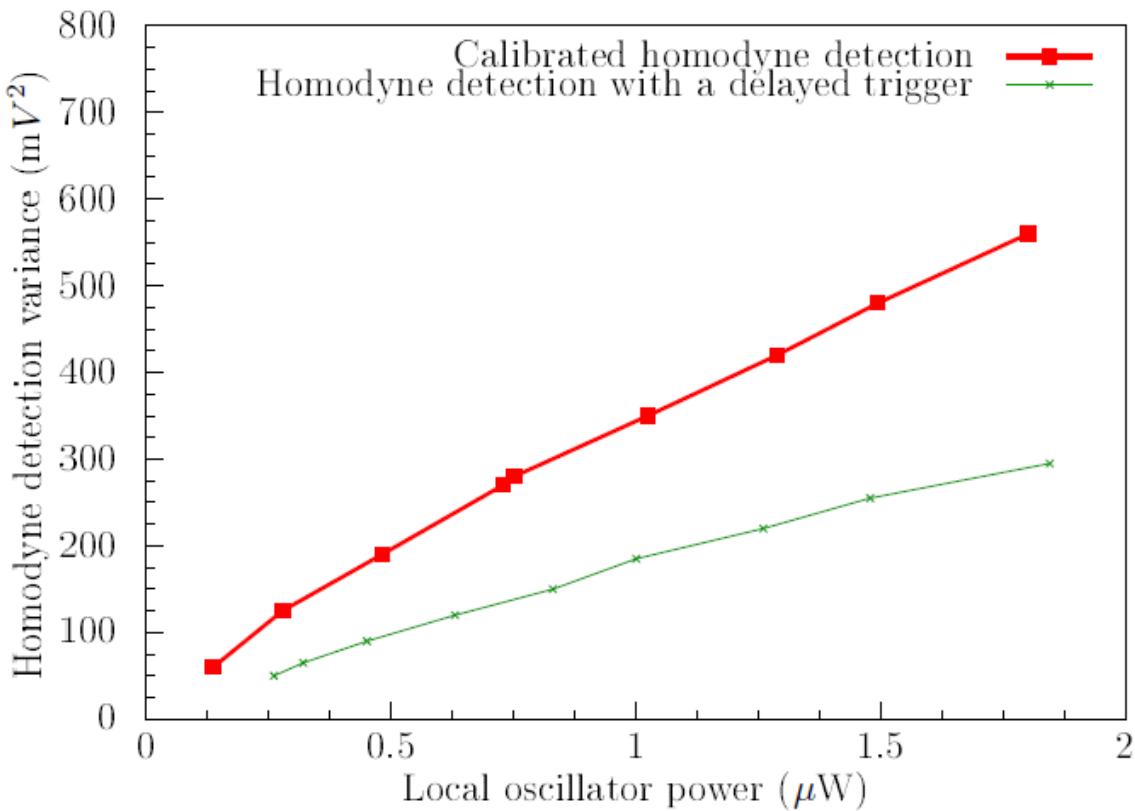


Рисунок 1.11 — График распределения шума гомодинного детектора без атаки (красный цвет) и под действием атаки (зеленый) на ЛО.

переменных, так и на непрерывных. Изучен вопрос атак на техническую реализацию систем квантового распределения ключей. Особенно акцентировано внимание на атаках на источники излучения в КРК. Все рассмотренные вопросы создают базовое понимание технологии КРК, которые необходимы для понимания последующих глав.

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

2.1 Система квантового распределения ключа на боковых частотах

Одной из существующих реализаций систем квантового распределения ключа является реализация на боковых частотах, предложенная Юрием Тарасовичем Мазуренко [25]. 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) [25] генерируются квантовые состояния на дополнительных оптических каналах, которые получаются в результате модулирования оптического лазерного излучения переменным электрическим сигналом с помощью электрооптического модулятора на основе кристалла ниобата лития. Такая реализация системы квантового распределения ключа дает преимущества в виде

1. Устойчивость 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 информационной 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 боковых частотах среди остальных.

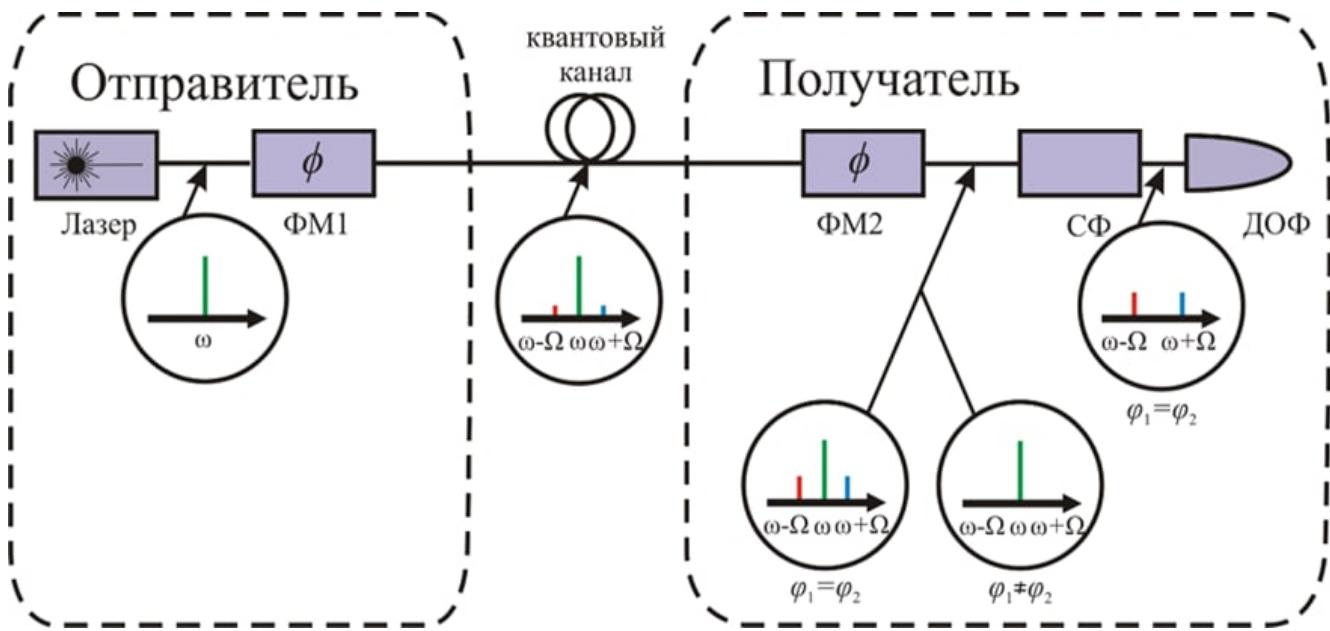


Рисунок 2.1 — Принципиальная схема установки системы квантового распределения ключей на боковых частотах.

Принцип работы системы КРКБЧ

Установка КРКБЧ, изображенная на рисунке 2.1 работает следующим образом. Полупроводниковый лазер с рабочей длиной волны генерирует излучение на длине волны 1550 нм. Это излучение передается по волоконно-оптическому тракту с сохранением поляризации на фазовый модулятор. На электрический же вход электро-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 сдвигов 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. Данное 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 переменный оптический аттенюатор (ПОА), который вносит затухание в пришедший сигнал до такого уровня, что на боковых частотах должна быть мощность, 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. Чтобы нивелировать искажения поляризации устанавливается поляризационный светофильтр, который разделяет пришедший сигнал по поляризации на линейную и циркулярную, при этом линейная проходит без изменений, а циркулярная поворачивается так, чтобы она стала линейной. После этого сигнал попадает на два фазовых модулятора. С помощью этих модуляторов происходит повторная модуляция, идентичная модуляции на стороне передатчика. В результате этого на боковых частотах будет наблюдаться интерференция, результат которой зависит от разности фаз между передатчиком и приемником. После повторной модуляции необходимо удалить несущую частоту, так как она не используется для генерации ключей. Для этого после поляризационного объединителя устанавливается спектральный фильтр на основе волоконной Брэгговской решетки. В результате после фильтра остаются только боковые частоты, которые несут в себе информацию о квантовых состояниях. Этот сигнал регистрируется детектором одиночных фотонов, который отправляет срабатывания в программируемую логическую интегрируемую схему, где формируется последовательность бит, называемая сырьем ключом. После формирования сырого ключа происходит общение по служебному каналу между приемником и передатчиком по служебному каналу для процедур просеивания ключа и ис-

правления ошибок. После исправления ошибок начинается операция усиления секретности, в результате которой формируется секретный ключ.

2.2 Метод оптической инжекции

Для систем квантового распределения ключа необходимы стабильные источники излучения с фиксированной длиной волны и без нелинейных эффектов в виде чирпа [42; 43]. Некачественные источники лазерного излучения приводят к нарушению интерференционной картины в случае протоколов MDI [41] или же снижению скорости генерации секретного ключа и уменьшения дальности его передачи в протоколах BB84 с применением состояний ловушек [45]. Одним из активно развивающихся решений этой проблемы является метод фазовой синхронизации с помощью оптической инжекции [24].

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 предполагает использование второго лазера, излучение которого попадает в резонатор другого лазера, образуя пару ведущий - ведомый [23]. 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 состав 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 квантового распределения ключей, в которых они используются.

2.2.1 Математическая модель оптической инжекции

Система уравнений описывающих излучение ведомого лазера:

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

и связанную систему для ведомого лазера:

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

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

2.3 Определение частотного 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

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

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

$$\Delta\omega_{\text{сих}} = z \sqrt{1 + \alpha^2(1 + 2\gamma_Q Q_c)}, \quad (2.4)$$

и где мы ввели обозначение

$$z = \kappa_i \sqrt{Q_c^m / Q_c}. \quad (2.5)$$

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

$$|\Delta\Omega| \leq \Delta\omega_{\text{сих}}. \quad (2.6)$$

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

Для этого используются исследуемые лазеры и оптический 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 минимизации 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 перестраиваемого аттенюатора в волоконном тракте лазера-ведущего для изменения соотношения мощностей лазера-ведущего и лазера-ведомого.

2.4 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 передатчике
2. Лазер-ведомый, установленный в приемнике
3. Оптический анализатор спектра Yokogawa 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 измерение длин волн лазеров ведущего и ведомого без воздействия внешнего излучения. Результаты этих измерений отображены на рисунке 2.2 Измеренные длины волн лазеров - длина волны лазера-ведущего 1549.964 нм, длина волны лазера-ведомого без действия внешнего излучения -

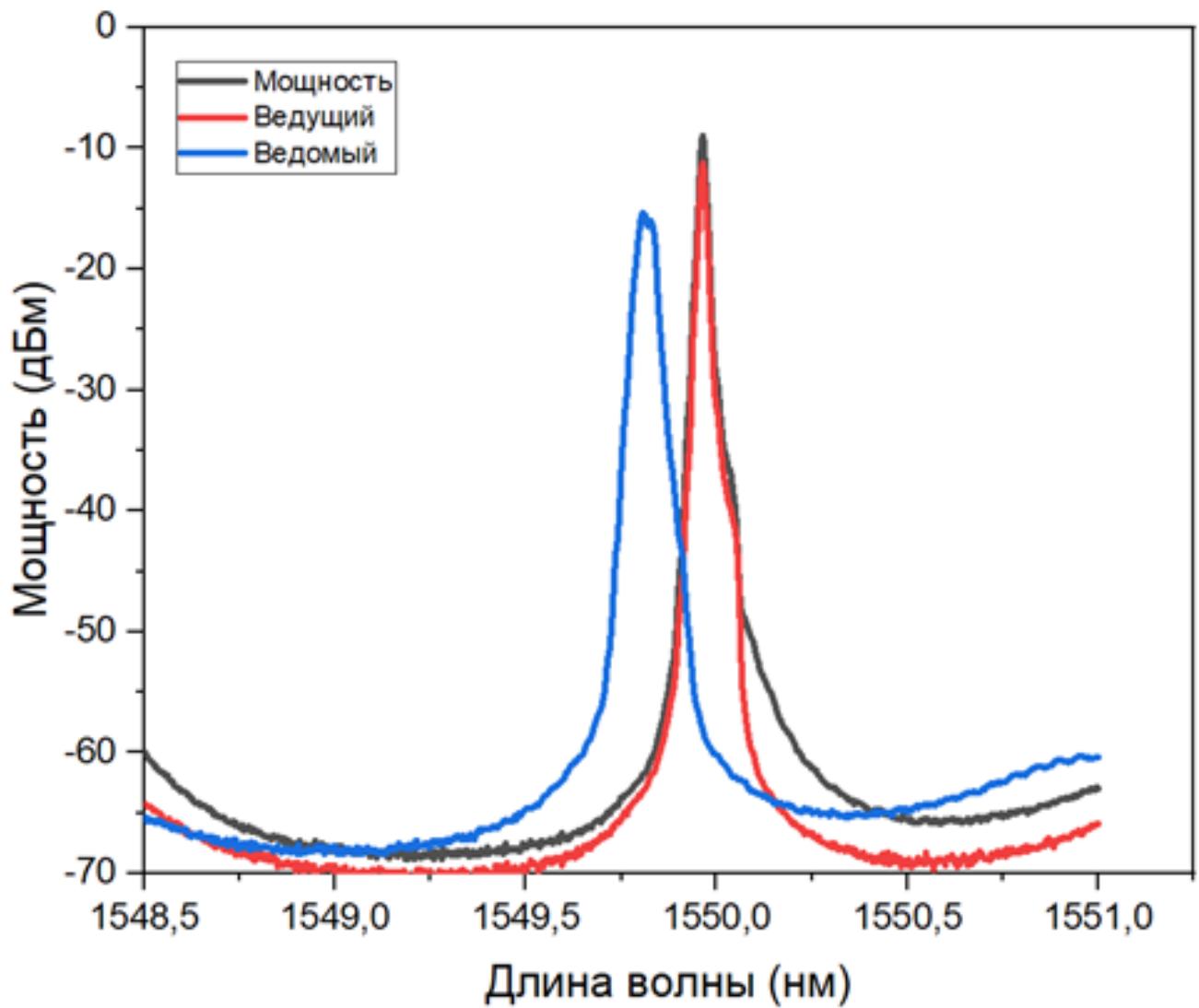


Рисунок 2.2 — *

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

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 корректировка только из-за прохождения квантовыми состояниями волоконно-оптической линии связи.

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

Излучение лазера может быть представлено следующим образом:

$$F(t) = A_0 * \sin(\omega_0 t + \varphi_0), \quad (2.7)$$

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

$$S(t) = (1 + m \sin(\Omega t + \varphi(t))), \quad (2.8)$$

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

Лазерное излучение после модуляции выглядит следующим образом:

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

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

$$\begin{aligned} F_d(t) = F(t)^2 * S(t)^2 &= (A_0 * \sin(\omega_0 t + \varphi_0))^2 * (1 + m * \sin(\Omega t + \varphi_0 + \varphi(t)))^2 = \\ &= \frac{1}{8} \left\{ 4A_0^2 + 2A_0^2 * m^2 - 4A_0^2 \cos(2\omega t + 2\varphi_0) - 2A_0^2 * m^2 \cos(2\omega t + 2\varphi_0) - \right. \\ &- 2A_0^2 * m^2 \cos(2\Omega t + 2\varphi(t)) + A_0^2 * m^2 \cos(2\omega t - 2\Omega t + 2\varphi_0 - 2\varphi(t)) + \\ &+ A_0^2 * m^2 \cos(2\omega t + 2\Omega t + 2\varphi_0 + 2\varphi(t)) + 8A_0^2 m \sin(\Omega t + 2\varphi(t)) - \\ &\left. + 4A_0^2 m \sin(2\omega t - \Omega t + 2\varphi_0 - \varphi(t)) - 4A_0^2 m \sin(2\omega t + \Omega t + 2\varphi_0 + \varphi(t)) \right\}, \end{aligned} \quad (2.10)$$

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

$$I = R(\lambda) GCF_d, \quad (2.11)$$

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.

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

Для системы квантового 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 [12; 105]. Эта особенность позволяет не применять частотную подстройку источников излучения и упростить конечную систему.

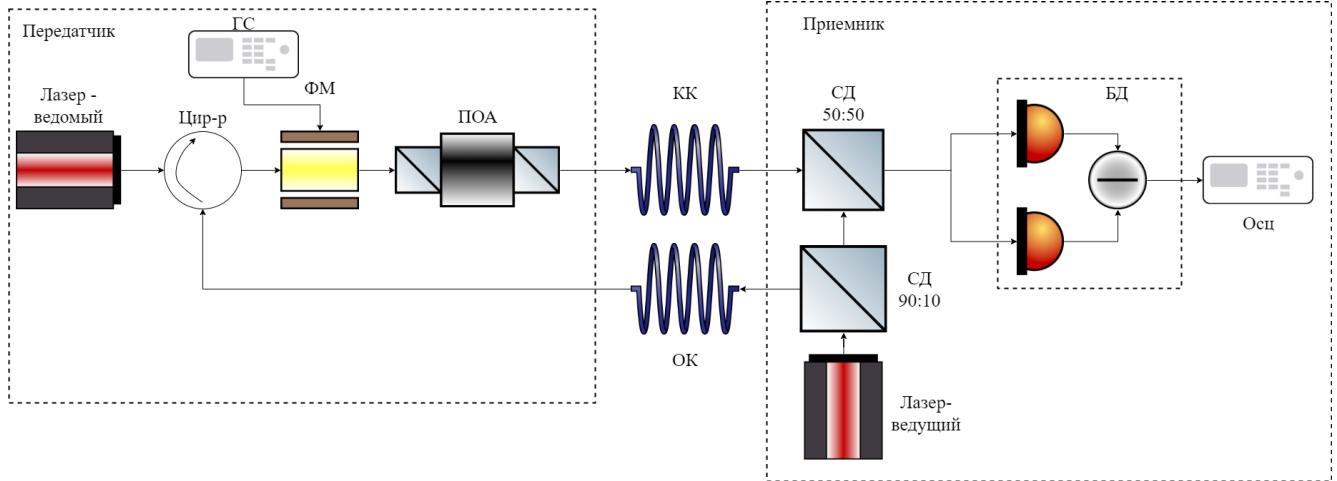


Рисунок 2.3 – Оптическая схема установки системы КРК на поднесущих гармониках с оптической инжекцией, где СД - светоделитель, ГС - генератор сигналов, ФМ - фазовый модулятор, ПОА - переменный оптический аттенюатор, КК - квантовый канал, ОК - открытый канал, Цир-р - циркулятор, БД - балансный детектор, Осц - осциллограф

2.7 Описание экспериментальной установки

Оптическая схема установки по экспериментальной передаче фазово-кодированных сигналов и применением гетеродинного метода детектирования и оптической инжекции на рисунке. Данная схема работает следующим 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 принятый сигнал попадает на симметричный светоделитель с 2 входами и 2 выходами с коэффициентом деления 50:50. На второй же вход этого делителя попадает излучение 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 благодаря выносу фазово-кодированных состояний на поднесущие гармоники, то их интерференция с ЛО и дает результат в виде промежуточной частоты, которая равна частоте модуляции, применённой в Алисе. Эта частота на выходе балансного детектора оцифровывается с помощью осциллографа и в дальнейшем обрабатывается.

2.8 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 сдвиг для передачи информации. Этот сигнал изображен на рисунке 2.4 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 появляется из-за прохождения канала и собственных шумов балансного детектора. Результат цифровой фильтрации сигнала с рисунка 2.4 отображается ниже. После применения к сигналу с рисунка 2.5 алгоритма Быстрого Преобразования Фурье для изучения спектрального состава. Результат изображен на рисунке ниже. На рисунке 2.6 изображен результат БПФ, применённого к сигналу после фильтрации. Единственная 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

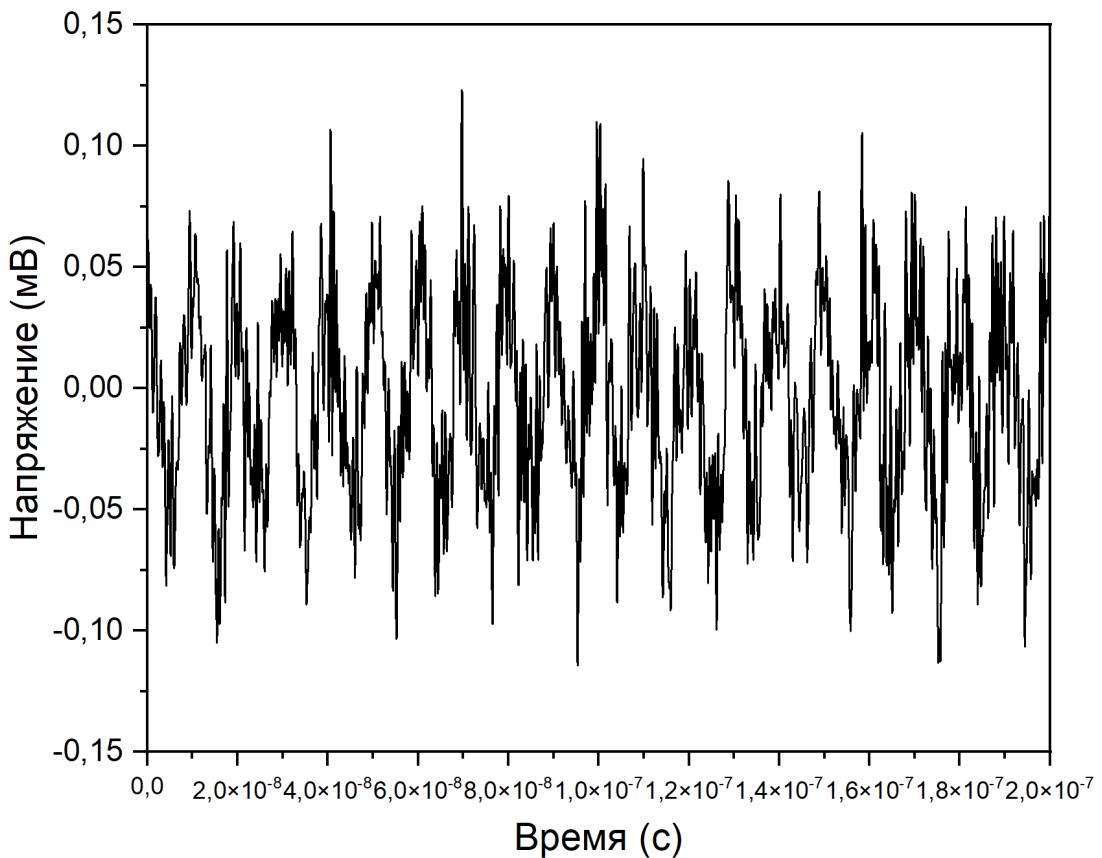


Рисунок 2.4 — Выходной зашумленный сигнал на выходе балансного детектора.

также возможно использование быстрого преобразования Фурье. Результат этого преобразования отображен на рисунке 2.7 В результате работы алгоритма по извлечению информации из принятого сигнала, на выходе формируется последовательность фазовых сдвигов, которым сопоставляется определенному значению бита. Такая последовательность будет являться сырым ключом. На рисунке 2.7 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.

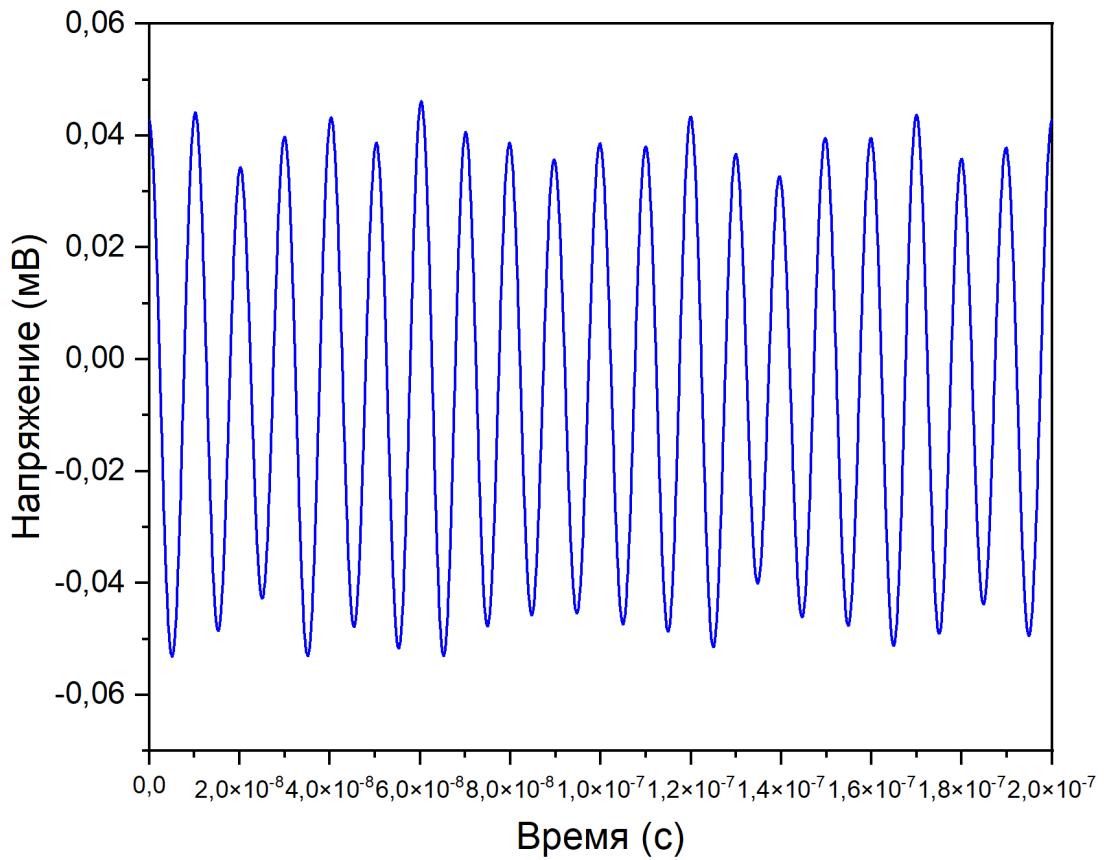


Рисунок 2.5 — Выходной сигнал балансного детектора после фильтрации.

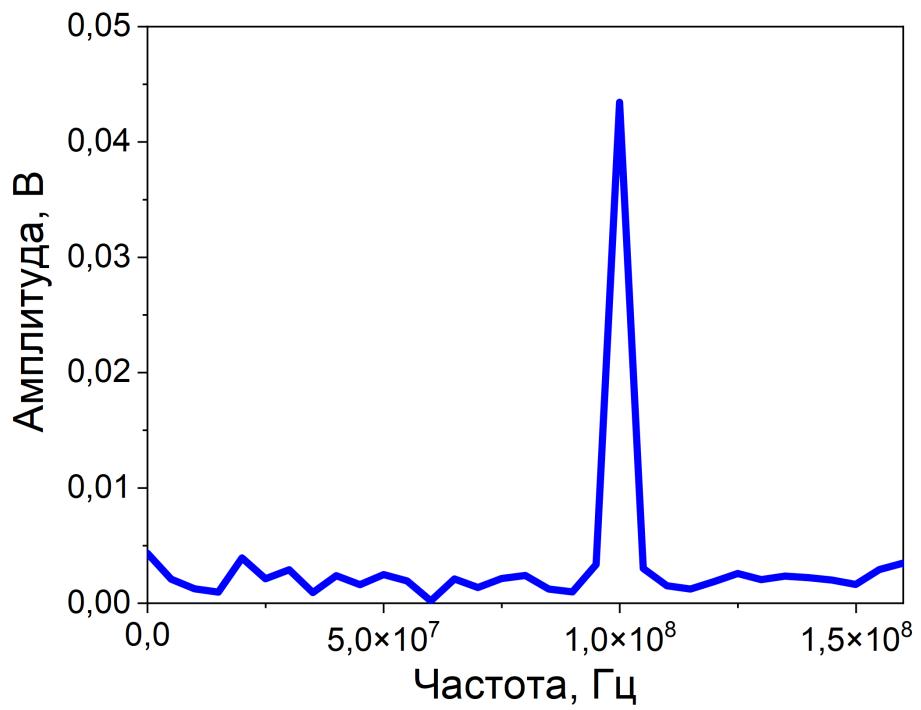


Рисунок 2.6 — Спектр полученного сигнала

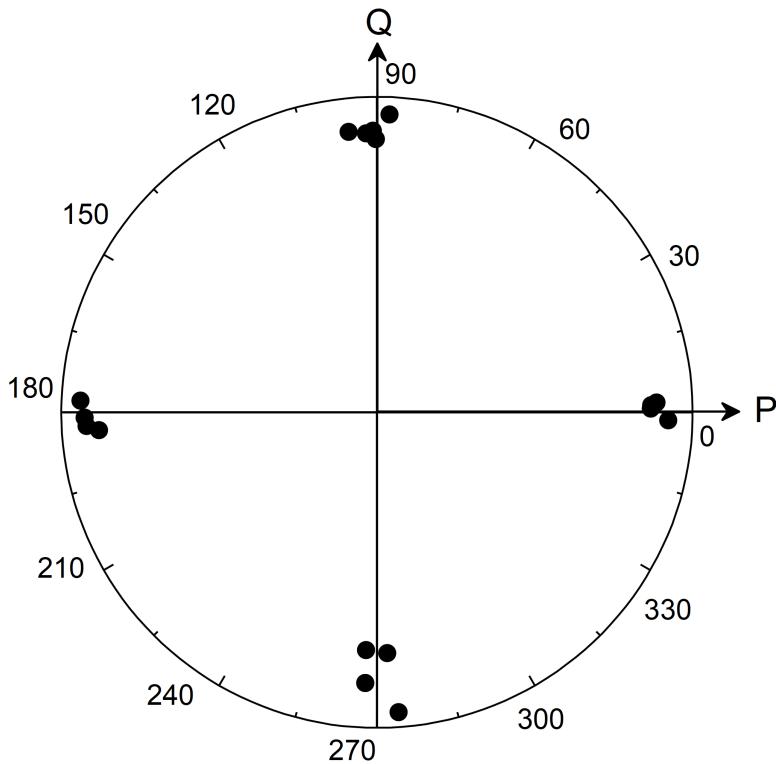


Рисунок 2.7 — Измеренные значения фазовых сдвигов в выходном сигнале балансного детектора

2.9 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, соответственно, бит информации. Данный метод требует наличия дополнительного оптического канала для создания обратной связи и более тщательного

исследования на уязвимость технической реализации для дальнейшего внедрения в реальные системы КРК.

ГЛАВА 3. Система квантового распределения ключа на боковых частотах 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 [9]. 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 [106]. Вторая причина ограничения мощности локального осциллятора - нелинейные эффекты, возникающие во время прохода мощного сигнала по волоконно-оптическому тракту, связанный с рассеянием Рэлея и прочими. Соответственно, передача мощного ЛО может перекрыть все преимущества его мощности дополнительными шумами. И самая главная проблема - это возможные атаки на ЛО от злоумышленника [19]. Итогом всех этих проблем стало использование "локального" локального осциллятора на стороне приемника, сгенерированного отдельным независимым лазером [97; 107–109].

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 боковых частотах и с частотным мультиплексированием на одной несущей частоте.

3.2 Протокол квантового распределения ключа на боковых частотах с гетеродинном методом детектирования сигналов

Протокол работает следующим образом:

1. Алиса готовит квантовые состояния, кодируя информацию в фазовый сдвиг 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 произвольной формы. Этот генератор подготавливает модулирующий сигнал. В нем содержатся фазовые сдвиги, которые соответствуют кодировке QPSK с фазами 45, 135, 215 и 305 градусов [110]. Этот сигнал модулирует оптическое излучение и на выходе получаются дополнительные гармоники сигнала в выходном спектре фазового модулятора. После этого сигнал попадает на волоконно-оптический

перестраиваемый аттенюатор для снижения уровня мощности на боковых частотах до однофotonного уровня [111]. 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 светоделиль 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 подстройке разностной частоты между ЛО и квантовыми состояниями. 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 отфильтровать 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 возможно измерение мгновенной фазы промежуточной частоты 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

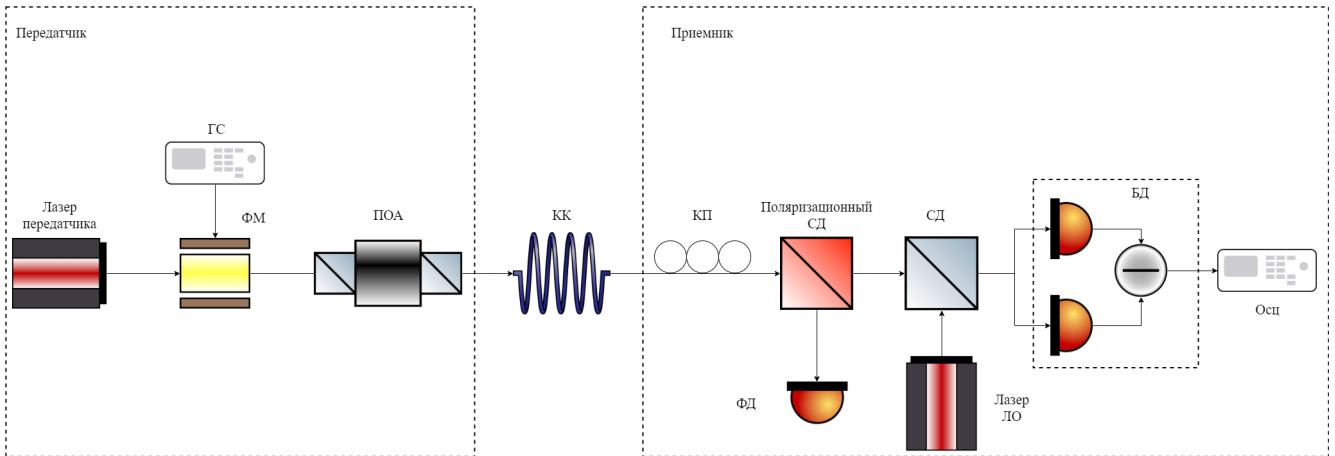


Рисунок 3.1 — Схема эксперимента по реализации гетеродинного метода приема сигналов для КРК, где ГС - генератор сигналов, ФМ - фазовый модулятор, ПОА - перестраиваемый оптический аттенюатор, КК - квантовый канал, КП - контроллер поляризации, СД - светофильтр, ФД - фотодиод, ЛО - локальный осциллятор,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

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

Излучение лазера может быть представлено следующим образом:

$$F(t) = A_0 * \sin(\omega_0 t + \varphi_0), \quad (3.1)$$

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

$$S(t) = (1 + m \sin(\Omega t + \varphi(t))), \quad (3.2)$$

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

Лазерное излучение после модуляции выглядит следующим образом:

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

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 $\frac{A_{sig}^2 * A_{het}^2 * m}{2} * \sin(\Omega t)$. 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 [112]. Как известно, сигналы в ортогональный поляризациях не взаимодействуют. Что существенно снижает эффективность передачи данных в системах КРК на непрерывных переменных. В рамках данного раздела предлагается реализация алгоритма подстройки поляризации пришедшего сигнала. При использовании связки поляризационного светофильтра и контроллера поляризации можно подстраивать поляризацию за счет анализа спектрального состава принятого сигнала с помощью быстрого преобразования Фурье. В случае неправильной поляризации, на выходе поляризационного светофильтра сигнал разделяется на две поляризации: линейную и циркулярную. В итоге получается так, что на балансном детекторе уровень сигнала будет зависеть от поляризации квантовых состояний. Для снижения QBER необходимо подстраивать поляризацию так, чтобы уровень сигнала был максимальным, что можно отслеживать по изменению двух частотных гармоник - промежуточной частоте между сигнальным лазером и между ЛО, а также по гармонике на частоте модуляции. С помощью Быстрого Преобразования Фурье возможно получать амплитуды этих гармоник и использовать эти амплитуды в качестве обратной

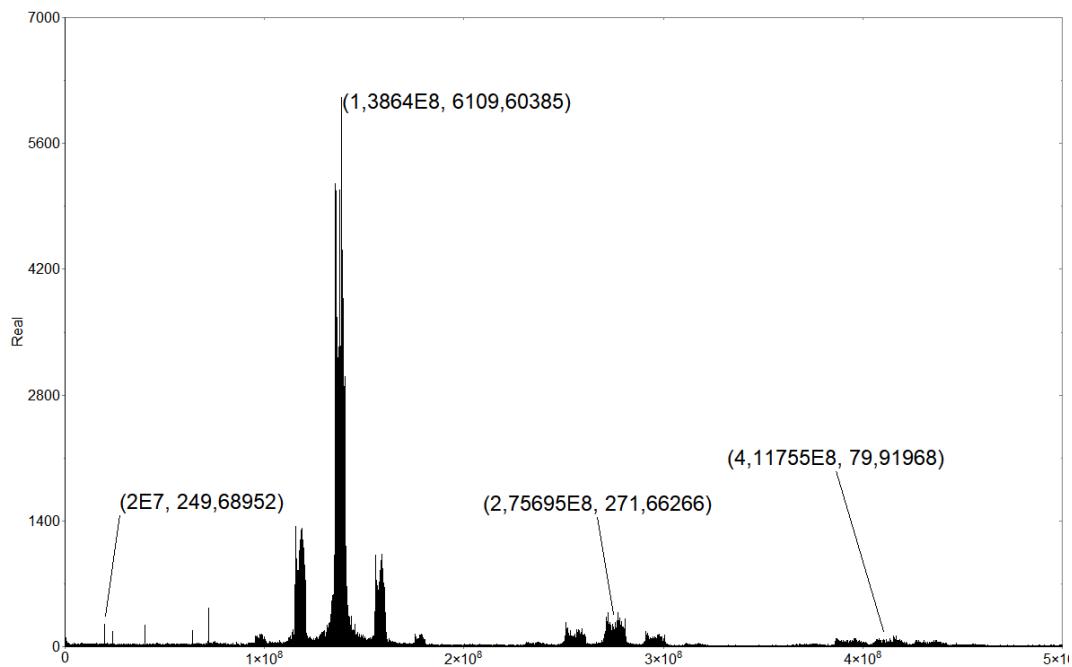


Рисунок 3.2 — Спектр выходного сигнала с неправильной поляризацией

связи для контроллера поляризации. На рисунке 3.2 изображен спектр сигнала с балансного детектора при неправильной поляризации. При этом во втором плече поляризационного светоделителя будет наблюдаться некоторый уровень сигнала, который будет сообщать о том, что поляризация отлична от линейной. Этот уровень мощности в идеале должен быть равен нулю и этот же сигнал возможно использовать в качестве дополнительного контроля качества подстройки поляризации. В спектре этого сигнала наблюдается гармоники на частоте 20 МГц, что соответствует частоте модулирующего излучения. На основе этой информации система обратной связи должна дать команду на контроллер поляризации для ее контроля. В результате действий КП должен привести сигнал к виду, отображенном 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 максимума гармоники на частоте модуляции

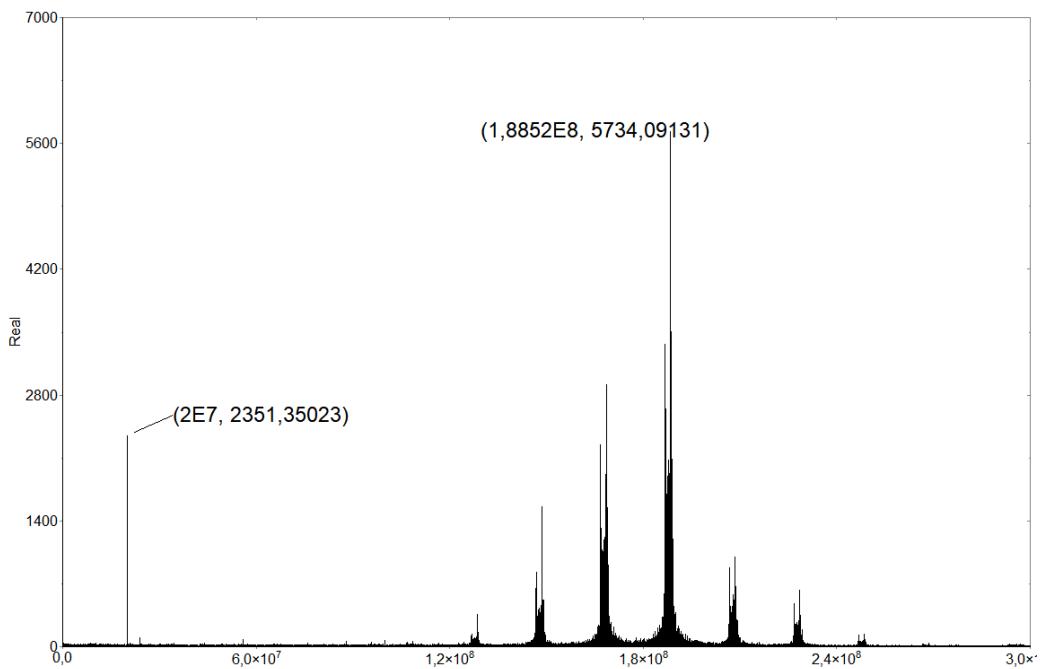


Рисунок 3.3 — Спектр выходного сигнала с балансного детектора с правильной поляризацией

4. Получение минимума сигнала на фотоприемнике, установленном во втором плече поляризационного светоделителя

3.6 Описание экспериментальной установки

Для реализации системы квантового распределения ключей на боковых частотах 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 EO Space с полосой пропускания 40 ГГц и вносимыми потерями 4 дБ. В качестве балансного детектора использовался детектор фирмы General Photonics BDP-003 с чувстви-

тельностью 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 частотой дискретизации 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 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 рассказано в разделе [?]. 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.

3.7 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 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

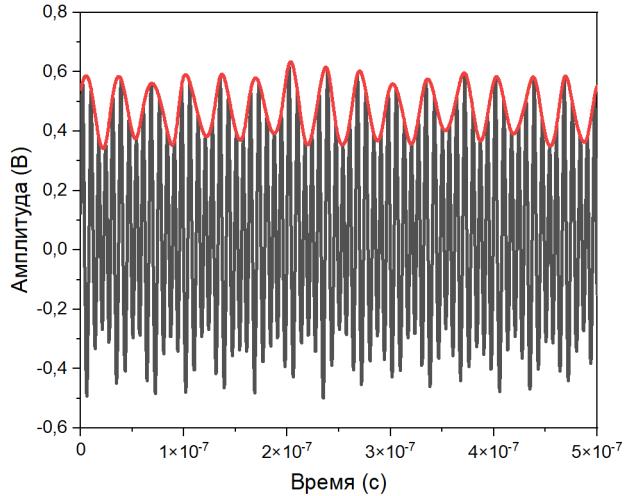


Рисунок 3.4 — Выходной сигнал с балансного детектора во временной области

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 3.5.

3.8 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. Дан-

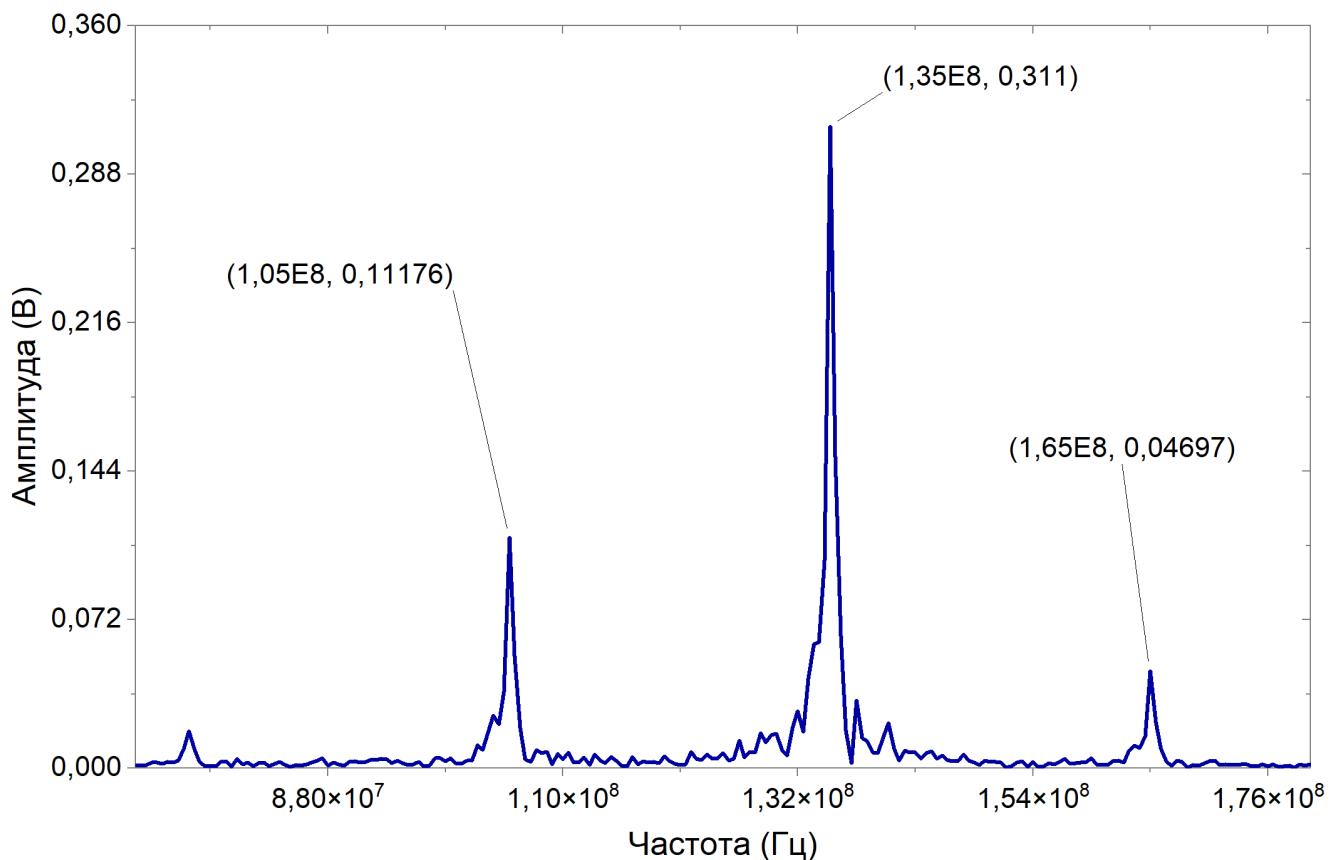


Рисунок 3.5 — Спектр сигнала на выходе балансного детектора после гетеродинного детектирования с применением двумя независимых источников излучения.

ный подход позволяет распределять сырую последовательность бит в системе КРКБЧ-НП с гетеродинным методом детектирования. Благодаря которому информация об измеренных квантовых состояниях переносится 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 амплитудно-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 когерентного излучения

Использование технологии квантового распределения ключей дает 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 безопасность за счет фундаментальных законов квантовой физики [1; 113]. 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 [114–117]. 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 засеванием. 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 [16; 118]. При этом воздействие возможно даже изменение длины волны. Эти эффекты могут быть использованы Евой для получения информации о ключе. Данная атака

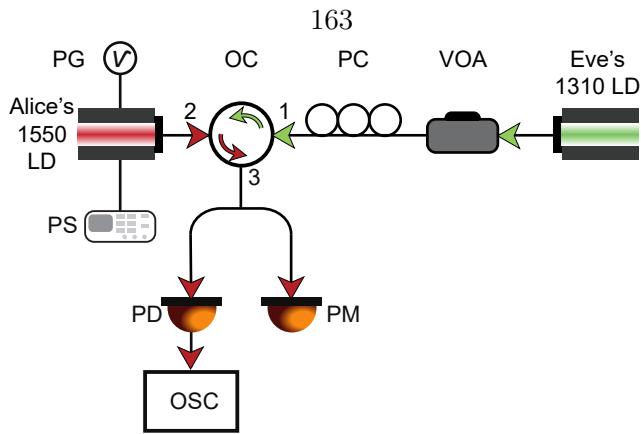


Рисунок 4.1 — Экспериментальная установка по проведению атаки оптической накачкой на источник когерентного излучения из состава системы квантового распределения ключей. Alice's LD - лазерный диод Алисы, PG - генератор импульсов, PS - источник напряжения, ОС - оптический циркулятор, PC - контроллер поляризации,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

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

Однако существующие уязвимости в пассивных оптических компонентах [34–36], используемых для защиты от других типов атак, позволяют Еве использовать другие длины волн для проведения своих манипуляций по изменению характеристик излучения [17]. Для этих целей может быть использовано излучение на длине волны 1310 нм. Данная глава посвящена проведению атаки оптической накачкой [39; 40; 119; 120] на полупроводниковый лазер с распределенной обратной связью, работающим в режиме переключения усиления [38]. Измерялись параметры выходного излучения, его мощность, ватт-амперная характеристика. Изучается влияние 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, Agilent WSL5-934010C4124-82) 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 повторяемости 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. Распространяясь 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 населеностей 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

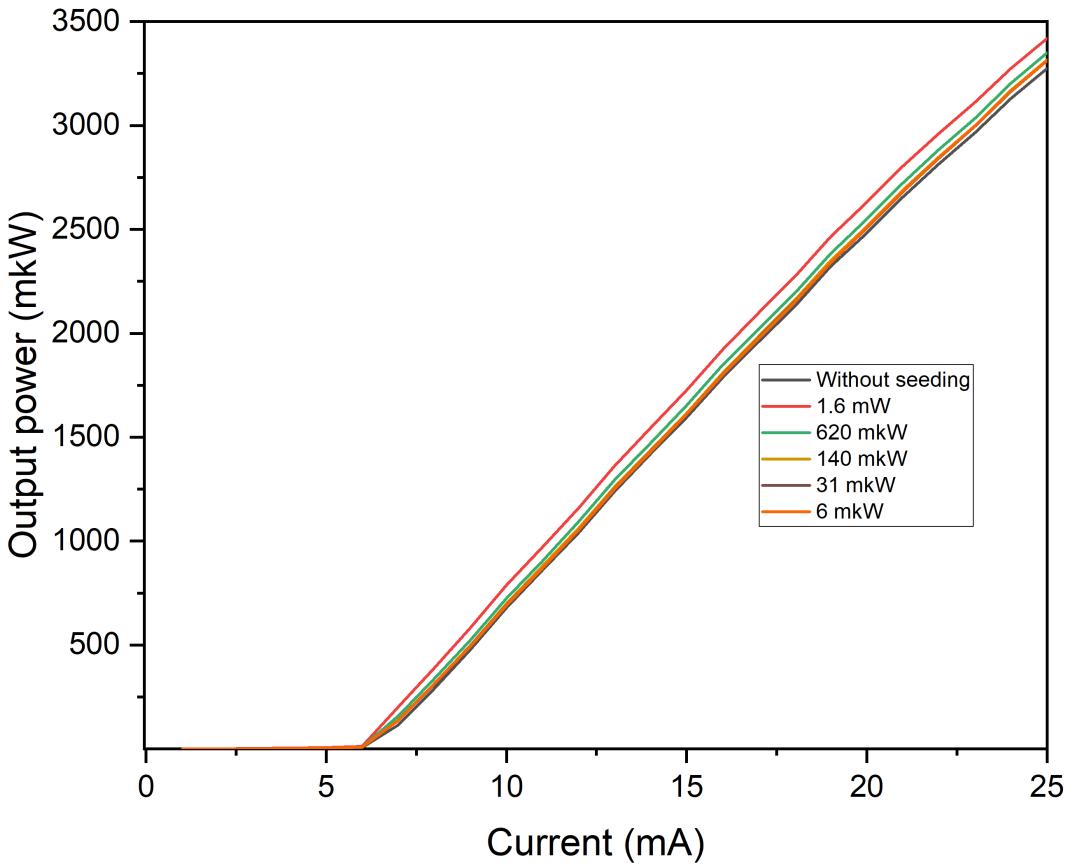


Рисунок 4.2 — Ватт-Амперные характеристики лазера Алисы под действием внешней оптической накачки от Евы.

режиме только с накачкой током от лабораторного 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 эффективности [121; 122]. Эта величина показывает эффективность преобразования электронного тока в фотоны, излучаемые лазером. Формула расчета величины дифференциальной квантовой эффективности ниже

$$\eta = \frac{2e}{\hbar\omega} \frac{dP}{dI} \quad (4.1)$$

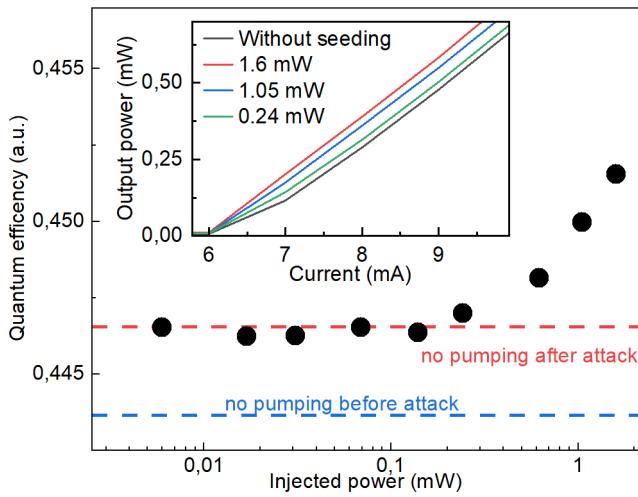


Рисунок 4.3 — График зависимости дифференциальной квантовой эффективности в зависимости от мощности накачки Евы. Красная пунктирная линия обозначает значение дифференциальной квантовой эффективности после проведенной атаки, а синяя пунктирная линия обозначает значение дифференциальной квантовой эффективности 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 эффективность лазера Алисы, что приводит к увеличению выходной мощности лазера при неизменном токе накачки. В результате аппроксимации наклона ватт-амперных характеристик и расчета дифференциальной квантовой эффективности (ДКЭ) по формуле 4.1 было показано, что Ева может увеличивать ДКЭ на несколько процентов. Это изменение приводит к тому, что повышается среднее число фотонов, излучаемое Алисой. В результате необходима переоценка скорости выработки секретного ключа из-за увеличения среднего числа фотонов, но этого не происходит, что позволяет Еве перехватывать разницу в ключах и использовать его в своих целях.

4.3 Изменение формы импульса при атаке на лазер с распределенной обратной связью, работающим 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 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 ГГц, скорость оцифровки 40 ГС/с. 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 МГц и длительность импульса составляла 700 пс. 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 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 уменьшиться при некоторых 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 измерите-

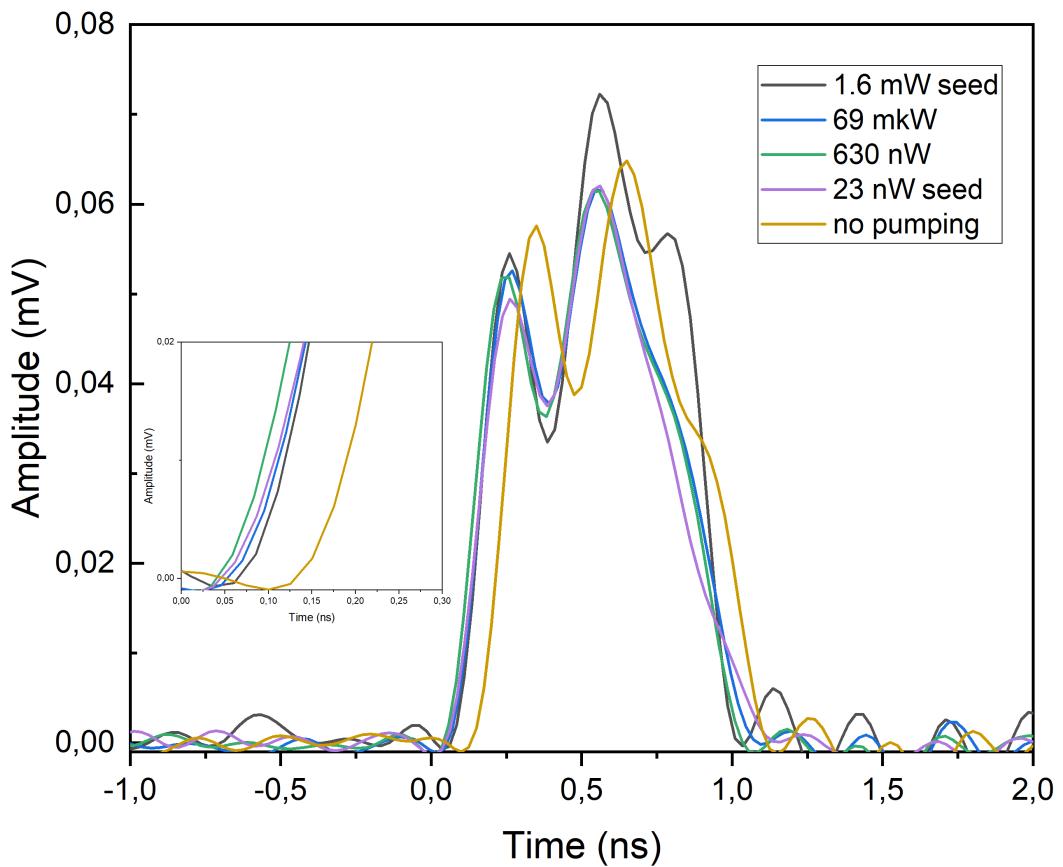


Рисунок 4.4 — Формы импульсов, сгенерированных Алисой, под действием оптической накачки и без нее.

ля 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.

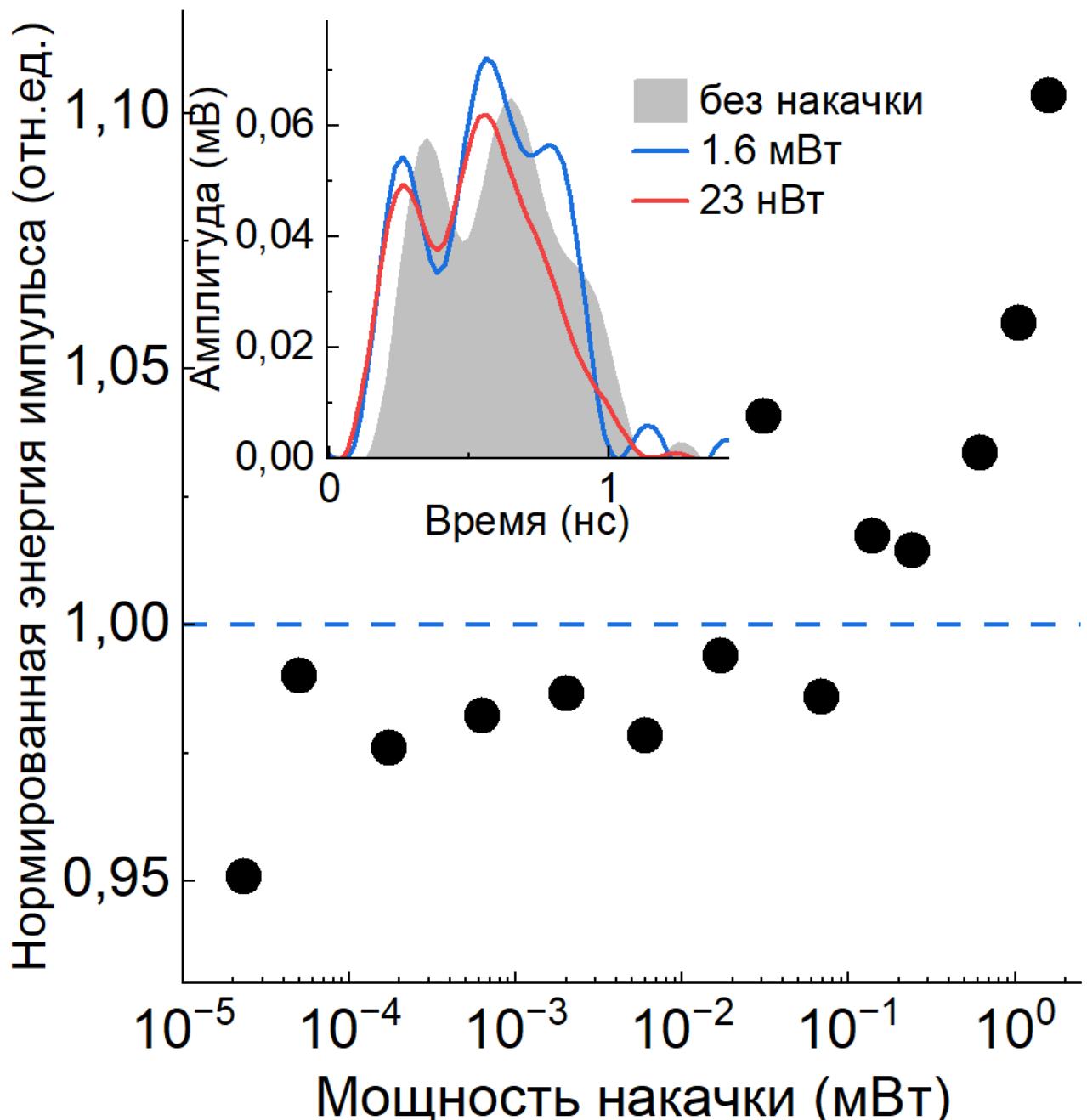


Рисунок 4.5 — Изменение энергии импульсов под действием накачки лазером на длине волны 1310 нм Евы.

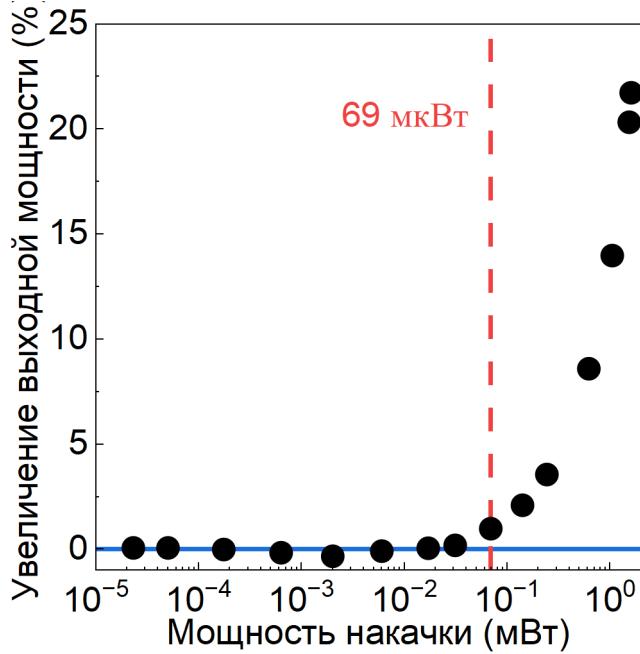


Рисунок 4.6 — Изменение средней мощности лазера Алисы под действием оптической накачки Евы.

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

В качестве исходной мощности, которая необходима для создания заметного эффекта, определенная по графику 4.6, составляет 69 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 [123]. Для определения изоляции необходимо вычесть из мощности лазера минимально необходимую мощность для создания эффекта по формуле 4.2.

$$\alpha_{iso} = P_{laser} - P_{req} \quad (4.2)$$

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

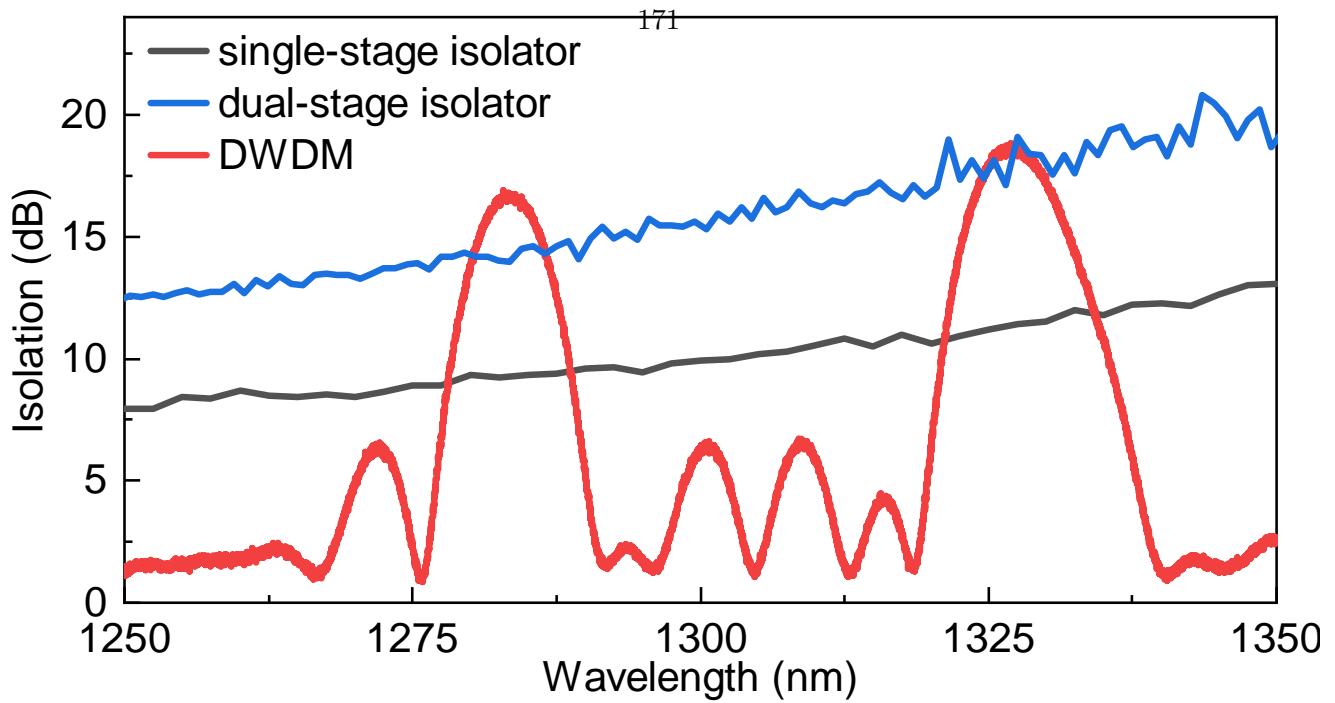


Рисунок 4.7 — Величина изоляции пассивных элементов, используемых в системах КРК. Красным цветом обозначен спектр изоляции DWDM фильтра, серым - одностадийного изолятара, синим - двухстадийного изолятара

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 позволяют 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 примеру, изоляция одностадийного изолятара на длине волны 1550 нм составляет 30 дБ, а

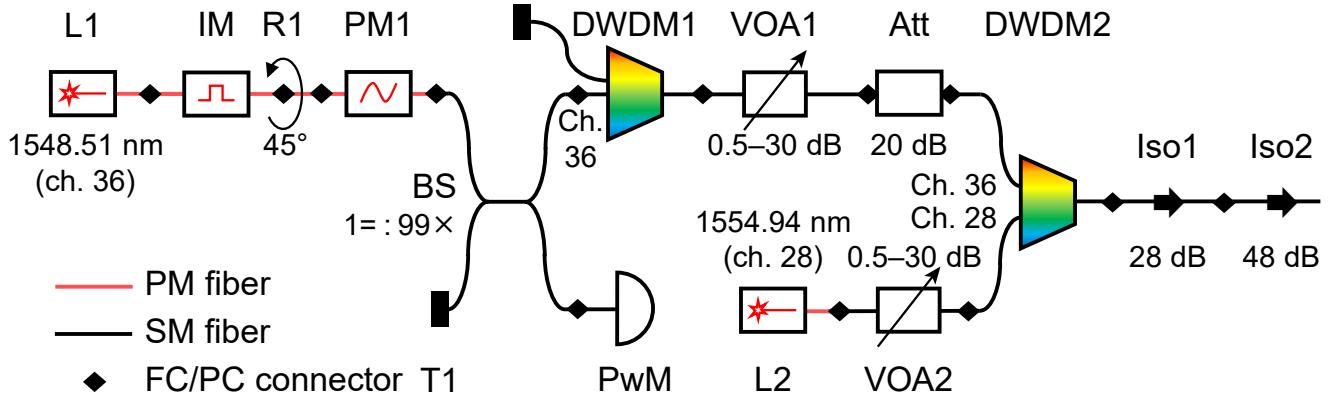


Рисунок 4.8 — Оптическая схема блока Алиса

Таблица 1 — Потери элементов в системе квантового распределения ключей на длине волны 1310 нм

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

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 [124]. Таким образом видно, что пассивные элементы не вносят заявленной изоляции и эта лазейка может быть использована злоумышленником. В качестве схемы КРК будет использоваться схема из работы [117]. Для расчета необходимой минимальной зондирующей мощности необходимо просуммировать все потери, вносимые элементами на длине волны 1310 нм. Измеренные значения потерь элементов продемонстрированы в таблице 1

Вычисления производятся по формуле

$$\alpha_{1310} = \alpha_{Iso1} + \alpha_{Iso2} + \alpha_{Att} + \alpha_{VOA1} + 2\alpha_{DWDM} + \alpha_{PM} + \alpha_{IM} + \alpha_{LD}, \quad (4.3)$$

где α_{Iso} вносимые потери изолятором на длине волны 1310 нанометров, α_{att} , α_{VOA} , α_{DWDM} , α_{PM} , α_{IM} , и α_{LD} вносимые потери компонентов 4.8. Для определения потерь использовались схожие компоненты как в работе [117]. Раскрывать модели всех элементов не представляется возможным по соображениям конфиденциальности. Но эти элементы представляют собой стандартные телекоммуникационные элементы доступные для заказа. Потери на длине волны 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 [117]. Потери на изоляторе, встроенным в лазерный диод, считаем аналогичными одностадийному изолятору в 10 дБ. В итоге изоляция всей системы, изображенной 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 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 69 мкВт. Определена минимально необходимая изоляция для предотвращения атаки оптической накачкой на длине волны 1310 нм и зондирующей мощности 14 Вт в 53 дБ. Определена стойкость существующей системы квантового распределения ключей к атаке оптической накачкой. Ее суммарная изоляция составила 97.55 дБ, что превышает минимальное пороговое 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 злоумышленника 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 [117; 125]. 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 [126]. Однако, поскольку полупроводниковые лазеры очень чувствительны ко внешним воздействиям, существует несколько атак с лазерным засевом, которые открывают лазейки для подслушивающих [16; 17; 118]. Например, предыдущие экспериментальные исследования показали, что мощности инжекции в диапазоне 100 - 160 нВт может быть достаточно для управления интенсивностью импульсов Алисы [16; 118], а мощности даже около 1 нВт может быть достаточно для частичного управления фазой импульсов Алисы [17].

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 с недоверенным приемным узлом (НПУ КРК) [127; 128].

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 [41]. 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 [45].

К сожалению, конфигурация источника с оптической фазовой синхронизацией ранее не тестировалась на устойчивость к атакам с засевом лазерным излучением. В этой работе 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 оптической фазовой синхронизацией является эффективной контрмерой против известных атак на источник фотонов КРК. Между тем, это исследование демонстрирует и другие эффекты, которые могут иметь место

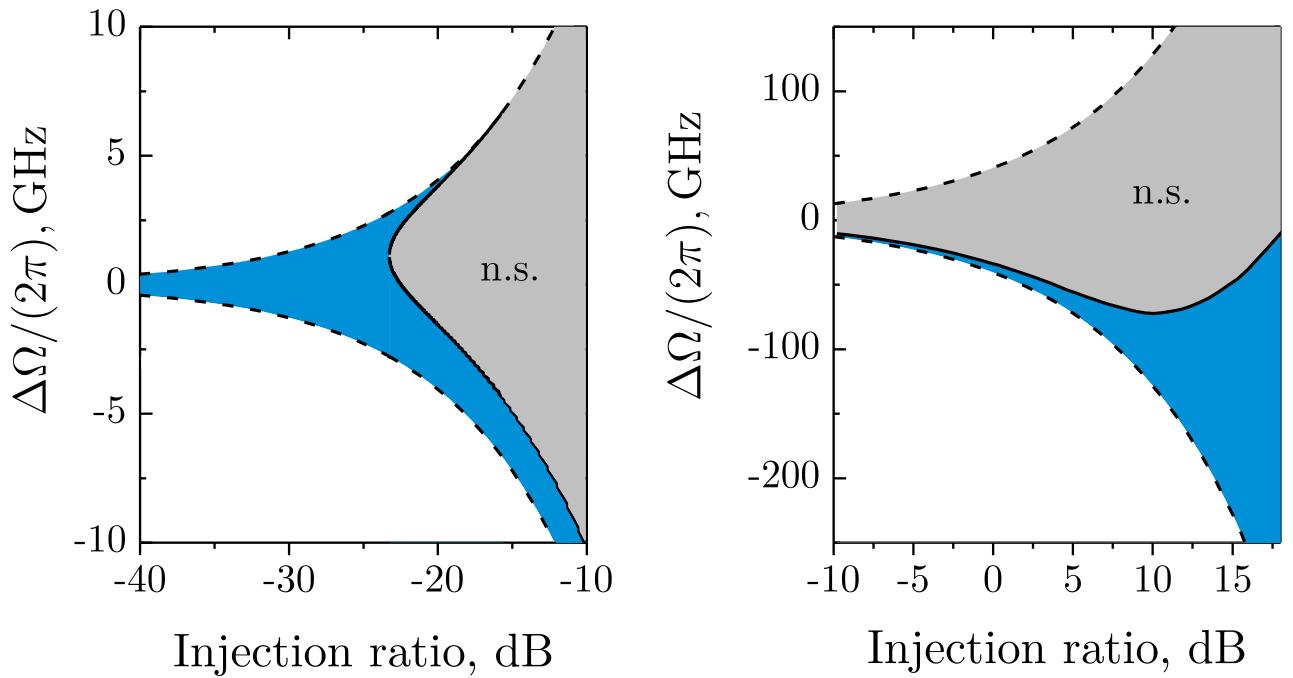


Рисунок 5.1 — Карта фазовой синхронизации двух лазеров(область стабильной синхронизации обозначена синим цветом).

только в исследуемой конфигурации источника. 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

Таблица 2 — 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}	$5.0 \times 10^{10} \text{ ns}^{-1}$
I	22 mA	γ_Q	0

"ведущий-лазер, который обеспечивает внешнее излучение для воздействия на "ведомый-лазер [24].

В зависимости от интенсивностей и спектральных показателей ведущего и ведомого ЛД, источник может обеспечивать режим свободной генерации, стабильной или нестабильной синхронизации [129]. 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

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

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

$$Q = \frac{\langle P \rangle}{f_R \times \tau_P}, \quad (5.2)$$

где $\langle P \rangle$ - 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 [130]. Между тем, в реальных 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 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 [131; 132]. 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-

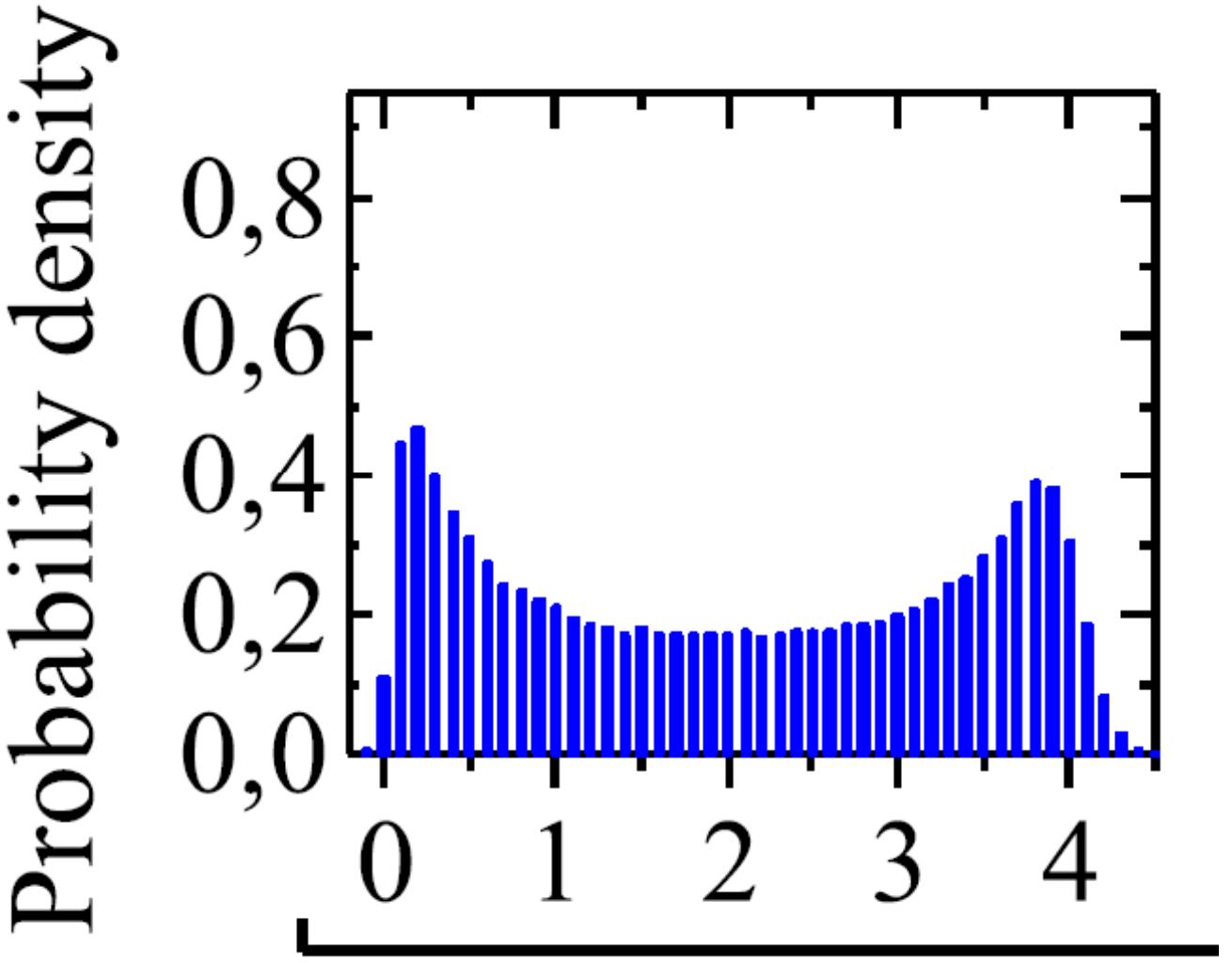


Рисунок 5.2 — Нормализованная функция плотности распределения интерференции колоколообразных импульсов без чирпа [132].

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

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

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 рисунке 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 были использованы пару идентичных волоконно-оптических DFB лазерных диодов с выходным волокном, сохраняющим поляризацию (Agilecom, WSL-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

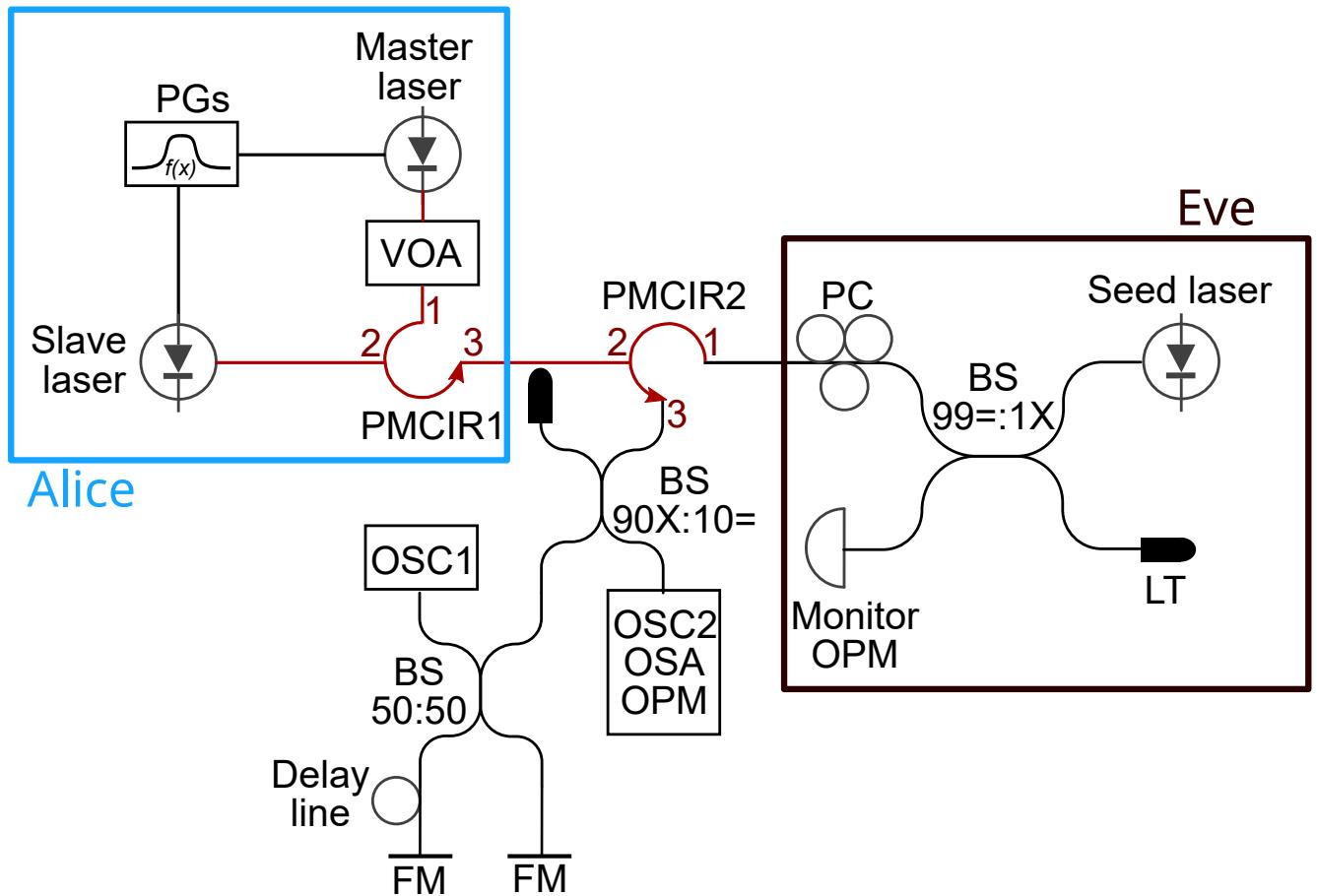


Рисунок 5.3 — Экспериментальная установка (PM-волокна выделены красным цветом): VOA - перестраиваемый оптический аттенюатор, BS - светоделитель, PMCIR - циркулятор с сохранением поляризации, PMBS - светоделитель с сохранением поляризации, PG - генератор импульсов, OPM - измеритель оптической мощности, OSC - осциллограф, OSA - оптический анализатор спектра, BS - светоделитель, LT - световая ловушка, FM - зеркало Фарадея. Коэффициент связи светоделителя (BS) обозначается $99 =: 1\times$ означает, что 99% света проходит в порт, горизонтально противоположный графическому обозначению СД, в то время как 1% света 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 5.4 и 5.5 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.

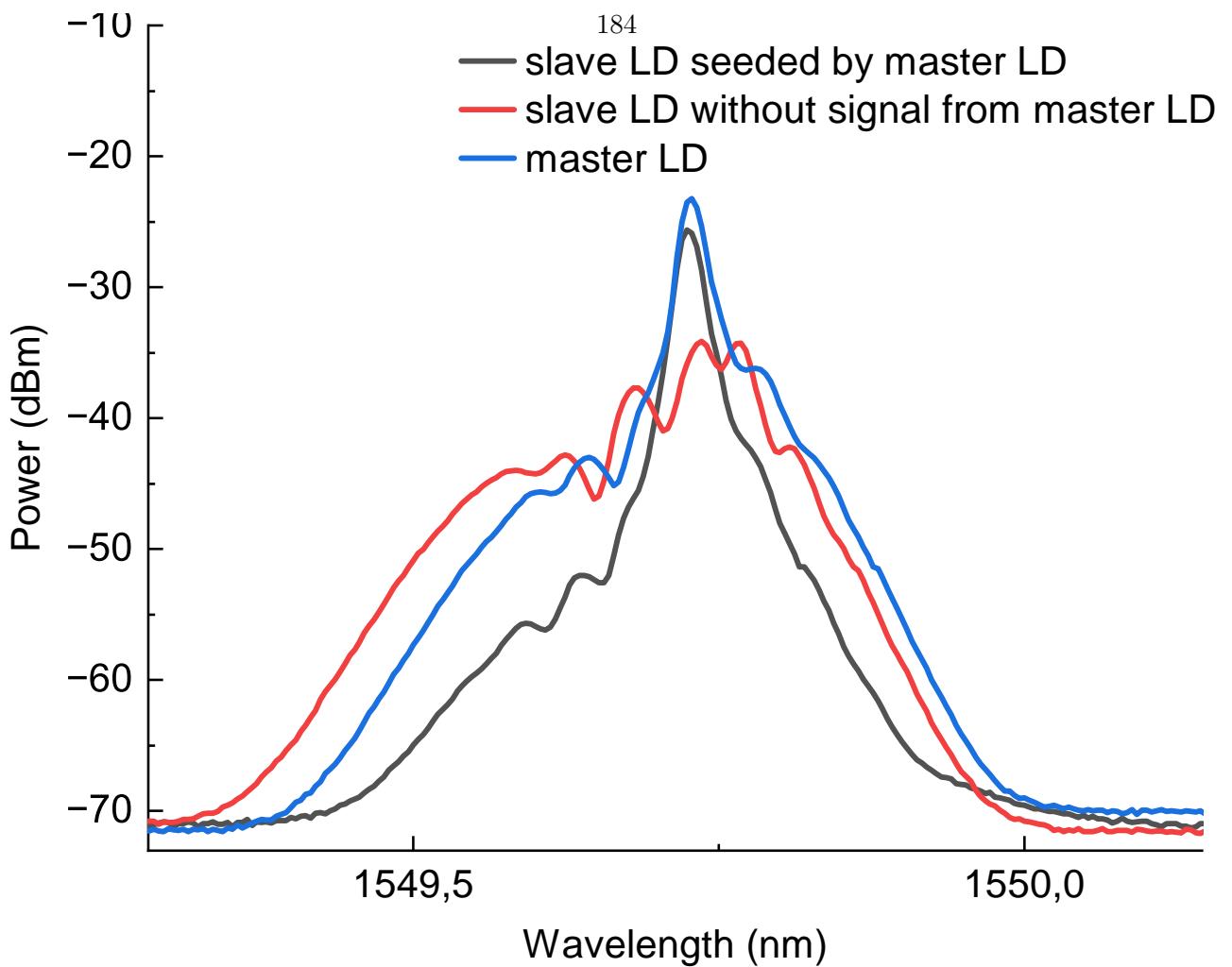


Рисунок 5.4 — Спектры лазерных диодов ведущего, ведомого и источника излучения для КРК

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-

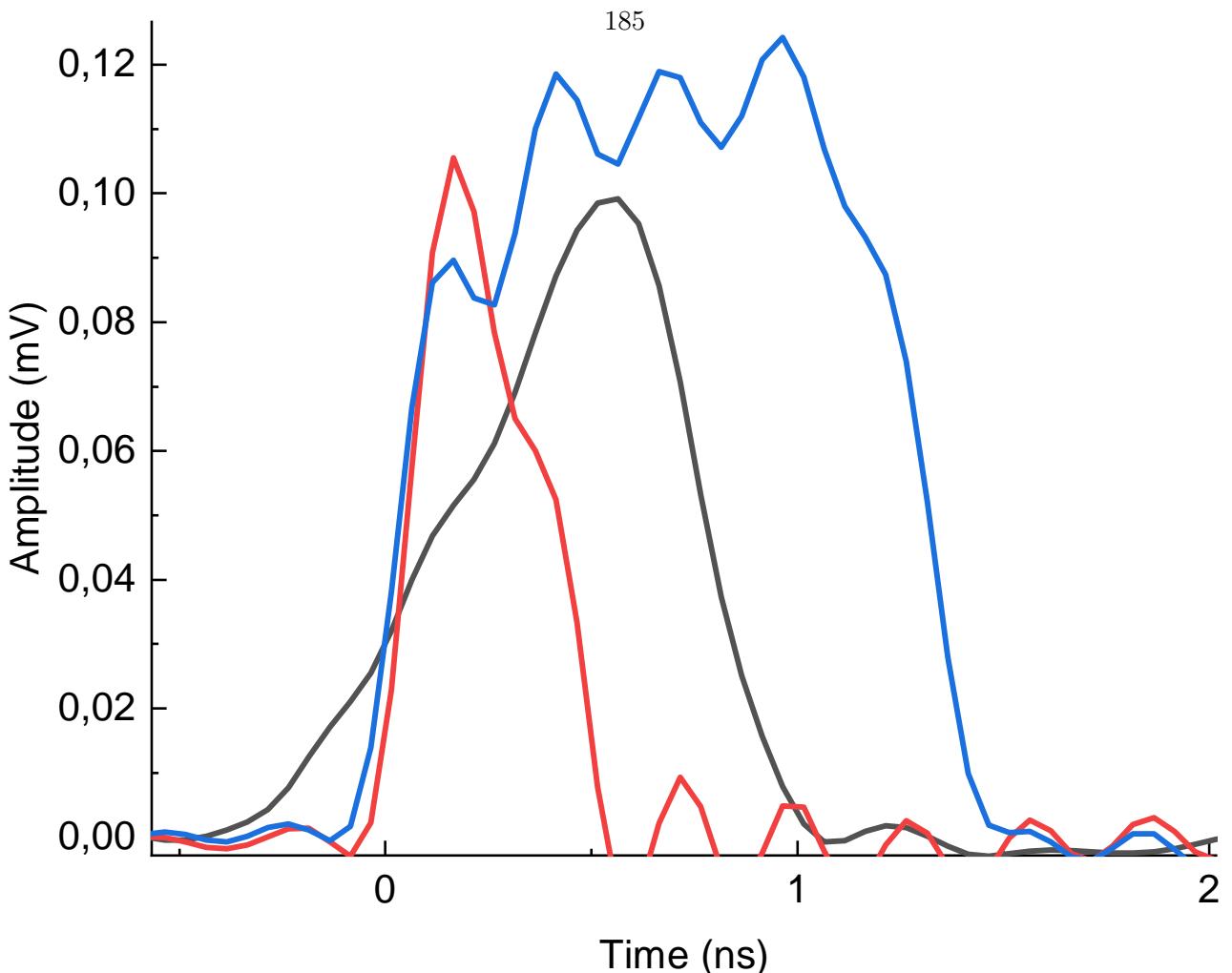


Рисунок 5.5 — Формы импульсов лазеров мастера, слейва и источника излучения КРК

бием волокна (EDFA, заказной блок QGLex) [133]. 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 зондирующая мощность атакующего лазера уменьшается из-за этих потерь и 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

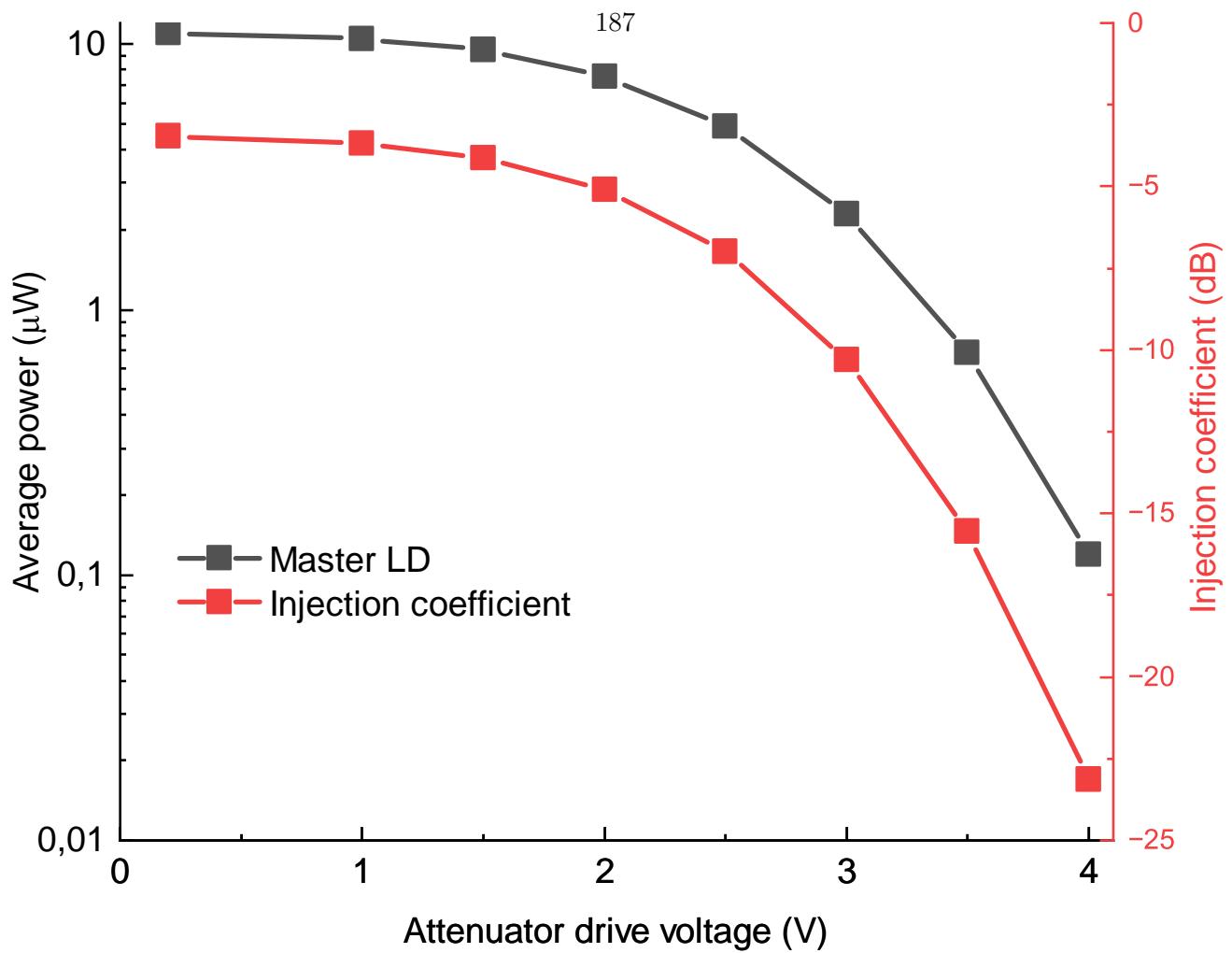


Рисунок 5.6 — Зависимость мощности ведущего лазера (черный) и коэффициента инжекции(красный) от напряжения на аттенюаторе.

зависимости всех характеристик источника лазерного излучения для КРК от средней мощности ведущего ЛД. И, наконец, мы исследовали выходные спектры КРК под воздействием внешнего излучения с различной рабочей длиной волны.

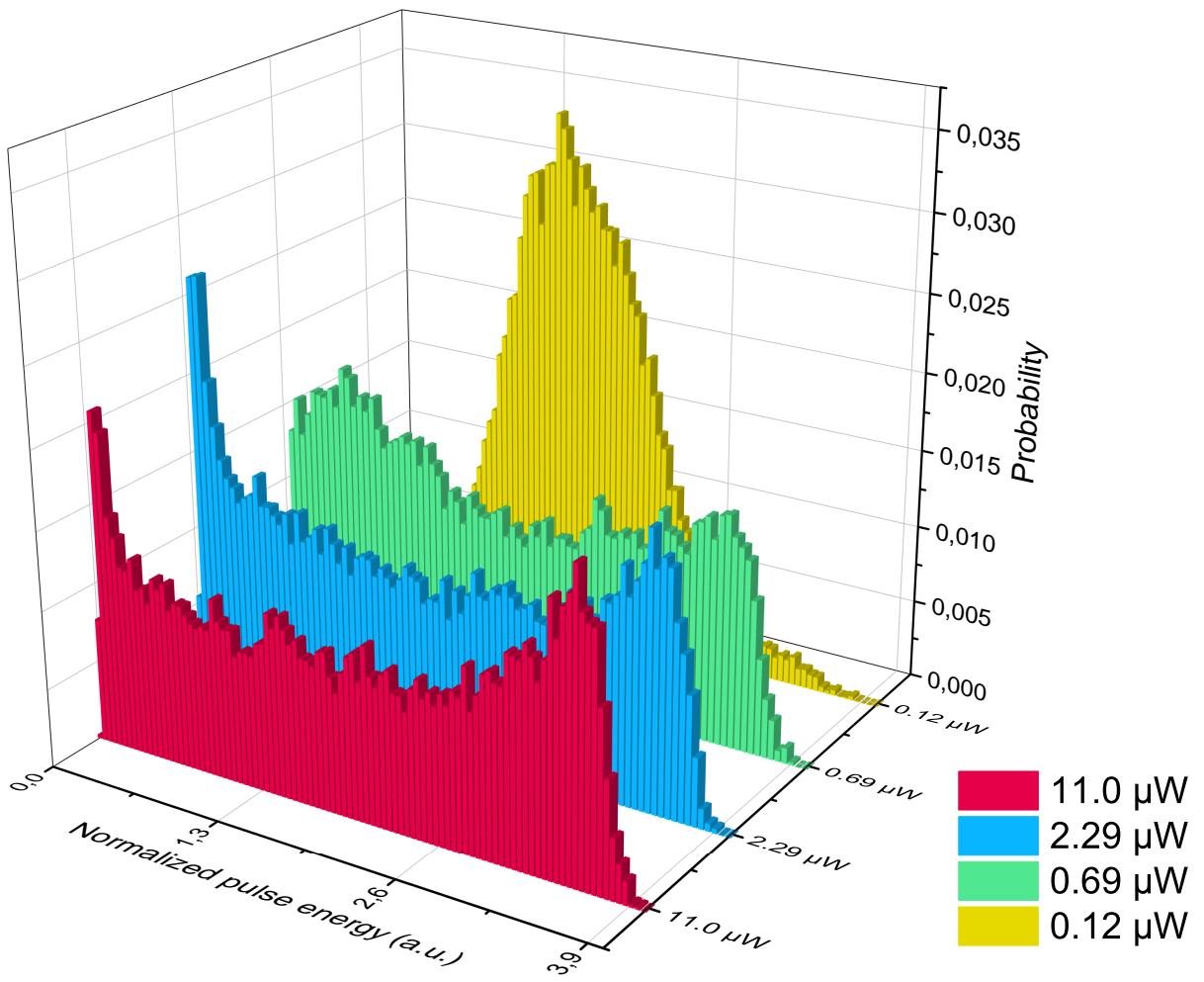


Рисунок 5.7 — Функции плотности вероятности интерференции импульсов источника КРК под действием различной мощности лазера-ведущего

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 5.1 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).

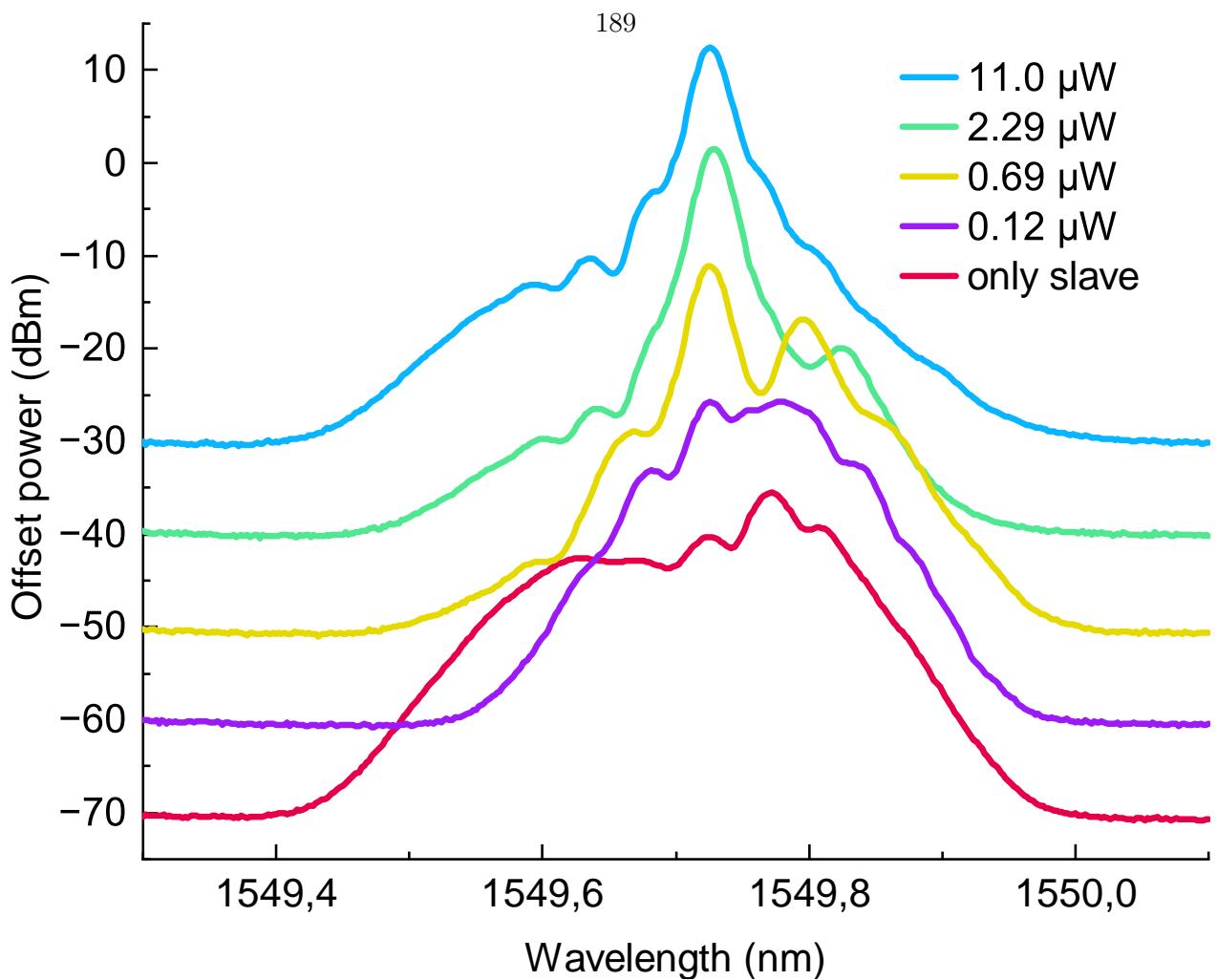


Рисунок 5.8 — Спектры излучения лазера-ведомого под действием переменных мощностей лазера-ведущего

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 5.6. ФПВ, измеренные для различных мощностей ведущего ЛД на рисунке 5.7, показывают, что синхронизация происходит, когда мощность ведущего ЛД находится в диапазоне от 2.29 до 11 мкВт. Форма ФПВ имеет два пика, соответствующих идеальной конструктивной и деструктивной интерференции. При мощности основного ЛД 0.69 мкВт видность интерференции ухудшается. И, наконец, при минимальной мощности ведущего 0.12 мкВт, ФПВ имеет только один высокий пик в центре. Это означает, что ведомый не имеет оптической синхронизации с ведущим. Без

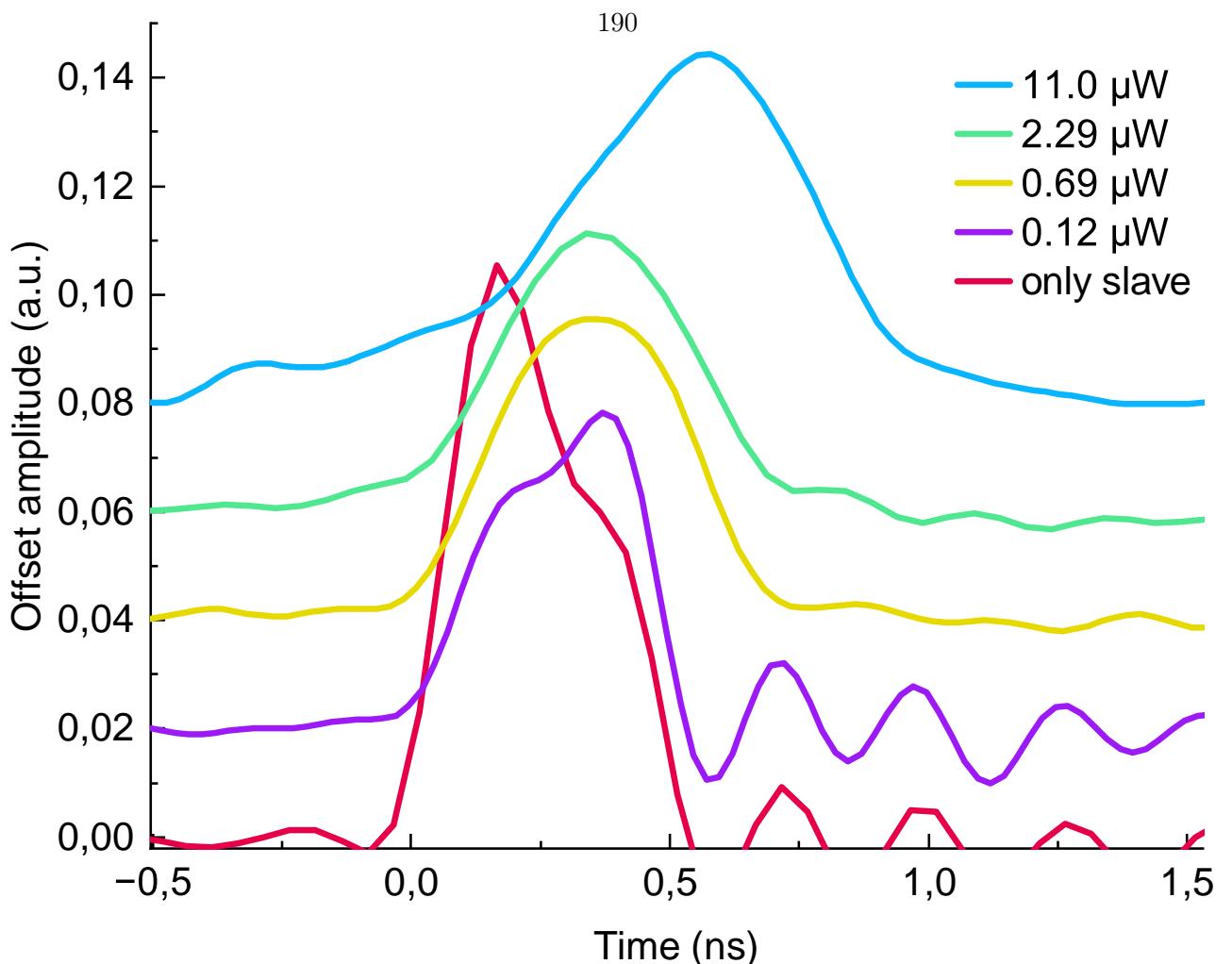


Рисунок 5.9 — Формы импульсов лазера-ведомого под действием различных мощностей лазера-ведущего

синхронизации временной джиттер импульсов увеличивается, что приводит к увеличению вероятности отсутствия помех.

Из спектров на рисунке 5.8 и измерений огибающей импульсов на рисунке 5.9 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 “границном” состоянии при мощности ведущего излучения 0.69 мкВт релаксационные 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, в то время как варьируется мощность ведущего лазера. На рисунке 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 общую среднюю мощность, а затем вычитаем отраженную мощность Евы, измеренную при выключенном источнике КРК. Было обнаружено 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 %, 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 измерялась средняя амплитуда и длительность импульса, а также их стандартное отклонение, рассчитанное на основе выборки размером 30 тысяч. Рисунок 5.13 показывает измеренные амплитуду и длительность, а также рассчитанную нормализованную энергию импульса с атакой и без нее. Из рисунков 5.11 и 5.12 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,

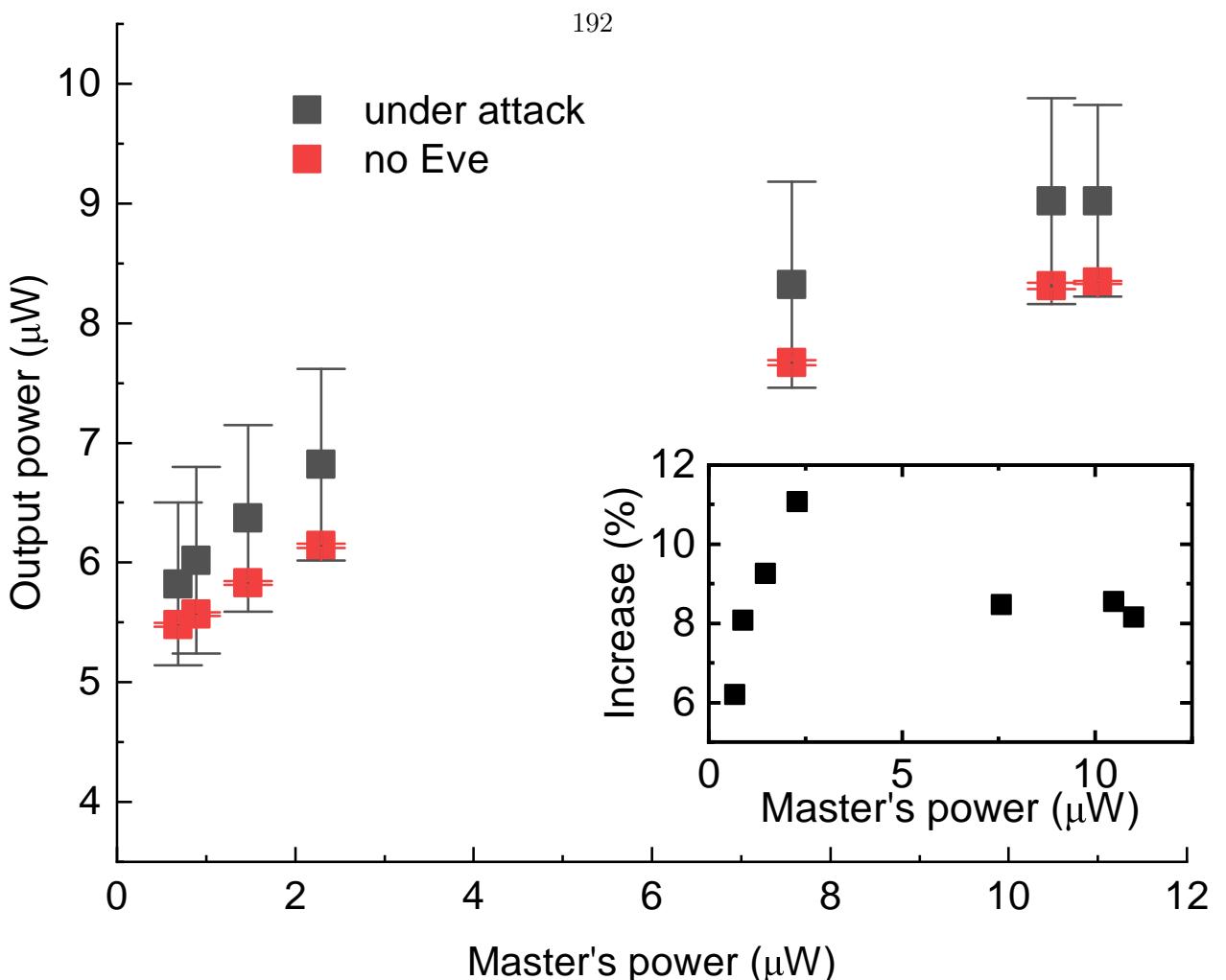


Рисунок 5.10 — Средняя выходная мощность источника КРК без Евы и в присутствии атаки с лазерным засевом.

и, таким образом, площадь импульса должна быть получена из прямых измерений, а не из отдельных измерений амплитуды и длительности импульса). Рисунок 5.13 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%, 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.

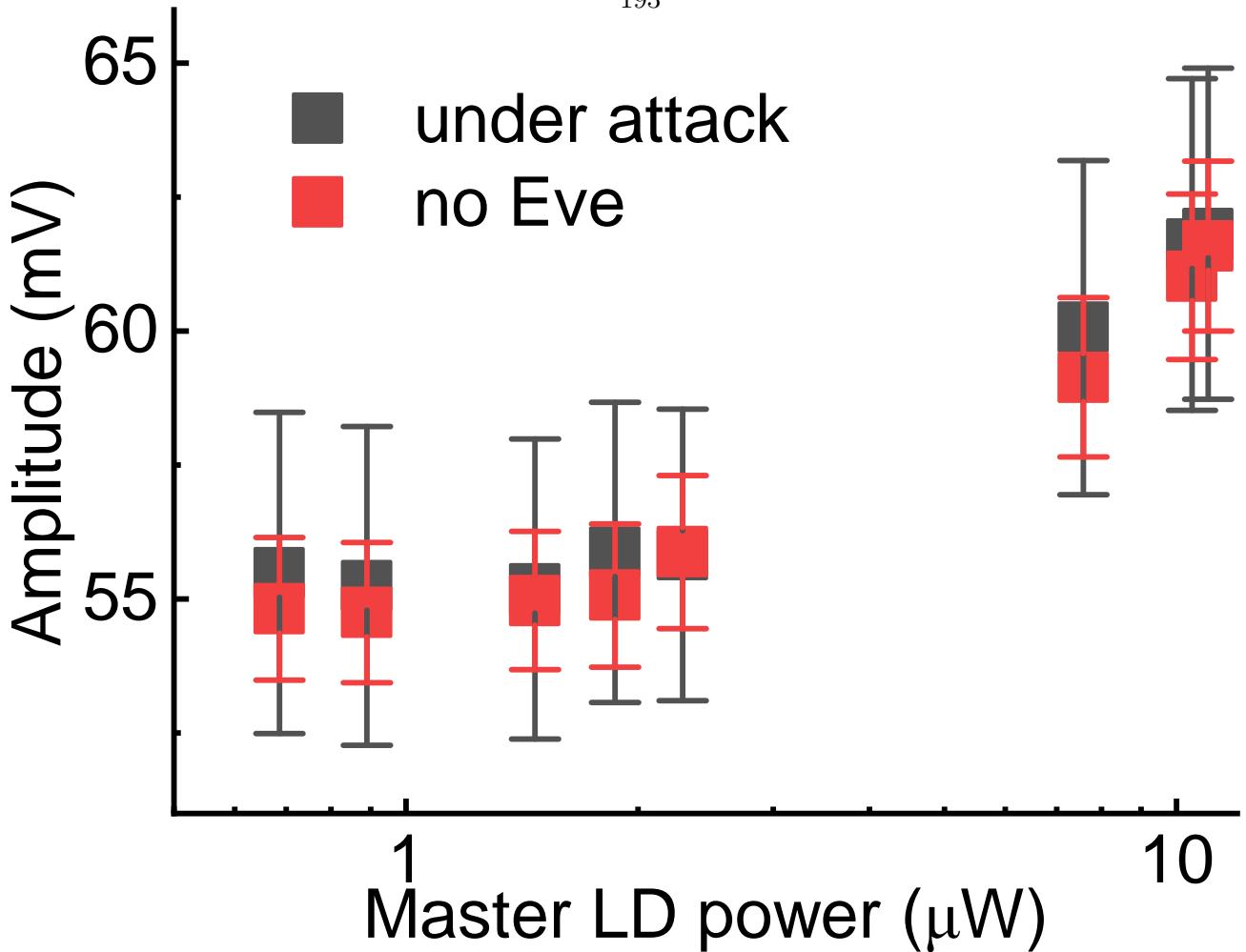


Рисунок 5.11 — Изменение средней амплитуды импульсов. Черным цветом обозначены амплитуды импульсов под действием атаки, а красным без нее.

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.

Предполагается, 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 валентной зоне, вызванными стимулированным поглощением инжектированного света Евы.

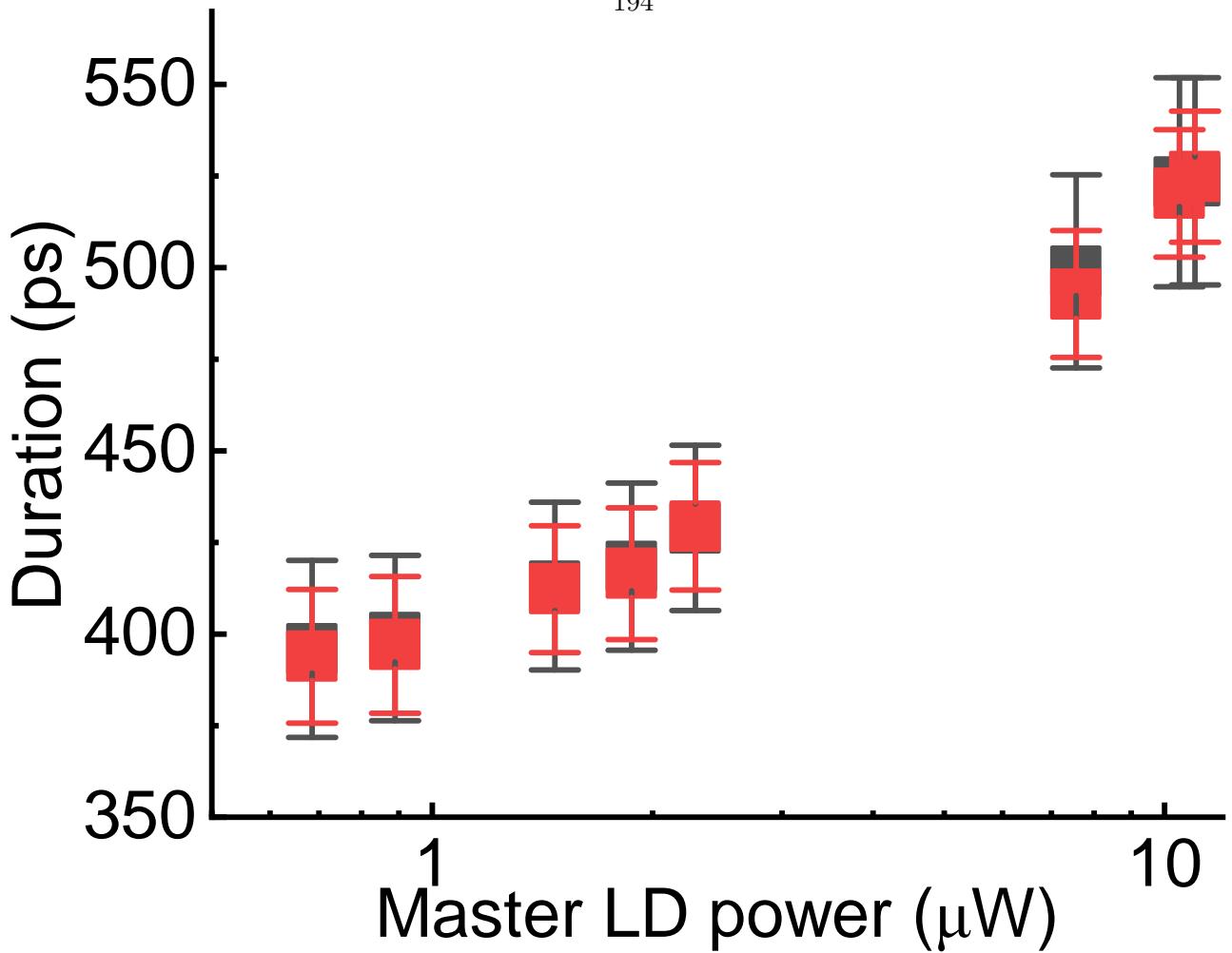


Рисунок 5.12 — Изменение средней длительности импульсов. Чёрным цветом обозначены длительности импульсов под действием атаки, а красным без нее.

В наших экспериментах мы также количественно оценили влияние инжектированного света на статистику интерференции. Рисунок 5.14 и Рисунок 5.15 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 ФПВ из-за атаки внешним излучением.

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 значениям вероятности экспериментальных ФПВ. Видность уменьшается примерно с 86.4 до 80.1 , когда мощность ведущего устройства принимает максималь-

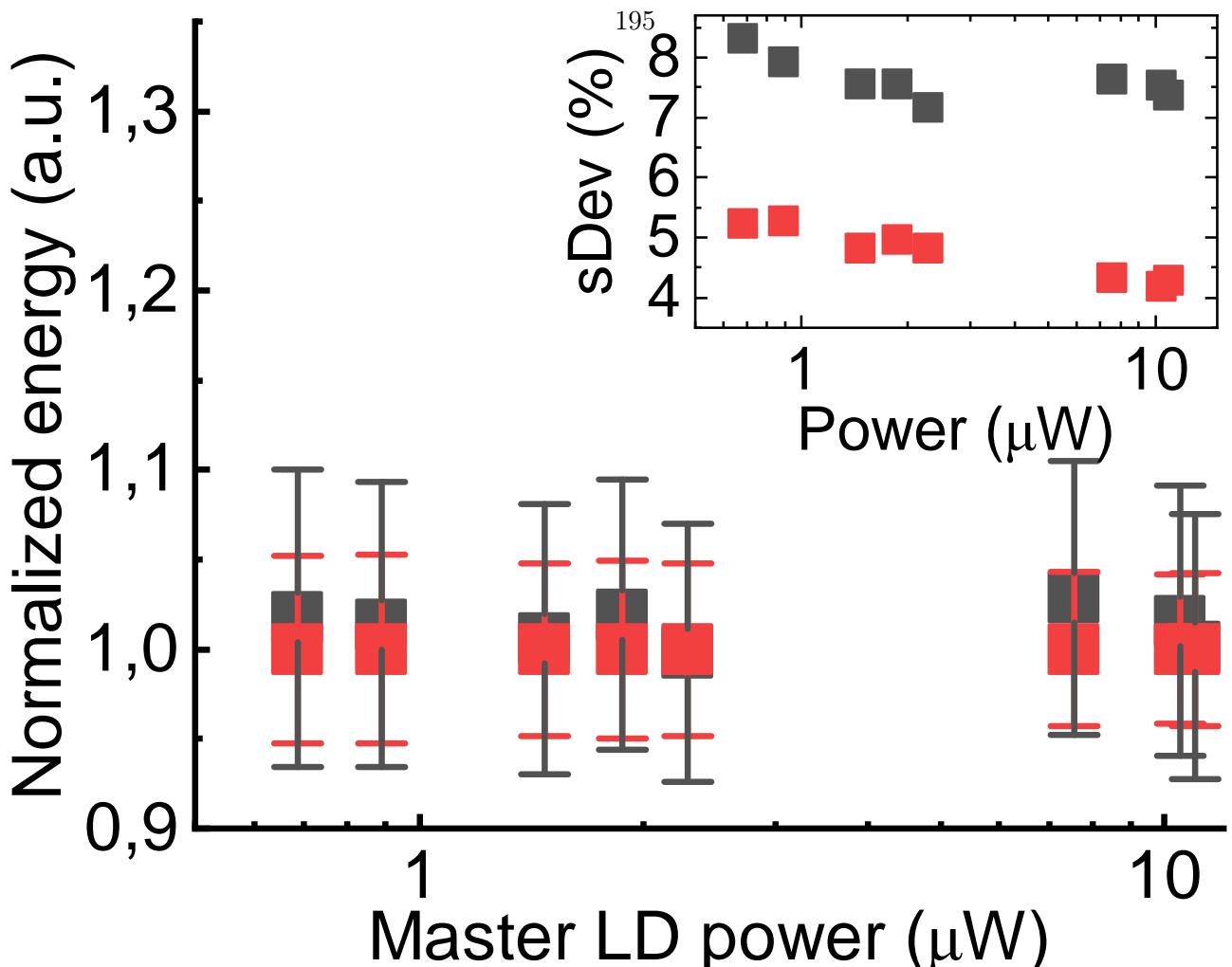


Рисунок 5.13 — Изменение средней площади импульсов. Чёрным цветом обозначены площади импульсов под действием атаки, а красным без нее.

ное 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 лазера-ведущего и лазера Евы. Возможно, что этот эффект вызван смешением усиленного света Евы с интерферирующими 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.

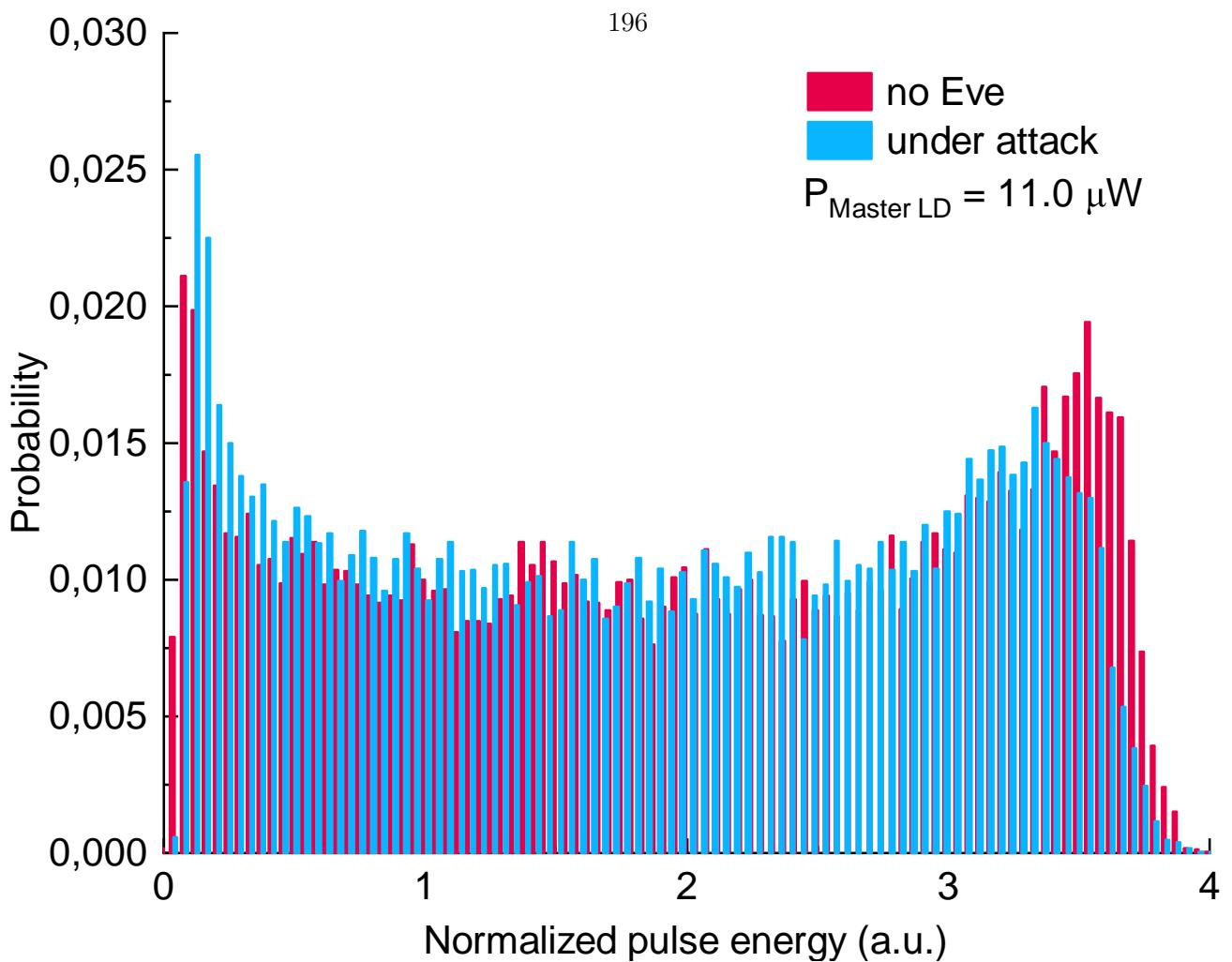


Рисунок 5.14 — Функция плотности вероятности интерференции при мощности лазера-ведущего 11 мкВт. Красным обозначена ФПВ без атаки, синим цветом обозначена ФПВ под действием атаки.

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 оце-

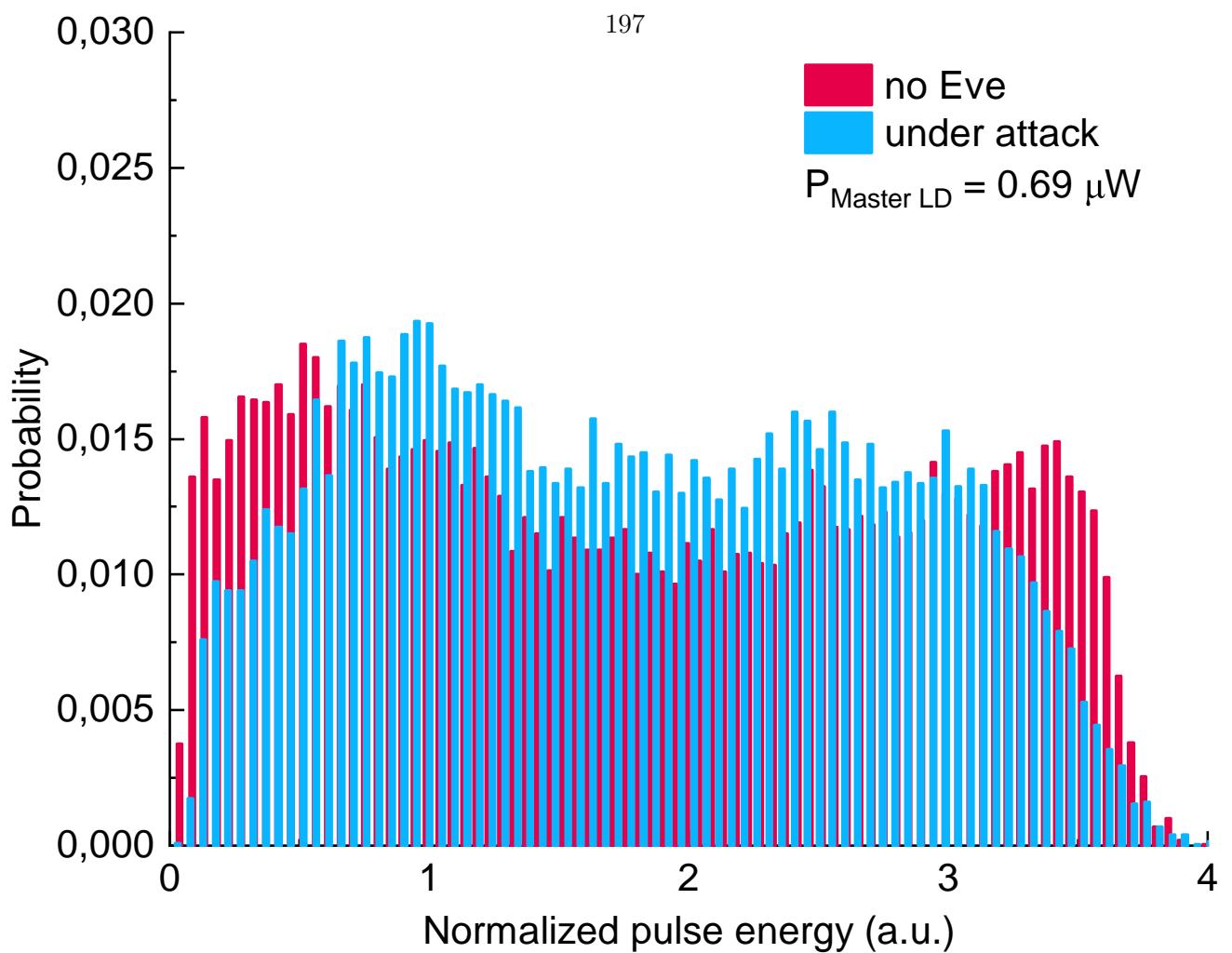


Рисунок 5.15 — Функция плотности вероятности интерференции при мощности лазера-ведущего 0.69 мкВт. Красным обозначена ФПВ без атаки, синим цветом обозначена ФПВ под действием атаки.

нить, усиливает ли ведомый лазер излучение Евы или нет, отраженные спектры вычитываются из спектров атакуемого источника QKD.

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.

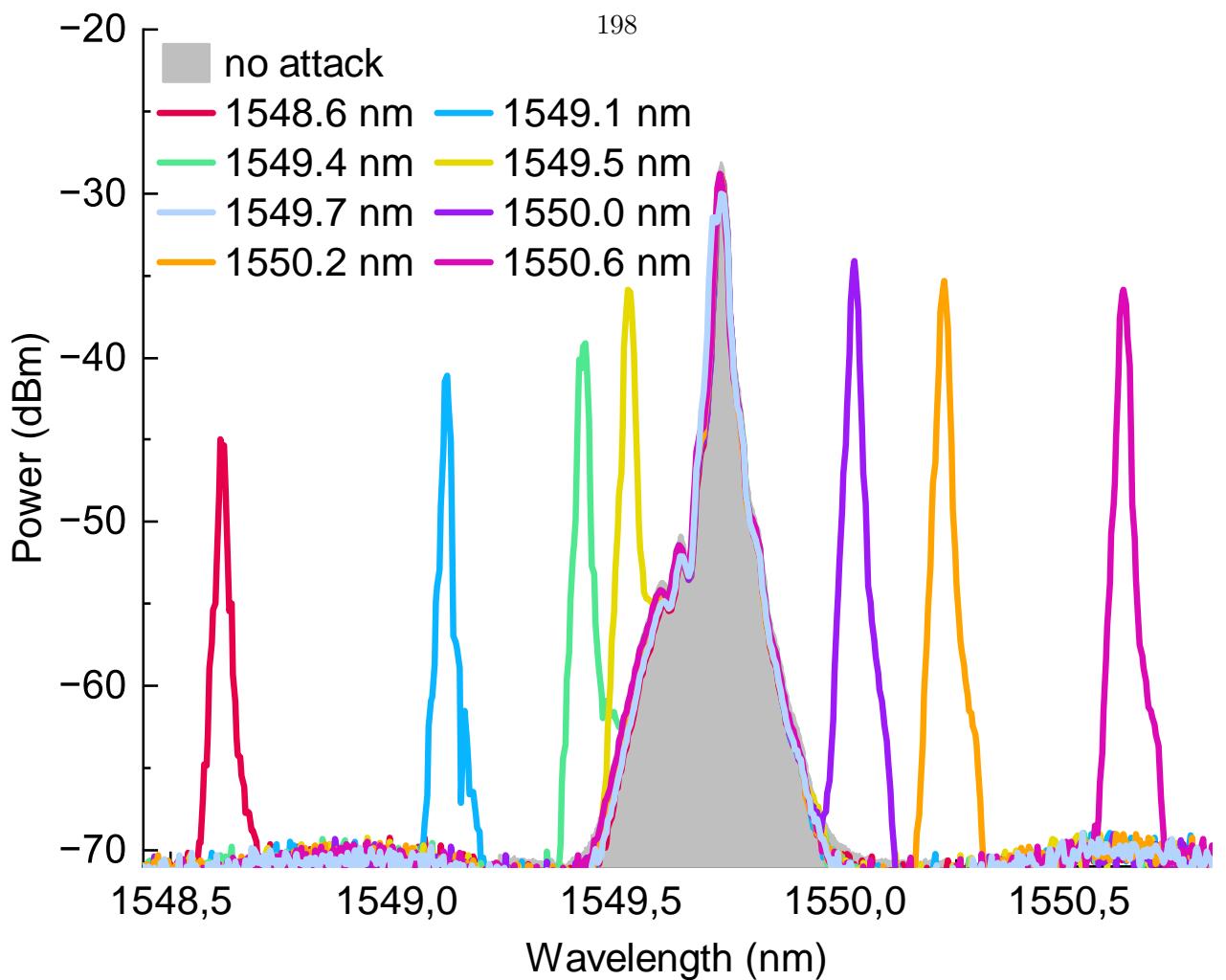


Рисунок 5.16 — Спектры выходного сигнала источника QKD для разных длин волн лазера Евы. (Спектры отраженного излучения Евы исключены из измеренных выходных спектров)

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-

ния, построенный на основе оптической инжекции, является устойчивым к атаке лазерным "засевом" 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.

Влияние атаки лазерным засевом на источник излучения на основе оптической фазовой синхронизации может быть предотвращено достаточным количеством изоляции, а также оптическими предохранителями для защиты от мощного излучения.

Заключение

В Главе 1 проведен обзор современной литературы по тематике квантового распределения ключей, теоретической основы технологии КРК. Описываются различные протоколы квантового распределения ключей: BB84, B92, Measurement-Device-Independent (Недоверенный Приемный Узел), Twin-Field QKD(протокол с использованием 'полей-близницив') и GG02, их технические особенности. Описываются возможные атаки на техническую реализацию систем квантового распределения ключей, особое внимание уделено атакам на источники лазерного излучения в составе систем КРК.

В Главе 2 изучается реализация обратной связи для двух источников лазерного излучения в виде оптической инжекции. С помощью этого метода продемонстрирован эффект синхронизации частот лазеров. При помощи этого метода экспериментально реализована система квантового распределения ключей на боковых частотах на непрерывных переменных. В разделе описывается этапы протокола, а также математическая модель детектирования сигналов. В результате продемонстрировано, что при использовании обратной связи в виде оптической инжекции на балансном детекторе наблюдается только одна частота - частота модуляции Алисы. Из этой промежуточной частоты с помощью метода быстрого преобразования Фурье извлечены значения фаз, закодированные Алисой, которые после постобработки преобразуются в значения бит сырого ключа.

В Главе 3 проводится экспериментальная реализация системы квантового распределения ключей на боковых частотах на непрерывных переменных с применением двух независимых источников лазерного излучения. Для данной системы построена математическая модель детектирования сигналов, демонстрирующая все сигналы, формирующиеся в результате взаимодействия двух сигналов на балансном детекторе, из которых выделяется полезный. Для этой системы также решается проблема компенсации поляризационных искажений из-за прохождения волоконно-оптической линии. Это происходит с

помощью контроллера поляризации, который работает по сигналу обратной связи, сформированного на основе результата Быстрого Преобразования Фурье к регистрируемому сигналу и описывается все этапы алгоритма подстройки поляризации. А также показано из какого сигнала возможно извлекать информацию о сыром ключе.

В Главе 4 описывается новый тип атаки на техническую реализацию систем КРК - атака оптической накачкой. Суть этой атаки заключается в увеличении энергии излучаемых импульсов за счет поглощения более высокочастотного лазерного излучения Евы. В ходе работы изучены зависимости Ватт-Амперной характеристики лазера и его дифференциальной квантовой эффективности от мощности накачки Евы. Изучено влияние мощности накачки Евы на выходную среднюю мощность и энергию импульсов Алисы. Определена пороговая мощность на длине волны 1310 нм в $70\mu W$. Проанализирована стойкость промышленной системы КРК к данному типу атаки и произведен расчет минимально необходимой изоляции для защиты от данного типа атаки.

В Главе 5 изучается атака лазерным 'засевом' на источник лазерного излучения на основе оптической инжекции. В рамках работы изучены зависимости средней мощности, энергии импульсов, длительности импульсов и влияния этой атаки на интерференцию. Показано, что атака 'засевом' увеличивает излучаемую среднюю мощность и энергию импульсов, а также увеличивает среднеквадратическое отклонение этих параметров. Показано, что длительность импульсов под действием этой атаки не изменяется. Интерференционная картина под действием атаки ухудшается, что негативно влияет на QBER рабочей системы КРК. Также определена минимальная изоляция, необходимая для защиты источника лазерного излучения на основе оптической инжекции от атаки 'засевом' лазерным излучением.

Список литературы

1. *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.
2. *Bennett C. H.* Quantum Cryptography Using Any 2 Nonorthogonal States // *Phys. Rev. Lett.* — 1992. — Vol. 68, no. 21. — Pp. 3121–3124.
3. *Ekert A. K.* Quantum Cryptography Based on Bell's Theorem // *Phys. Rev. Lett.* — 1991. — Vol. 67, no. 6. — Pp. 661–663.
4. *Wang X.-B.* Decoy-state protocol for quantum cryptography with four different intensities of coherent light // *Phys. Rev. A.* — 2005. — Vol. 72, no. 1. — P. 012322.
5. *Yuan Z., Shields A.* Continuous operation of a one-way quantum key distribution system over installed telecom fibre // *Opt. Express.* — 2005. — Vol. 13, no. 2. — Pp. 660–665.
6. *Andersen U. L., Leuchs G., Silberhorn C.* Continuous-variable quantum information processing // *Laser Photon. Rev.* — 2010. — Vol. 4. — P. 337.
7. Continuous operation of high bit rate quantum key distribution / A. R. Dixon, Z. L. Yuan, J. F. Dynes et al. // *Appl. Phys. Lett.* — 2010. — Vol. 96, no. 16. — P. 161102.
8. Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator / Adnan A. E. Hajomer, Ivan Derkach, Nitin Jain et al. // *Science Advances.* — 2024. — Vol. 10, no. 1. — P. eadi9474. — URL: <https://www.science.org/doi/abs/10.1126/sciadv.ad9474>.
9. *Diamanti Eleni, Leverrier Anthony.* Distributing Secret Keys with Quantum Continuous Variables: Principle, Security and Implementations // *Entropy.* —

2015. — Vol. 17, no. 9. — Pp. 6072–6092. — URL: <https://www.mdpi.com/1099-4300/17/9/6072>.
10. Coherent detection in optical fiber systems / Ezra Ip, Alan Pak Tao Lau, Daniel J. F. Barros, Joseph M. Kahn // *Opt. Express.* — 2008. — Jan. — Vol. 16, no. 2. — Pp. 753–791. — URL: <https://opg.optica.org/oe/abstract.cfm?URI=oe-16-2-753>.
 11. High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation / Heng Wang, Yaodi Pi, Wei Huang et al. // *Optics Express.* — 2020. — oct. — Vol. 28, no. 22. — P. 32882. — URL: <http://dx.doi.org/10.1364/OE.404611>.
 12. *Khaksar Zeinab S., Bahrampour Alireza.* Generating local oscillator locally in continuous variable quantum key distribution using optical injection phase locked loop: a theoretical approach // *Opt. Express.* — 2023. — Nov. — Vol. 31, no. 23. — Pp. 37911–37928. — URL: <https://opg.optica.org/oe/abstract.cfm?URI=oe-31-23-37911>.
 13. Hacking commercial quantum cryptography systems by tailored bright illumination / L. Lydersen, C. Wiechers, C. Wittmann et al. // *Nat. Photonics.* — 2010. — Vol. 4. — Pp. 686–689.
 14. Trojan-horse attacks on quantum-key-distribution systems / N. Gisin, S. Fasel, B. Kraus et al. // *Phys. Rev. A.* — 2006. — Vol. 73, no. 2. — P. 022320.
 15. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack / Jing-Zheng Huang, Christian Weedbrook, Zhen-Qiang Yin et al. // *Physical Review A.* — 2013. — jun. — Vol. 87, no. 6. — URL: <http://dx.doi.org/10.1103/PhysRevA.87.062329>.
 16. Laser-seeding attack in quantum key distribution / Anqi Huang, Álvaro Navarrete, Shi-Hai Sun et al. // *Phys. Rev. Appl.* — 2019. — Vol. 12. — P. 064043.

17. 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.
18. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol / Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, Lin-Mei Liang // *Physical Review A*. — 2013. — may. — Vol. 87, no. 5. — URL: <http://dx.doi.org/10.1103/PhysRevA.87.052309>.
19. 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.
20. Phase-reference-intensity attack on continuous-variable quantum key distribution with a local local oscillator / Yun Shao, Yang Li, Heng Wang et al. // *Phys. Rev. A*. — 2022. — Mar. — Vol. 105. — P. 032601. — URL: <https://link.aps.org/doi/10.1103/PhysRevA.105.032601>.
21. Quantum Hacking Against Discrete-Modulated Continuous-Variable Quantum Key Distribution Using Modified Local Oscillator Intensity Attack with Random Fluctuations / Lu Fan, Yiming Bian, Mingze Wu et al. // *Phys. Rev. Appl.* — 2023. — Aug. — Vol. 20. — P. 024073. — URL: <https://link.aps.org/doi/10.1103/PhysRevApplied.20.024073>.
22. Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise / Shengjun Ren, Rupesh Kumar, Adrian Wonfor et al. // *J. Opt. Soc. Am. B*. — 2019. — Mar. — Vol. 36, no. 3. — Pp. B7–B15. — URL: <https://opg.optica.org/josab/abstract.cfm?URI=josab-36-3-B7>.
23. Р.А. Шаховой. Динамика полупроводниковых лазеров: Учебное пособие для вузов. — 1 edition. — Издательство "Лань 2024".
24. Liu Zhixin, Slavik Radan. Optical Injection Locking: from Principle to Applications // *J. Light. Technol.* — 2020. — Vol. 38, no. 1. — Pp. 43–59.

25. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference / A. V. Gleim, V. I. Egorov, Yu. V. Nazarov et al. // *Opt. Express.* — 2016. — Vol. 24. — Pp. 2619–2633.
26. Sideband quantum communication at 1  Mbit/s on a metropolitan area network / A. V. Gleim, V. V. Chistyakov, O. I. Bannik et al. // *J. Opt. Technol.* — 2017. — Jun. — Vol. 84, no. 6. — Pp. 362–367. — URL: <https://opg.optica.org/jot/abstract.cfm?URI=jot-84-6-362>.
27. HETERODYNE DETECTION FOR SUBCARRIER-WAVE QUANTUM KEY DISTRIBUTION SYSTEM / Fadeev M.a, Morozova P.A, Smirnov S.V. et al. // *Radiophys. and Quantum Electron.* — 2024. — sept. — Vol. 67, no. 9. — Pp. 784–793. — URL: https://doi.org/10.52452/00213462_2024_67_09_784.
28. A low-complexity heterodyne CV-QKD architecture / Hans H. Brunner, Lucian C. Comandar, Fotini Karinou et al. // 2017 19th International Conference on Transparent Optical Networks (ICTON). — 2017. — Pp. 1–4.
29. DeLange O. E. Optical heterodyne detection // *IEEE Spectrum*. — 1968. — Vol. 5, no. 10. — Pp. 77–85.
30. Kuri Toshiaki, ichi Kitayama Ken. Optical Heterodyne Detection Technique for Densely Multiplexed Millimeter-Wave-Band Radio-on-Fiber Systems // *J. Lightwave Technol.* — 2003. — Dec. — Vol. 21, no. 12. — P. 3167. — URL: <https://opg.optica.org/jlt/abstract.cfm?URI=jlt-21-12-3167>.
31. Coherent detection schemes for subcarrier wave continuous variable quantum key distribution / E. Samsonov, R. Goncharov, M. Fadeev et al. // *J. Opt. Soc. Am. B.* — 2021. — Jul. — Vol. 38, no. 7. — Pp. 2215–2222. — URL: <https://opg.optica.org/josab/abstract.cfm?URI=josab-38-7-2215>.
32. Laser-pumping attack on QKD sources / M. Fadeev, A.A. Ponosova, R. Shakhovoy, V. Makarov // 2024 International Conference Laser Optics (ICLO). — 2024. — Pp. 562–562.

33. Optical-pumping attack on a quantum key distribution laser source / M. Fadeev, A. Ponosova, Q. Peng et al. // *Phys. Rev. A.* — 2025. — Vol. -, no. -. — Pp. -.
34. Risk Analysis of Countermeasures Against the Trojan-Horse Attacks on Quantum Key Distribution Systems in 1260–1650 nm Spectral Range / A. V. Borisova, B. D. Garmaev, I. B. Bobrov et al. // *Opt. Spectrosc.* — 2020. — nov. — Vol. 128, no. 11. — Pp. 1892–1900. — URL: <http://dx.doi.org/10.1134/S0030400X20110077>.
35. Analyzing Transmission Spectra of Fiber-Optic Elements in the Near IR Range to Improve the Security of Quantum Key Distribution Systems / B. A. Nasedkin, I. M. Filipov, A. O. Ismagilov et al. // *Bull. Russ. Acad. Sci.: Phys.* — 2022. — oct. — Vol. 86, no. 10. — Pp. 1164–1167. — URL: <http://dx.doi.org/10.3103/S1062873822100148>.
36. Loopholes in the 1500–2100-nm Range for Quantum-Key-Distribution Components: Prospects for Trojan-Horse Attacks / Boris Nasedkin, Fedor Kiselev, Ilya Filipov et al. // *Phys. Rev. Appl.* — 2023. — Jul. — Vol. 20. — P. 014038. — URL: <https://link.aps.org/doi/10.1103/PhysRevApplied.20.014038>.
37. Deriving the absorption coefficients of lattice mismatched InGaAs using genetic algorithm / Hui Jing Lee, Mansur Mohammed Ali Gamel, Pin Jern Ker et al. // *Mater. Sci. Semicond. Process.* — 2023. — Vol. 153. — P. 107135.
38. *Svelto Orazio*. Transient Laser Behavior // Principles of Lasers. — Boston, MA: Springer US, 2010. — Pp. 313–373. — URL: https://doi.org/10.1007/978-1-4419-1302-9_8.
39. Optically pumped membrane BH-DFB lasers for low-threshold and single-mode operation / Takeshi Okamoto, Nobuhiro Nunoya, Yuichi Onodera et al. // *IEEE J. Sel. Top. Quantum Electron.* — 2003. — sep. — Vol. 9, no. 5. — Pp. 1361–1366. — URL: <http://dx.doi.org/10.1109/jstqe.2003.819495>.

40. *Guina M., Rantamäki A., Häkkinen A.* Optically pumped VECSELs: review of technology and progress // *J. Phys. D: Appl. Phys.* — 2017. — aug. — Vol. 50, no. 38. — P. 383001. — URL: <http://dx.doi.org/10.1088/1361-6463/aa7bfd>.
41. 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.
42. Directly Phase-Modulated Light Source / Z. L. Yuan, B. Fröhlich, M. Lucamarini et al. // *Phys. Rev. X.* — 2016. — Sep. — Vol. 6. — P. 031044. — URL: <https://link.aps.org/doi/10.1103/PhysRevX.6.031044>.
43. A direct GHz-clocked phase and intensity modulated transmitter applied to quantum key distribution / G L Roberts, M Lucamarini, J F Dynes et al. // *Quantum Science and Technology.* — 2018. — aug. — Vol. 3, no. 4. — P. 045010. — URL: <https://dx.doi.org/10.1088/2058-9565/aad9bd>.
44. Secure laser source for QKD systems / M. Fadeev, A.A. Ponosova, A. Huang et al. // 2024 International Conference Laser Optics (ICLO). — 2024. — Pp. 571–571.
45. 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.
46. Eavesdrop-detecting quantum communications channel / C. H. Bennett, G. Brassard, S. Breidbart, S. Wiesner // *IBM Tech. Discl. Bull.* — 1984. — Vol. 26. — Pp. 4363–4366.
47. *Lo H.-K., Curty M., Qi B.* Measurement-device-independent quantum key distribution // *Phys. Rev. Lett.* — 2012. — Vol. 108. — P. 130503.
48. 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.

49. *Inamori H., Lütkenhaus N., Mayers D.* Unconditional security of practical quantum key distribution // *Eur. Phys. J. D.* — 2007. — Vol. 41. — Pp. 599–627.
50. 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.
51. *Lo Hoi-Kwong, Ma Xiongfeng, Chen Kai.* Decoy state quantum key distribution // *Phys. Rev. Lett.* — 2005. — Vol. 94, no. 23. — P. 230504.
52. *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>.
53. *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>.
54. *Takeoka Masahiro, Guha Saikat, Wilde Mark M.* Fundamental rate-loss trade-off for optical quantum key distribution // *Nature Communications.* — 2014. — Oct. — Vol. 5, no. 5. — URL: <https://doi.org/10.1038/ncomms6235>.
55. Fundamental limits of repeaterless quantum communications / Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, Leonardo Banchi // *Nature Communications.* — 2017. — apr. — Vol. 8, no. 1. — URL: <http://dx.doi.org/10.1038/ncomms15043>.
56. *Koashi M.* Simple security proof of quantum key distribution via uncertainty principle // *arXiv*.
57. 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>.

58. Practical decoy state for quantum key distribution / Xiongfeng Ma, Bing Qi, Yi Zhao, Hoi-Kwong Lo // *Phys. Rev. A.* — 2005. — Vol. 72. — P. 012326.
59. 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.
60. 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.
61. The security of practical quantum key distribution / V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf et al. // *Rev. Mod. Phys.* — 2009. — Vol. 81, no. 3. — Pp. 1301–1350.
62. Wang Xiang-Bin, Yu Zong-Wen, Hu Xiao-Long. Twin-field quantum key distribution with large misalignment error // *Phys. Rev. A.* — 2018. — Vol. 98. — P. 062323.
63. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters / M. Lucamarini, Z. L. Yuan, J. F. Dynes, A. J. Shields // *Nature.* — 2018. — Vol. 557. — P. 400.
64. 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.
65. Braunstein S. L., van Loock P. Quantum information with continuous variables // *Rev. Mod. Phys.* — 2005. — Jun. — Vol. 77, no. 2. — Pp. 513–577.
66. Ralph T. C. Continuous variable quantum cryptography // *Phys. Rev. A.* — 1999. — Vol. 61, no. 1. — P. 010303.
67. Ralph T. Security of continuous-variable quantum cryptography // *Physical Review A.* — 2000. — nov. — Vol. 62, no. 6. — URL: <http://dx.doi.org/10.1103/PhysRevA.62.062306>.

68. *Hillery M.* Quantum cryptography with squeezed states // *Phys. Rev. A.* — 2000. — Vol. 61, no. 2. — P. 022309.
69. *Reid M. D.* Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations // *Phys. Rev. A.* — 2000. — Vol. 62, no. 6. — P. 062308.
70. *Cerf N. J., Lévy M., Assche G. Van.* Quantum distribution of Gaussian keys using squeezed states // *Phys. Rev. A.* — 2001. — Apr. — Vol. 63. — P. 052311. — URL: <https://link.aps.org/doi/10.1103/PhysRevA.63.052311>.
71. *Van Assche G., Cardinal J., Cerf N.J.* Reconciliation of a quantum-distributed Gaussian key // *IEEE Transactions on Information Theory.* — 2004. — Vol. 50, no. 2. — Pp. 394–400.
72. *Gottesman Daniel, Preskill John.* Secure quantum key distribution using squeezed states // *Physical Review A.* — 2001. — jan. — Vol. 63, no. 2. — URL: <http://dx.doi.org/10.1103/PhysRevA.63.022309>.
73. *Grosshans Frédéric, Grangier Philippe.* Continuous Variable Quantum Cryptography Using Coherent States // *Physical Review Letters.* — 2002. — jan. — Vol. 88, no. 5. — URL: <http://dx.doi.org/10.1103/PhysRevLett.88.057902>.
74. *Grosshans Frédéric, Grangier Philippe.* Quantum cloning and teleportation criteria for continuous quantum variables // *Physical Review A.* — 2001. — jun. — Vol. 64, no. 1. — URL: <http://dx.doi.org/10.1103/PhysRevA.64.010301>.
75. Continuous Variable Quantum Cryptography: Beating the 3BrdB Loss Limit / Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, G. Leuchs // *Physical Review Letters.* — 2002. — sep. — Vol. 89, no. 16. — URL: <http://dx.doi.org/10.1103/PhysRevLett.89.167901>.
76. *Grosshans Frédéric, Grangier Philippe.* Reverse reconciliation protocols for quantum cryptography with continuous variables // *arXiv.* — 2002. — URL: <https://arxiv.org/abs/quant-ph/0204127>.

77. Quantum Cryptography Without Switching / Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen et al. // *Physical Review Letters*. — 2004. — oct. — Vol. 93, no. 17. — URL: <http://dx.doi.org/10.1103/PhysRevLett.93.170504>.
78. Navascués Miguel, Grosshans Frédéric, Acín Antonio. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography // *Physical Review Letters*. — 2006. — nov. — Vol. 97, no. 19. — URL: <http://dx.doi.org/10.1103/PhysRevLett.97.190502>.
79. García-Patrón Raúl, Cerf Nicolas J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution // *Phys. Rev. Lett.* — 2006. — Nov. — Vol. 97. — P. 190503. — URL: <https://link.aps.org/doi/10.1103/PhysRevLett.97.190503>.
80. Pirandola Stefano, Braunstein Samuel L., Lloyd Seth. Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography // *Phys. Rev. Lett.* — 2008. — Nov. — Vol. 101. — P. 200504. — URL: <https://link.aps.org/doi/10.1103/PhysRevLett.101.200504>.
81. Direct and Reverse Secret Key Capacities of a Quantum Channel / Stefano Pirandola, Raul García-Patrón, Samuel L. Braunstein, Seth Lloyd // *Physical Review Letters*. — 2009. — feb. — Vol. 102, no. 5. — URL: <http://dx.doi.org/10.1103/PhysRevLett.102.050503>.
82. Renner R., Cirac J. I. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography // *Phys. Rev. Lett.* — 2009. — Vol. 102, no. 11. — P. 110504.
83. Pirandola Stefano. Quantum discord as a resource for quantum cryptography // *Scientific Reports*. — 2014. — nov. — Vol. 4, no. 1. — URL: <http://dx.doi.org/10.1038/srep06956>.

84. *Usenko Vladyslav, Filip Radim.* Trusted Noise in Continuous Variable Quantum Key Distribution: A Threat and a Defense // *Entropy*. — 2016. — jan. — Vol. 18, no. 1. — P. 20. — URL: <http://dx.doi.org/10.3390/e18010020>.
85. *Laudenbach Fabian, Pacher Christoph.* Analysis of the Trusted Device Scenario in Continuous Variable Quantum Key Distribution // *Advanced Quantum Technologies*. — 2019. — aug. — Vol. 2, no. 11. — URL: <http://dx.doi.org/10.1002/quate.201900055>.
86. *Hosseinidehaj Nedasadat, Walk Nathan, Ralph Timothy C.* Optimal realistic attacks in continuous-variable quantum key distribution // *Physical Review A*. — 2019. — may. — Vol. 99, no. 5. — URL: <http://dx.doi.org/10.1103/PhysRevA.99.052336>.
87. Secret-Key Distillation across a Quantum Wiretap Channel under Restricted Eavesdropping / Ziwen Pan, Kaushik P. Seshadreesan, William Clark et al. // *Physical Review Applied*. — 2020. — aug. — Vol. 14, no. 2. — URL: <http://dx.doi.org/10.1103/PhysRevApplied.14.024044>.
88. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction / Ying Guo, Qin Liao, Yijun Wang et al. // *Phys. Rev. A*. — 2017. — Mar. — Vol. 95. — P. 032304. — URL: <https://link.aps.org/doi/10.1103/PhysRevA.95.032304>.
89. Continuous-variable quantum key distribution with non-Gaussian quantum catalysis / Ying Guo, Wei Ye, Hai Zhong, Qin Liao // *Physical Review A*. — 2019. — mar. — Vol. 99, no. 3. — URL: <http://dx.doi.org/10.1103/PhysRevA.99.032327>.
90. Long-Distance Continuous-Variable Quantum Key Distribution With Quantum Scissors / Masoud Ghalaii, Carlo Ottaviani, Rupesh Kumar et al. // *IEEE Journal of Selected Topics in Quantum Electronics*. — 2020. — may. — Vol. 26, no. 3. — Pp. 1–12. — URL: <http://dx.doi.org/10.1109/JSTQE.2020.2964395>.

91. Field test of a continuous-variable quantum key distribution prototype / S. Fossier, E. Diamanti, T. Debuisschert et al. // *New J. Phys.* — 2009. — Vol. 11, no. 4. — P. 045023.
92. Experimental demonstration of long-distance continuous-variable quantum key distribution / Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier et al. // *Nature Photonics*. — 2013. — apr. — Vol. 7, no. 5. — Pp. 378–381. — URL: <http://dx.doi.org/10.1038/NPHOTON.2013.63>.
93. Kumar Rupesh, Qin Hao, Alléaume Romain. Coexistence of continuous variable QKD with intense DWDM classical channels // *New Journal of Physics*. — 2015. — apr. — Vol. 17, no. 4. — P. 043027. — URL: <https://dx.doi.org/10.1088/1367-2630/17/4/043027>.
94. Atmospheric continuous-variable quantum communication / B Heim, C Peuntinger, N Killoran et al. // *New Journal of Physics*. — 2014. — nov. — Vol. 16, no. 11. — P. 113018. — URL: <http://dx.doi.org/10.1088/1367-2630/16/11/113018>.
95. Ip Ezra, Kahn Joseph M. Feedforward Carrier Recovery for Coherent Optical Communications // *Journal of Lightwave Technology*. — 2007. — Vol. 25, no. 9. — Pp. 2675–2692.
96. Homodyne Coherent Optical Receiver Using an Optical Injection Phase-Lock Loop / Martyn J. Fice, Andrea Chiuchiarelli, Ernesto Ciaramella, Alwyn J. Seeds // *Journal of Lightwave Technology*. — 2011. — Vol. 29, no. 8. — Pp. 1152–1164.
97. Khaksar Zeinab Sadat, Bahrampour Alireza. Simultaneous BPSK classical communication and continuous variable quantum key distribution with a locally local oscillator regenerated by optical injection phase locked loop // *Journal of Laser Applications*. — 2023. — 09. — Vol. 35, no. 4. — P. 042016. — URL: <https://doi.org/10.2351/7.0001068>.

98. *Makarov V.* Controlling passively quenched single photon detectors by bright light // *New J. Phys.* — 2009. — Vol. 11, no. 6. — P. 065003.
99. Bright-light detector control emulates the local bounds of Bell-type inequalities / Shihan Sajeeb, Nigar Sultana, Charles Ci Wen Lim, Vadim Makarov // *Scientific Reports.* — 2020. — aug. — Vol. 10, no. 1. — URL: <http://dx.doi.org/10.1038/s41598-020-70045-7>.
100. Controlling single-photon detector ID210 with bright light / Vladimir Chistikov, Anqi Huang, Vladimir Egorov, Vadim Makarov // *Opt. Express.* — 2019. — Vol. 27. — P. 32253.
101. Hacking the quantum key distribution system by exploiting the avalanche-transition region of single-photon detectors / Yong-Jun Qian, De-Yong He, Shuang Wang et al. // *Phys. Rev. Appl.* — 2018. — Vol. 10. — P. 064062.
102. *Lydersen L., Skaar J.* Security of quantum key distribution with bit and basis dependent detector flaws // *Quant. Inf. Comp.* — 2010. — Vol. 10. — Pp. 60–76.
103. Trojan-horse attacks threaten the security of practical quantum cryptography / Nitin Jain, Elena Anisimova, Imran Khan et al. // *New J. Phys.* — 2014. — Vol. 16. — P. 123030.
104. Draft ETSI GS QKD 010 V0.4.1 (2021-06). Quantum key distribution (QKD); Implementation security: protection against Trojan horse attacks. — https://docbox.etsi.org/ISG/QKD/Open/GS-QKD-0010 ISTrojan_v0.4.1_OpenArea.pdf, visited 13 Oct 2023.
105. Optical injection locking based local oscillator regeneration for continuous variable quantum key distribution / Zikang Su, Dajian Cai, Hao Jiang et al. // *Opt. Lett.* — 2022. — Mar. — Vol. 47, no. 5. — Pp. 1287–1290. — URL: <https://opg.optica.org/ol/abstract.cfm?URI=ol-47-5-1287>.
106. Performance of continuous variable quantum key distribution system at different detector bandwidth / X. Tang, R. Kumar, S. Ren et al. // *Optics*

Communications. — 2020. — Vol. 471. — P. 126034. — URL: <https://www.sciencedirect.com/science/article/pii/S003040182030451X>.

107. Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator / Adnan A. E. Hajomer, Ivan Derkach, Nitin Jain et al. // *Science Advances*. — 2024. — Vol. 10, no. 1. — P. eadi9474. — URL: <https://www.science.org/doi/abs/10.1126/sciadv.ad9474>.
108. Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator / Fabian Laudenbach, Bernhard Schrenk, Christoph Pacher et al. // *Quantum*. — 2019. — oct. — Vol. 3. — P. 193. — URL: <http://dx.doi.org/10.22331/q-2019-10-07-193>.
109. Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator / Tao Wang, Peng Huang, Yingming Zhou et al. // *Phys. Rev. A*. — 2018. — Jan. — Vol. 97. — P. 012310. — URL: <https://link.aps.org/doi/10.1103/PhysRevA.97.012310>.
110. Toward the Integration of CV Quantum Key Distribution in Deployed Optical Networks / Fotini Karinou, Hans H. Brunner, Chi-Hang Fred Fung et al. // *IEEE Photonics Technology Letters*. — 2018. — Vol. 30, no. 7. — Pp. 650–653.
111. M Oxborrow, Sinclair Alastair G. Single-photon sources // *Contemporary Physics*. — 2005. — Vol. 46, no. 3. — Pp. 173–206.
112. Continuous-variable quantum key distribution under strong channel polarization disturbance / Wenyuan Liu, Yanxia Cao, Xuyang Wang, Yongmin Li // *Phys. Rev. A*. — 2020. — Sep. — Vol. 102. — P. 032625. — URL: <https://link.aps.org/doi/10.1103/PhysRevA.102.032625>.
113. Quantum Key Distribution Based on Private States: Unconditional Security Over Untrusted Channels With Zero Quantum Capacity / Karol Horodecki, Michal Horodecki, Paweł Horodecki et al. // *IEEE Trans. Inf. Theory*. — 2008. — Vol. 54, no. 6. — Pp. 2604–2620.

114. *Lo Hoi-Kwong, Curty Marcos, Tamaki Kiyoshi.* Secure quantum key distribution // *Nat. Photonics.* — 2014. — Vol. 8. — Pp. 595–604.
115. Quantum key distribution with hacking countermeasures and long term field trial / A. R. Dixon, J. F. Dynes, M. Lucamarini et al. // *Sci. Rep.* — 2017. — Vol. 7. — P. 1978.
116. Secure quantum key distribution with realistic devices / Feihu Xu, Xiongfeng Ma, Qiang Zhang et al. // *Rev. Mod. Phys.* — 2020. — Vol. 92, no. 2. — P. 025002.
117. Preparing a commercial quantum key distribution system for certification against implementation loopholes / Vadim Makarov, Alexey Abrikosov, Poompong Chaiwongkhot et al. // *arXiv.* — 2023.
118. 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.
119. *Svelto Orazio.* Pumping Processes // Principles of Lasers. — Boston, MA: Springer US, 1998. — Pp. 201–248. — URL: https://doi.org/10.1007/978-1-4757-6266-2_6.
120. Continuously tunable solution-processed organic semiconductor DFB lasers pumped by laser diode / Sönke Klinkhammer, Xin Liu, Klaus Huska et al. // *Opt. Express.* — 2012. — mar. — Vol. 20, no. 6. — Pp. 6357–6364. — URL: <http://dx.doi.org/10.1364/OE.20.006357>.
121. *Cassidy Daniel T.* Differential quantum efficiency of a homogeneously broadened injection laser // *Appl. Opt.* — 1984. — Sep. — Vol. 23, no. 17. — Pp. 2870–2873. — URL: <https://opg.optica.org/ao/abstract.cfm?URI=ao-23-17-2870>.
122. High-differential quantum efficiency operation of GaInAsP/InP membrane distributed-reflector laser on Si / Takahiro Tomiyasu, Takuo Hiratani,

Daisuke Inoue et al. // *Appl. Phys. Express.* — 2017. — may. — Vol. 10, no. 6. — P. 062702. — URL: <https://dx.doi.org/10.7567/APEX.10.062702>.

123. High-power, high-efficiency, semi-random Raman fiber lasers / Andrew Grimes, Anand Hariharan, Ian Sun, Jeffrey W. Nicholson // Proc. SPIE 11981, Fiber Lasers XIX: Technology and Systems. — 2022. — P. 119810J.
124. Protecting fiber-optic quantum key distribution sources against light-injection attacks / Anastasiya Ponosova, Daria Ruzhitskaya, Poompong Chaiwongkhon et al. // *PRX Quantum*. — 2022. — Vol. 3. — P. 040307.
125. *Sun Shihai, Huang Anqi.* A review of security evaluation of practical quantum key distribution system // *Entropy*. — 2022. — Vol. 24, no. 2. — P. 260.
126. 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.
127. 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.
128. 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.
129. *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.
130. 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.

131. 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.
132. Influence of Chirp, Jitter, and Relaxation Oscillations on Probabilistic Properties of Laser Pulse Interference / Roman Shakhovoy, Violetta Sharoglazova, Alexander Udal'tsov et al. // *IEEE J. Quantum Electron.* — 2021. — Vol. 57, no. 2. — P. 2000307.
133. 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.

Тексты публикаций

Coherent detection schemes for subcarrier wave continuous variable quantum key distribution

E. SAMSONOV^{1,2,3,*}, R. GONCHAROV^{1,3}, M. FADEEV¹, A. ZINOVIEV¹,
D. KIRICHENKO^{1,3}, B. NASEDKIN^{1,3}, A. D. KISELEV^{1,3}, AND
V. EGOROV^{1,2,4}

¹ Quantum Information Laboratory, ITMO University, Kadetskaya Line, 3, Saint Petersburg, 199034, Russia

² Quanttelecom LLC, 6th Vasilyevskogo Ostrova Line, 59, Saint Petersburg, 199178, Russia

³ Laboratory of Quantum Processes and Measurements, ITMO University, Kadetskaya Line, 3, Saint Petersburg, 199034, Russia

⁴ Leading Research Center "National Center of Quantum Internet", ITMO University, Birzhevaya Line, 16, Saint Petersburg, 199034, Russia

* eosamsonov@itmo.ru

Abstract: We examine different methods to implement coherent detection in the subcarrier wave quantum key distribution (SCW QKD) systems. For classical wavefields, we present the models describing homodyne-type and heterodyne-type coherent detection schemes needed to extract information from the quadrature phase-coded multimode signals used in SCW QKD. Practical feasibility of the proposed schemes is corroborated by the experiments.

© 2023 Optical Society of America

1. Introduction

Since 1896, when the "beat receptor", the first heterodyne detector, as we know it now, was invented by Nicola Tesla [1], various forms of coherent detection methods, including homodyne and heterodyne detection, have found wide use in a variety of applications. Starting with radio communications [2], the coherent detection methods have been expanded to the optical domain [3]. Nowadays there are numerous examples of optical coherent detection usage in different fields including telecommunications [4–8] and quantum optics [9–11]. The quantum key distribution (QKD), which is one of the most active areas in quantum information and represents a promising quantum technology, in combination with coherent detection leads to a separate branch, known as the continuous variable (CV) QKD [12–21]. The CV-QKD systems rely on the methods of coherent detection for gaining information encoded in the electromagnetic field quadratures. In other words, single-photon detection can be replaced by conventional detection methods.

Active development of novel QKD systems utilising modulated multimode states of light necessitates reconsideration and modification of the existing detection schemes. A striking example of such a system is the subcarrier wave (SCW) QKD [22–29]. The method for quantum state encoding is the distinguishing feature of the SCW QKD. In this method, a strong monochromatic wave emitted by a laser is modulated in an electro-optic phase modulator to produce weak sidebands, whose relative phase with respect to the strong (carrier) wave encodes the quantum information (a detailed description of the discrete variable (DV) SCW QKD conventional protocol and the SCW CV-QKD protocol can be found in [24] and [29], respectively).

In this paper we present three coherent detection schemes with phase estimation to demodulate the quadrature phase-coded multimode signals. This type of signals is used to encode quantum information in the SCW QKD systems. The main advantage of the proposed schemes is using the carrier wave which plays a leading part in the SCW methodology as a local oscillator (LO). In practice, it provides an alternative solution of the well-known problem of transmitting the local

oscillator through the quantum channel (or its generation on the receiver's side). This is the novel approach that has not been previously discussed in works on the multimode CV-QKD [30–32]. So we present the theoretical models describing the proposed detection schemes and experimentally demonstrate how to implement coherent detection using the carrier wave as a local oscillator.

2. Phase-coded multimode signals

Our first step is to describe generation of the phase-coded multimode signals that is the essential part of the SCW QKD system. Since our proof-of-principle experiments use classical light, we shall utilise the classical model of electro-optic phase modulation [33]. Note that quantum description of electro-optic modulation applicable to quantum states can be found in [34–36].

As is shown in Figure 1, a monochromatic lightwave with the frequency ω and the amplitude E_0 is modulated by the traveling wave electro-optic phase modulator using the microwave field with the frequency Ω and the phase φ_A [37]. The phase-modulated optical field $E(t)$ then can be expressed in terms of Jacobi–Anger expansion as follows

$$E(t) = E_0 e^{i\omega t} e^{im_A \cos(\Omega t + \varphi_A)} = E_0 e^{i\omega t} \sum_{k=-\infty}^{\infty} i^k J_k(m_A) e^{ik(\Omega t + \varphi_A)}, \quad (1)$$

where $J_k(m_A)$ is the k -order Bessel function of the first kind and m_A is the modulation index which is typically small in the SCW QKD protocols. As a result, the sidebands are formed at the frequencies $\omega_k = \omega + k\Omega$, where k is the integer.

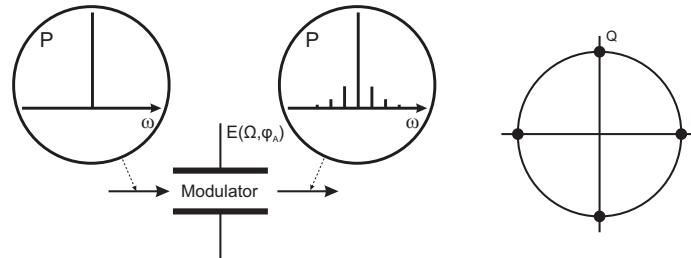


Fig. 1. Modulated light emerging after the electro-optic phase modulator and 4-PSK constellation diagram. The typical power spectrum at the modulator output in SCW QKD is also shown.

The modulated light beam emerging at the output of the phase modulator contains the reference carrier ($k = 0$) and the sidebands ($k \neq 0$). The relative phase and amplitude between reference and all the sidebands are determined by the inner microwave field that controls the phase φ_A and the modulation index m_A , respectively. Therefore one may encode the information into the sidebands of the phase-modulated light by applying different forms of quadrature amplitude modulation [23, 24, 38–40]. In this paper, for simplicity, we concentrate on the quadrature phase-shift keying which is extensively used in CV-QKDs with discrete modulation [18, 19, 41, 42]. We prepare the phase-coded multimode signals by selecting the phase of the microwave field from the finite set of $\varphi_A \in \{0, \pi/2, \pi, 3\pi/2\}$ which is equivalent to the four states commonly used in the CV-QKD protocols with discrete modulation. An example of the modulated signal constellation diagram is presented in Figure 1.

3. Subcarrier wave implementations of coherent detection

3.1. Classical coherent detection

For comparison purposes, we begin with a brief discussion of the basic concepts of coherent detection which is based on using a 50/50 beam splitter to mix an initial weak signal of the power

P_s and the reference field generated by an external source of the power P_{LO} also known as the local oscillator (LO). The mixed optical fields at the outputs of the beam splitter are detected by a photodiode, and the difference between the signals is registered by a balanced detector. It turned out that the output signal whose power is proportional to the square root of LO power, $\sqrt{P_{LO}}$, carries the information about the initial signal. In addition, subtraction of the signals results in reduction of noise components, whereas the amplification scheme installed in the balanced detector is used for further amplification of its response.

In the case of homodyne detection, the signal frequency ω_s and the LO frequency ω_{LO} are equal. The constant signal level that will be observed is determined by the phase difference between the initial signal and the LO, $\Delta\phi = \phi_s - \phi_{LO}$. For instance, when the constant signal on the oscilloscope is positive at zero phase difference, it will be negative provided the phase difference equals π . More precisely, in the absence of noise, the output of the detector is proportional to the difference between the photocurrents registered by the photodiodes and can be written in the following form [6]:

$$I(t) = I_1(t) - I_2(t) = 2R(\lambda)G\sqrt{P_s(t)P_{LO}} \cos \Delta\phi = 2R(\lambda)GCE_s(t)E_{LO} \cos \Delta\phi, \quad (2)$$

where $R(\lambda)$ is the responsivity of photodiodes; G is the electronic gain of balanced detector; $C = S/(2\xi)$ is the ratio of the effective beam area S and the doubled impedance ξ of the medium; E_s and E_{LO} are the amplitudes of the initial signal field and the LO, respectively.

In the case of heterodyning with $\omega_s \neq \omega_{LO}$, the intensities of the mix of two harmonic signals contain harmonics oscillating at the difference and the sum frequencies: $\omega_- = \omega_s - \omega_{LO}$ and $\omega_+ = \omega_s + \omega_{LO}$. Since both the optical and the sum frequencies are much larger than the bandwidth of any existing photodiode, the photodetectors are unable to register these high frequency harmonics. Therefore, the output of the balanced detector will be the electrical signal of the difference frequency ω_- that stores the information about the phase of the initial signal [43, 44]. This approach allows detecting two quadrature components at once, since the receiver now does not need to set any phase of the local oscillator. The output photocurrent is given by

$$I(t) = 2R(\lambda)G\sqrt{P_s(t)P_{LO}} \cos (\omega_- t + \Delta\phi). \quad (3)$$

3.2. Coherent detection with single quadrature selection

In this section we describe the coherent detection scheme with single quadrature selection for the SCW QKD system. We keep the Alice's block identical to the original sender block of the system [24] and change the block of Bob by replacing the single photon detector with the balanced detector (see Fig. 2) [29].

SCW coherent detection is functionally similar to conventional homodyne detection described in the previous section. By contrast to the homodyne detection scheme, as is illustrated in Fig. 3a (3b), the phase modulator in the Bob's module plays the role of the 50/50 beam splitter. After the second modulation the interference is observed at frequencies $\omega_k = \omega + k\Omega$ provided that Alice and Bob use the microwave modulating field with identical frequencies and the phases φ_A and φ_B , respectively. An important point is that the detection result will depend on the phase difference $\Delta\varphi \equiv \varphi_A - \varphi_B$.

In other words, the local oscillator is not used directly as a separate source. SCW homodyning occurs as a result of redistribution of the energy between the intense carrier mode and the weak sidebands, as if a strong coherent beam is mixed with them at a beam splitter. It turns out that the power of subcarrier wave can be either higher or lower than the carrier wave power depending on the phase difference $\Delta\varphi$. These cases of the phase dependent energy redistribution can be interpreted in terms of the interference that might be either constructive or destructive, respectively.

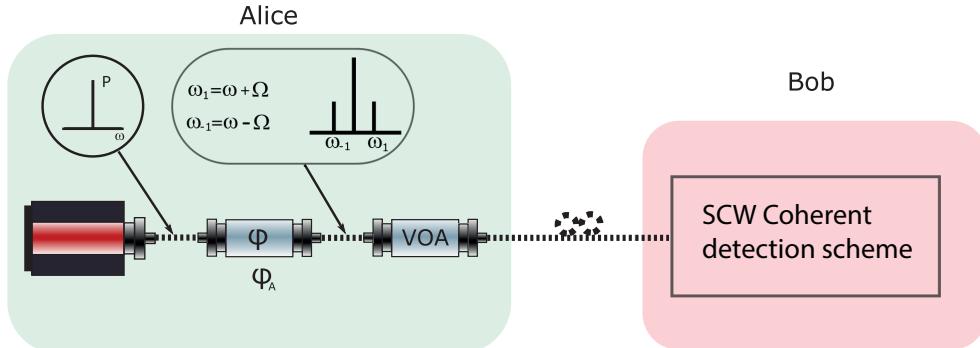


Fig. 2. Principal scheme of SCW CV-QKD setup. The electro-optic phase modulator is denoted by φ ; VOA is the variable optical attenuator. Diagrams in circles show the simplified power spectrum.

Our system is calibrated in such way that the differences in power between the sidebands and the carrier mode at $\Delta\varphi = 0$ and $\Delta\varphi = \pi$ are approximately of the same magnitude. A narrow spectral filter then separates the carrier from the sidebands. After that, the sidebands and the central mode are transmitted through the two arms of the balanced detector through the circulator. Finally, the outputs (the carrier and the sidebands) are detected by two different photodiodes, and their photocurrents are subtracted. Thus, one can extract information encoded in the oscillating signal phase. Similar to the conventional homodyne detection in QKD, Bob measures only one quadrature component at a time by selecting the phase of the microwave field from the set of $\varphi_B \in \{0, \pi/2\}$.

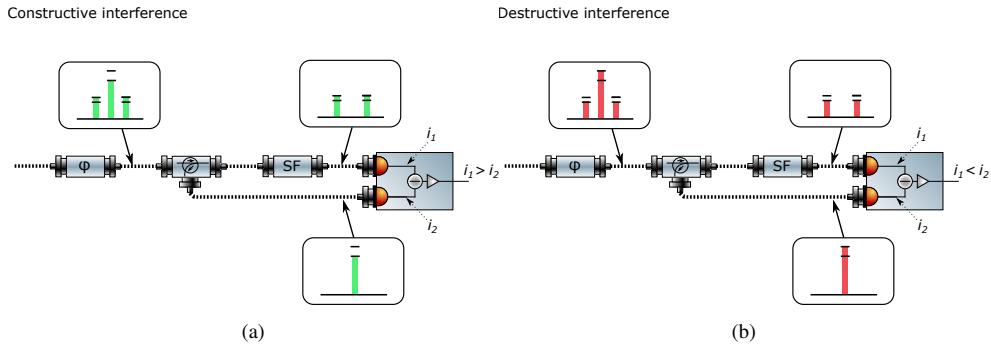


Fig. 3. SCW coherent detection scheme. SF is the spectral filter that cuts off the carrier. The charts show the energy distribution between the carrier and the subcarriers for (a) constructive and (b) destructive interference.

Now we describe a simple classical model (quantum considerations can be found in [29]) of the above homodyne-like coherent detection scheme. The traveling wave phase modulator on the Bob's side generally differs from the Alice's modulator both in the modulation index, $m_B \neq m_A$, and in the phase, $\varphi_B \neq \varphi_A$, thus introducing the phase difference $\Delta\varphi = \varphi_A - \varphi_B$. The expression for the output field emerging after the second modulator $E'(t)$

$$E'(t) = E_0 e^{i\omega t} e^{im_A \cos(\Omega t + \varphi_A)} e^{im_B \cos(\Omega t + \varphi_B)} \quad (4)$$

can be simplified with the help of identities

$$m_A \cos(\Omega t + \varphi_A) + m_B \cos(\Omega t + \varphi_B) = m \cos(\Omega t + \phi), \quad (5a)$$

$$m = \sqrt{m_A^2 + m_B^2 + 2m_A m_B \cos(\varphi_A - \varphi_B)}, \quad (5b)$$

$$m e^{i\phi} = m_A e^{i\varphi_A} + m_B e^{i\varphi_B}, \quad (5c)$$

where m can be regarded as an effective modulation index describing the wave emerging after two modulators. This index depends on the phase difference $\varphi_A - \varphi_B$, whereas the modulation indices m_A and m_B are both phase independent.

Similar to Eq. (1), the output field can now be written in the form of the Jacobi-Anger expansion:

$$E'(t) = E_0 e^{i\omega t} \sum_{k=-\infty}^{\infty} i^k J_k(m) e^{ik\phi} e^{ik\Omega t} \equiv \sum_{k=-\infty}^{\infty} E_k e^{ik\Omega t}, \quad E_k = E_0 e^{i\omega t} i^{|k|} J_{|k|}(m) e^{ik\phi}. \quad (6)$$

The carrier wave is separated from the sidebands using spectral filtering in the Bob's module. For simplicity, we shall neglect the losses and imperfection of the spectral filter. So, we can single out the component at the central frequency to obtain the following expressions for the fields in two arms of the detector

$$E_1(t) = E_0 e^{i\omega t} J_0(m), \quad E_2(t) = \sum_{\substack{k=-\infty, \\ k \neq 0}}^{\infty} E_k e^{ik\Omega t}. \quad (7)$$

Now we can closely follow the line of reasoning leading to Eq. (2), and obtain the time averaged difference of the photocurrents in the form

$$I = R(\lambda) G C \langle |E_2(t)|^2 - |E_1(t)|^2 \rangle_t = R(\lambda) G C E_0^2 (1 - 2J_0^2(m)), \quad (8)$$

where $\langle \dots \rangle_t = \tau^{-1} \int_0^\tau \dots dt$, $\tau = 2\pi/\Omega$. Using temporal averaging assumes that the detectors are insensitive to harmonics of intensities $|E_1(t)|^2$ and $|E_2(t)|^2$ oscillating at radio frequencies. Note that modulation keeps the amplitude of the phase-modulated wave (4) unchanged with $|E'(t)|^2 = E_0^2$, so that Eq. (6) leads to the unitarity condition $\sum_{k=-\infty}^{\infty} J_k^2(m) = 1$ used in derivation of the right-hand side of formula (8).

When the phase difference $\Delta\varphi = \varphi_A - \varphi_B$ is changed, the modulation index m varies between its minimal value $m_{\min} = |m_B - m_A|$ at $\cos(\varphi_A - \varphi_B) = -1$ to the maximal index of modulation $m_{\max} = m_B + m_A$ at $\cos(\varphi_A - \varphi_B) = 1$. In the case where Alice sends non-modulated wave with $m_A = 0$, the output voltage (8) will be zero provided the Bob's index of modulation is adjusted to meet the condition: $J_0(m_B) = 1/\sqrt{2}$ giving $m_B \approx 1.13$.

Figure 4 shows the curves representing dependence of the output voltage on the phase shift φ_A for the in-phase component I and the quadrature component Q that are computed at $\varphi_B = 0$ and $\varphi_B = \pi/2$, respectively. In our calculations, the parameters are taken to be close to those used in the experiments verifying our model. These are: the carrier wave power is $P_c = 10 \mu\text{W}$; the modulation index of Alice is $m_A = 0.09$; the responsivity of the photodiodes is $R = 0.6$; and the additional gain of the detectors is $G = 4 \times 10^3$.

In order to draw analogy between the proposed scheme and conventional homodyne detection, we assume that the temporally averaged intensities $\langle |E_1(t)|^2 \rangle_t$ and $\langle |E_2(t)|^2 \rangle_t$ of the carrier and the subcarrier waves at the output of Alice's modulator correspond to the amplitudes of the

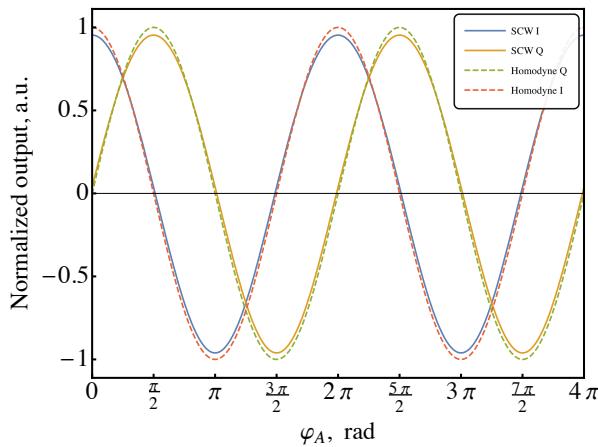


Fig. 4. The in-phase (I) and the quadrature (Q) components of the normalized output signals from the SCW coherent detection scheme (see Eq. (9)) and the classical homodyne scheme.

signal and reference waves: $E_s = E_0 \sqrt{1 - J_0^2(m_A)}$ and $E_{LO} = E_0 J_0(m_A)$. Then, for the classical homodyne scheme, the curves for the normalized output (2) $I/I_{\max} = \cos(\Delta\varphi)$ are plotted in Figure 4. It can be seen that the normalized output signal (8) for our scheme

$$\frac{I}{I_{\max}} = \frac{1 - 2J_0^2(m)}{2J_0(m_A) \sqrt{1 - J_0^2(m_A)}} \quad (9)$$

agrees closely with the predictions of the classical homodyne scheme.

3.3. Simultaneous selection of both quadrature component

An important point is that it is possible to construct an optical phase-diversity coherent detection scheme. In this scheme, the receiver is similar to 90° optical hybrid and both the quadrature components can be measured simultaneously. The principal scheme of SCW CV-QKD setup utilizing such a receiver is shown in Figure 5. In this setup, the beam splitter is combined with the two coherent detection schemes where the electro-optic phase modulators are displaced in phase by 90° .

By using the detection scheme depicted in Figure 5, we can measure the two output signals, $E_{1I}(t)$ and $E_{2I}(t)$, from the top arm of the detector with the phase $\varphi_B = 0$, whereas the output signals, $E_{1Q}(t)$ and $E_{2Q}(t)$, from the bottom arm emerge from the detector with the phase $\varphi_B = \pi/2$. Then the output currents after the balanced detectors are converted to the voltages $V_{I,Q}$.

Assuming that the beam splitter dividing the signal in half is ideal and insertion losses are negligible, it is rather straightforward to extend our model presented in the Sec. 3.2 to the case of doubled detection shown in Figure 5. In this case, we can use Eq. (8) to obtain the outputs of the detectors related to quadratures I and Q in the form:

$$I_{I,Q} = \frac{1}{2} R(\lambda) G C E_0^2 (1 - 2J_0^2(m_{I,Q})), \quad (10)$$

where $m_I = m|_{\varphi_B=0}$ and $m_Q = m|_{\varphi_B=\pi/2}$. Note, that since this approach introduces additional 3 dB loss at the detection stage, its QKD security should be carefully analyzed.

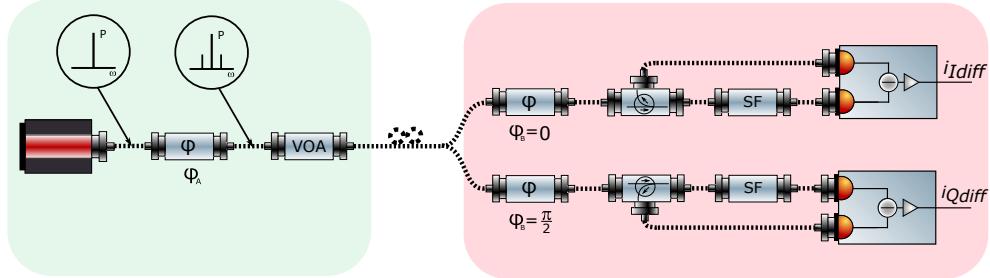


Fig. 5. Principal scheme of SCW CV-QKD setup with phase-diversity coherent receiver.

So, by using these two balanced detectors we can perform simultaneous I/Q measurements. In such measurements, analysis of the experimental results is reduced to obtaining a constellation diagram that will be detailed in Section 4.

3.4. Heterodyne detection

Another well-known method to obtain information about the complex amplitude of the optical fields is heterodyne detection [3, 6, 45–48]. In this section we show how a heterodyne-type detection scheme can be adopted for quadrature phase-coded multimode signals. The mode of operation of our coherent detection scheme demonstrating versatility of the SCW method is described in Figure 6. Note also that such scheme promises significant simplification of implementation.

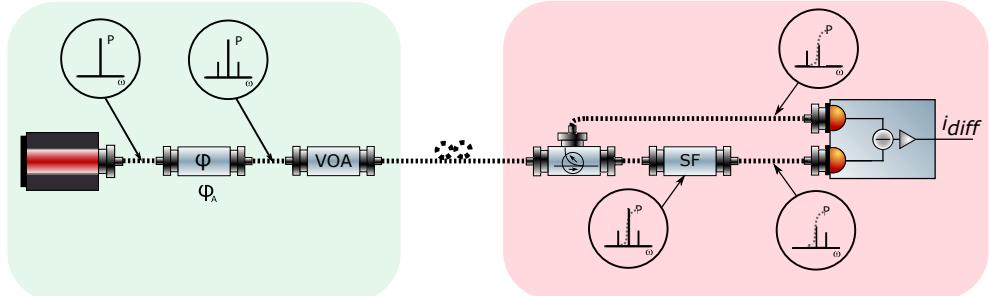


Fig. 6. Principal scheme of SCW CV-QKD setup with heterodyne detection. Examples of power spectra are shown in encircled diagrams and i_{diff} stands for the output photocurrent.

As is shown in Figure 6, similar to the scheme presented in Figure 2, the only component changed in the initial system [24, 25] is the Bob's block whose detection scheme is no longer using the phase modulator. In this scheme spectral filtering is used to mix the carrier wave with the upper and the lower sidebands where subcarrier frequencies are higher and below the carrier frequency ω . For this purpose, the spectral filter bandpass is chosen so as to pass light at the frequency $\omega + \Omega$ and to halve the intensity of the carrier at the frequency ω , whereas the rest of light is reflected back. In other words, the transparency of the spectral filter, T , should meet the conditions: $T(\omega) \approx 0.5$, $T(\omega - \Omega) \rightarrow 0$ and $T(\omega + \Omega) \rightarrow 1$.

From Eq. (1) we obtain the fields in the separate arms in the following form:

$$E_1(t) = E_0 e^{i\omega t} \left(\sum_{k=1}^{\infty} i^k J_k(m_A) e^{ik(\Omega t + \varphi_A)} + \sqrt{0.5} J_0(m_A) \right), \quad (11)$$

$$E_2(t) = E_0 e^{i\omega t} \left(\sum_{k=1}^{\infty} i^k J_k(m_A) e^{-ik(\Omega t + \varphi_A)} + \sqrt{0.5} J_0(m_A) \right), \quad (12)$$

where we have used the identity $J_{-\alpha}(x) = (-1)^\alpha J_\alpha(x)$ for the Bessel functions. When the modulation index m_A is small, we can apply the lowest order approximation that takes into account only the first order subcarriers

$$E_1(t) \approx E_0 (i J_1(m_A) e^{i(\omega_t + \varphi_A)} + \sqrt{0.5} J_0(m_A) e^{i\omega t}), \quad (13)$$

$$E_2(t) \approx E_0 (i J_1(m_A) e^{i(\omega_t - \varphi_A)} + \sqrt{0.5} J_0(m_A) e^{i\omega t}), \quad (14)$$

where $\omega_{\pm} = \omega \pm \Omega$, and derive the output photocurrent in the absence of noise

$$I(t) = R(\lambda) G C (|E_2(t)|^2 - |E_1(t)|^2) = R(\lambda) G C 2 \sqrt{2} E_0^2 J_0(m_A) J_1(m_A) \sin(\Omega t + \varphi_A). \quad (15)$$

Clearly, this result bears a striking resemblance to the classical heterodyning.

As in the previous section, we now discuss this analogy using Eq. (3) with ω and $\Delta\varphi$ replaced by Ω and $\varphi_A + \pi/2$, respectively. For this purpose, we assume that the amplitudes of the signal and reference waves are $E_s = E_0 \sqrt{1 - J_0^2(m_A)}$ and $E_{LO} = E_0 J_0(m_A)$ and compare the output of the classical heterodyne, $I_{\max} \sin(\Omega t + \varphi_A)$, with the signal given in Eq. (15). Figure 7 shows that the normalized output of our scheme

$$\frac{I(t)}{I_{\max}} = \frac{\sqrt{2} J_1(m_A)}{\sqrt{1 - J_0^2(m_A)}} \sin(\Omega t + \varphi_A) \quad (16)$$

turns out to be very close to the output of the classical scheme. It should be stressed that, in this analysis, the detectors are assumed to be sensitive to the radio frequency Ω .

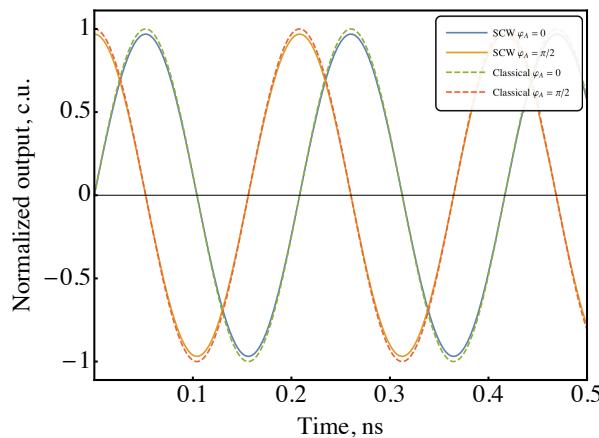


Fig. 7. Time dependence of the normalized heterodyne-derived signals for the SCW and the classical detection schemes.

Demodulation of the received signal can be carried out by standard telecommunication methods using a quadrature synchronous demodulator [6,49–52]. The demodulator setup allows one to observe the in-phase (initial) and quadrature (shifted by $\pi/2$ using a voltage generator) signal components simultaneously on the analyzer and thus extract the information on the phase selected by Alice.

The main disadvantage of this method is the need to find a balance between the capabilities of spectral filters and balanced detectors. On the one hand, an increase of modulation frequency Ω leads to the growth of required detector's bandwidth, what results in extra electronic noises [53]. Usually bandwidth of balanced detectors used for quantum measurements is less than 1 GHz [54]. On the other hand, low modulation frequencies perplex subcarriers' spectral filtering. Thus one of the main challenges for practical implementation of such scheme is to find an optimal modulation frequency that satisfies both of these conditions.

4. Experimental results

In this section we present the results of our experiments verifying the theoretical models presented in the previous section. For the homodyne-like detection setup shown in Figure 2, our proof-of-principle experiment have used a 1550 nm $10 \mu\text{W}$ fiber-coupled laser directed into the LiNbO₃ electro-optic phase modulator with the electrical signal frequency $\Omega = 4.8 \text{ GHz}$. The modulation index m_B is adjusted to maximize the difference between the results for different values of $\Delta\varphi$ and the phase dependence of the output voltage is expected to be nearly harmonic (see Figure 4). After the second modulation the spectral components are transmitted through the circulator to a fiber Bragg grating spectral filter. In the core of the fiber Bragg grating filter the refractive index periodically changes in the longitudinal direction, and the spectral selectivity of reflection from fiber Bragg gratings is due to diffraction by periodic optical inhomogeneities. The sideband components are transmitted through the filter to the first arm. The filter reflects the component at the central frequency back to the circulator. After passing the circulator, the reflected carrier wave propagates in the second arm of the balanced detector. The two output ports of the circulator are coupled to the input ports of a self-developed balanced detector (the measurement bandwidth is 100 MHz, the gain is $G = 4 \cdot 10^3$ and the responsivity is $R = 0.6$).

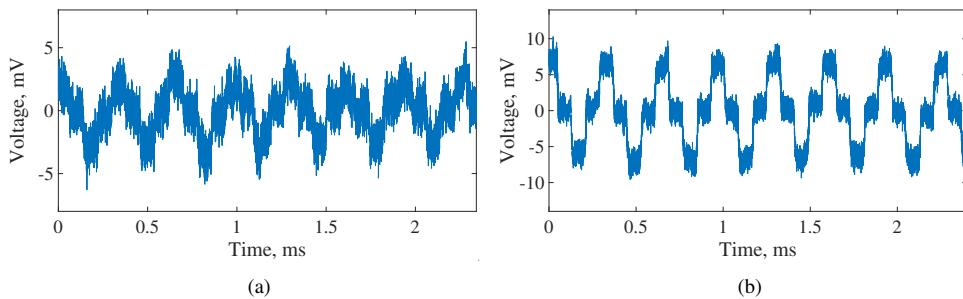


Fig. 8. Time dependence of the output voltage for the homodyne-like coherent detection scheme shown in Fig. 2. The extreme points correspond to the constructive and destructive interference. The phase difference $\Delta\varphi$ varies periodically in time switching between the values from a discrete set: $\{0, \pi/2, \pi, 3\pi/2\}$. Two cases are shown: (a) $P_c = 9.96 \mu\text{W}$, $P_s = 40.00 \text{ nW}$; and (b) $P_c = 9.5 \mu\text{W}$, $P_s = 500.00 \text{ nW}$.

Figure 8 presents the output voltage measured in relation of time when the phase difference (the phase φ_A is set to be zero), $\Delta\varphi$, undergoes time-periodic piecewise changes between the states with equidistant values from a discrete set $\{0, \pi/2, \pi, 3\pi/2\}$. Referring to Fig. 8a, it can be seen that, in the case where the carrier wave power after the modulation was $P_c = 9.96 \mu\text{W}$ and the total power of the subcarriers was $P_s = 40.00 \text{ nW}$, variations of the voltage level are almost indiscernible. By contrast, Figure 8b demonstrates the case with unambiguously distinguishable voltage levels that occurs at $P_c = 9.5 \mu\text{W}$ and $P_s = 500.00 \text{ nW}$. Thus, our coherent detection scheme is sufficiently sensitive to estimate the phase of the quadrature phase-coded multimode signals from the electro-optic phase modulator.

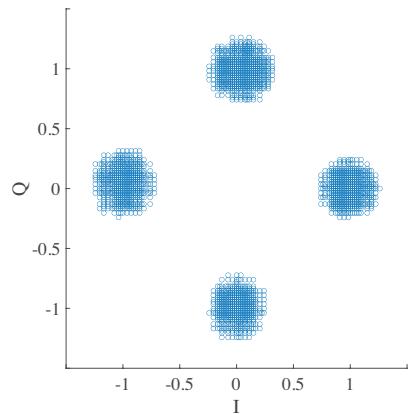


Fig. 9. 4-PSK constellation diagram recovered from the phase-modulated optical signal, $P_c = 9.5 \mu\text{W}$, $P_s = 500.00 \text{nW}$.

We have also performed the experiment for the optical phase-diversity coherent receiver sketched in Figure 5. The 4-PSK constellation diagram recovered from the phase-modulated optical signal using the optical phase-diversity coherent receiver is depicted in Figure 9.

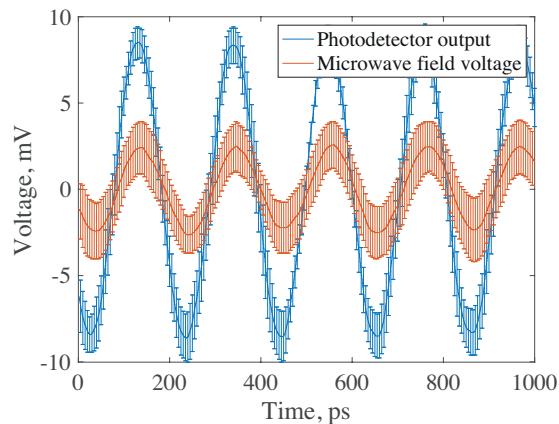


Fig. 10. Time dependence of microwave field voltage and the output voltage for balanced detector's single arm ($P_c = 225.00 \mu\text{W}$, $P_s = 146.50 \mu\text{W}$) using the SCW heterodyning. Mean values are indicated along with standard deviations.

In order to test the heterodyne scheme (see Figure 6), we need to get around the above-mentioned difficulties concerning the frequency bandwidth. For this purpose, we have utilized the photodetector with 6.17 GHz bandwidth in the single arm of the scheme described in Figure 6 to obtain the signal at the intermediate frequency. The measured curves for the output voltage and the microwave field are presented in Figure 10. The results show that the signal light is down-converted to the intermediate frequency coincident with the frequency of the microwave field used in the electro-optic phase modulator.

5. Conclusion

In this paper we have applied several approaches to put coherent detection schemes into the framework of the subcarrier wave QKD systems. In our homodyne-like coherent detection schemes (see Sec. 3.2 and Sec. 3.3), the phase-modulated light emerging from the Bob's modulator is splitted into the carrier and the subcarrier waves and the output signal is determined by the difference between the responses of the photodiodes to the light of these two waves. By contrast, in our heterodyne-type detection scheme described in Sec. 3.4 the light modulated by Alice is directly used as the input wave. This wave, similar to the homodyne-like scheme, is divided into two waves. But, in contrast to this scheme, these waves are obtained by filtering out either the lower or the upper sidebands. In this case, we have shown that the differential signal which is oscillating with the microwave frequency can be used to extract the information about the phase encoded by Alice.

In our theoretical considerations we have presented simple classical models emphasizing the analogy between the suggested coherent detection schemes and the standard homodyne/heterodyne methods. Interestingly, quantum considerations of our previous work [29] being necessary to perform security analysis can be related to the classical approach presented in Sec. 3.2. To this end, we begin with the modulated quantum state after Bob's modulator written in the form (see Ref. [34] for details)

$$|\Psi\rangle = V|\alpha_{\text{in}}\rangle = \otimes_{\nu=-S}^S |\alpha_\nu\rangle \equiv |\alpha_0\rangle \otimes |\alpha\rangle_{SB}, \quad (17)$$

$$\alpha_\nu = M_{\nu 0}^* \alpha_{\text{in}}, \quad |\alpha\rangle_{SB} = \otimes_{\nu \neq 0} |\alpha_\nu\rangle, \quad (18)$$

where $|\alpha_{\text{in}}\rangle$ is the input coherent state of the Alice's modulator and the matrix elements of the evolution operator $M_{\nu 0}$ are described in [34] and, in the large S limit, are given by

$$|M_{\nu 0}(\beta)|^2 \approx J_\nu^2(m), \quad m^2 \approx m_A^2 + m_B^2 + 2m_A m_B \cos(\varphi_A - \varphi'_B), \quad \varphi'_B = \varphi_B - \varphi_0. \quad (19)$$

Following the line of reasoning presented in Refs. [55, 56], it can be shown that the difference of photocounts follows the Skellam distribution

$$P(k) = e^{-\mu_{SB}-\mu_0} \left(\frac{\mu_{SB}}{\mu_0} \right)^k I_{|k|}(2\sqrt{\mu_0 \mu_{SB}}), \quad k = k_{SB} - k_0 \in \mathbb{Z},$$

$$\mu_0 = \xi |\alpha_0|^2, \quad \mu_{SB} = \sum_{\nu \neq 0} \xi_\nu |\alpha_\nu|^2, \quad (20)$$

where I_k is the k -order modified Bessel function of the first kind; ξ_μ is the efficiency of the photodetector for the μ th mode (for simplicity, we shall assume that the efficiency is independent of μ so that $\xi_\mu = \xi$). It is known that, under certain conditions, the above distribution can be approximated by the normal (Gaussian) distribution

$$P(k) \approx \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(k - \langle k \rangle)^2}{2\sigma^2}\right), \quad (21)$$

determined by the mean value

$$\langle k \rangle = \mu_{SB} - \mu_0 = \xi(1 - 2|M_{00}|^2)|\alpha_{\text{in}}|^2, \quad (22)$$

and the variance

$$\sigma^2 = \mu_{SB} + \mu_0 = \xi|\alpha_{\text{in}}|^2. \quad (23)$$

When $|M_{00}|^2 \approx J_0^2(m)$, we arrive at the conclusion that the mean value $\langle k \rangle$ is proportional to the difference of photocurrents given by Eq. (8).

Our experimental results clearly demonstrate practical feasibility of the presented detection schemes. Further development will require a more sophisticated and detailed analysis of these schemes using the methods of quantum optics. This will allow their legitimate employment in quantum computing, quantum cryptography, and quantum tomography. The concluding remark is that our continuous variable version of the SCW method can be regarded as an alternative to the method suggested in [30] and, in addition, the CV-SCW approach was recently demonstrated to be useful for designing quantum random number generators [57].

Acknowledgements

This work was funded by Government of Russian Federation (Grant No. MK-777.2020.8).

Disclosures

The authors declare no conflicts of interest.

References

1. L. I. Anderson, *Nicola Tesla: Lecture Before the New York Academy of Sciences - April 6, 1897* (Twenty First Century Books, 1994).
2. B. Roger and H. Georges, "Double heterodyne radio receiver," (1952). US Patent 2,606,285.
3. V. V. Protopopov, *Laser Heterodyning* (Springer Berlin Heidelberg, 2009).
4. D.-S. Ly-Gagnon, S. Tsukamoto, K. Katoh, and K. Kikuchi, "Coherent detection of optical quadrature phase-shift keying signals with carrier phase estimation," *J. Light. Technol.* **24**, 12 (2006).
5. S. Tanosaki, Y. Sasaki, M. Takagi, A. Ishikawa, H. Inage, R. Emori, J. Suzuki, T. Yuasa, H. Taniguchi, B. Devaraj *et al.*, "In vivo laser tomographic imaging of mouse leg by coherent detection imaging method," *Opt. Rev.* **10**, 447–451 (2003).
6. K. Kikuchi, "Fundamentals of coherent optical fiber communications," *J. Light. Technol.* **34**, 157–179 (2015).
7. A. Mecozzi and M. Shtaif, "Coherent detection with an incoherent local oscillator," *Opt. Express* **26**, 33970–33981 (2018).
8. Y. Lu, T. Zhu, L. Chen, and X. Bao, "Distributed vibration sensor based on coherent detection of phase-OTDR," *J. Light. Technol.* **28**, 3243–3249 (2010).
9. H. P. Yuen and V. W. Chan, "Noise in homodyne and heterodyne detection," *Opt. Lett.* **8**, 177–179 (1983).
10. A. Barchielli, "Direct and heterodyne detection and other applications of quantum stochastic calculus to quantum optics," *Quantum Opt. J. Eur. Opt. Soc. Part B* **2**, 423 (1990).
11. S. Wallentowitz and W. Vogel, "Unbalanced homodyning for quantum state measurements," *Phys. Rev. A* **53**, 4528 (1996).
12. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature* **421**, 238–241 (2003).
13. T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, "Quantum cryptography using pulsed homodyne detection," *Phys. Rev. A* **68**, 042331 (2003).
14. A. Leverrier and P. Grangier, "Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation," *Phys. Rev. A* **83**, 042312 (2011).
15. M. Heid and N. Lütkenhaus, "Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction," *Phys. Rev. A* **73**, 052316 (2006).
16. K. Brádler and C. Weedbrook, "Security proof of continuous-variable quantum key distribution using three coherent states," *Phys. Rev. A* **97**, 022310 (2018).
17. P. Papanastasiou, C. Lupo, C. Weedbrook, and S. Pirandola, "Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels," *Phys. Rev. A* **98**, 012340 (2018).
18. S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation," *Phys. Rev. X* **9**, 021059 (2019).
19. J. Lin, T. Upadhyaya, and N. Lütkenhaus, "Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution," *Phys. Rev. X* **9**, 041064 (2019).
20. G. Zhang, J. Haw, H. Cai, F. Xu, S. Assad, J. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu *et al.*, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," *Nat. Photonics* **13**, 839–842 (2019).
21. Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Phys. Rev. Lett.* **125**, 010502 (2020).
22. J.-M. Merolla, Y. Mazurenko, J.-P. Goedgebuer, H. Porte, and W. T. Rhodes, "Phase-modulation transmission system for quantum cryptography," *Opt. Lett.* **24**, 104–106 (1999).
23. J. Mora, A. Ruiz-Alba, W. Amaya, A. Martínez, V. García-Muñoz, D. Calvo, and J. Capmany, "Experimental demonstration of subcarrier multiplexed quantum key distribution system," *Opt. Lett.* **37**, 2031–2033 (2012).

24. A. Gleim, V. Egorov, Y. V. Nazarov, S. Smirnov, V. Chistyakov, O. Bannik, A. Anisimov, S. Kynev, A. Ivanova, R. Collins *et al.*, “Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference,” *Opt. Express* **24**, 2619–2633 (2016).
25. G. Miroshnichenko, A. Kozubov, A. Gaidash, A. Gleim, and D. Horoshko, “Security of subcarrier wave quantum key distribution against the collective beam-splitting attack,” *Opt. Express* **26**, 11292–11308 (2018).
26. A. Gaidash, A. Kozubov, and G. Miroshnichenko, “Methods of decreasing the unambiguous state discrimination probability for subcarrier wave quantum key distribution systems,” *JOSA B* **36**, B16–B19 (2019).
27. V. Chistiakov, A. Kozubov, A. Gaidash, A. Gleim, and G. Miroshnichenko, “Feasibility of twin-field quantum key distribution based on multi-mode coherent phase-coded states,” *Opt. Express* **27**, 36551–36561 (2019).
28. S. M. Kynev, V. V. Chistyakov, S. V. Smirnov, K. P. Volkova, V. I. Egorov, and A. V. Gleim, “Free-space subcarrier wave quantum communication,” *J. Physics: Conf. Ser.* **917**, 052003 (2017).
29. E. Samsonov, R. Goncharov, A. Gaidash, A. Kozubov, V. Egorov, and A. Gleim, “Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis,” *Sci. Reports* **10**, 10034 (2020).
30. J. Fang, P. Huang, and G. Zeng, “Multichannel parallel continuous-variable quantum key distribution with gaussian modulation,” *Phys. Rev. A* **89**, 022315 (2014).
31. L. Gyongyosi and S. Imre, “Subcarrier domain of multicarrier continuous-variable quantum key distribution,” *J. Stat. Phys.* **177**, 960–983 (2019).
32. Y. Wang, Y. Mao, W. Huang, D. Huang, and Y. Guo, “Optical frequency comb-based multichannel parallel continuous-variable quantum key distribution,” *Opt. Express* **27**, 25314–25329 (2019).
33. S. Haykin, *Communication systems* (John Wiley & Sons, 2008).
34. G. P. Miroshnichenko, A. D. Kiselev, A. I. Trifanov, and A. V. Gleim, “Algebraic approach to electro-optic modulation of light: exactly solvable multimode quantum model,” *JOSA B* **34**, 1177–1190 (2017).
35. J. Capmany and C. R. Fernández-Pousa, “Quantum model for electro-optical phase modulation,” *JOSA B* **27**, A119–A129 (2010).
36. P. Kumar and A. Prabhakar, “Evolution of quantum states in an electro-optic phase modulator,” *IEEE J. Quantum Electron.* **45**, 149–156 (2008).
37. A. Yariv and P. Yeh, *Optical waves in crystals*, vol. 5 (Wiley New York, 1984).
38. N. G. Gonzalez, D. Zibar, X. Yu, and I. T. Monroy, “Optical phase-modulated radio-over-fiber links with k-means algorithm for digital demodulation of 8psk subcarrier multiplexed signals,” in *Optical Fiber Communication Conference*, (Optical Society of America, 2010), p. OML3.
39. I. Gasulla and J. Capmany, “Phase-modulated radio over fiber multimode links,” *Opt. Express* **20**, 11710–11717 (2012).
40. Y. Zhang, K. Xu, R. Zhu, J. Li, J. Wu, X. Hong, and J. Lin, “Photonic dpask/qam signal generation at microwave/millimeter-wave band based on an electro-optic phase modulator,” *Opt. Lett.* **33**, 2332–2334 (2008).
41. T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru, “Implementation of continuous-variable quantum key distribution with discrete modulation,” *Quantum Sci. Technol.* **2**, 024010 (2017).
42. A. Leverrier, “Theoretical study of continuous-variable quantum key distribution,” Ph.D. thesis, Télécom ParisTech (2009).
43. M. Yoshida, H. Goto, K. Kasai, and M. Nakazawa, “64 and 128 coherent qam optical transmission over 150 km using frequency-stabilized laser and heterodyne pll detection,” *Opt. Express* **16**, 829–840 (2008).
44. J. Hongo, K. Kasai, M. Yoshida, and M. Nakazawa, “1-Gsymbol/s 64-QAM coherent optical transmission over 150 km,” *IEEE Photonics Technol. Lett.* **19**, 638–640 (2007).
45. H. Gebbie, N. Stone, E. Putley, and N. Shaw, “Heterodyne detection of sub-millimetre radiation,” *Nature* **214**, 165–166 (1967).
46. A. Maznev, K. Nelson, and J. A. Rogers, “Optical heterodyne detection of laser-induced gratings,” *Opt. Lett.* **23**, 1319–1321 (1998).
47. D. L. Fried, “Optical heterodyne detection of an atmospherically distorted signal wave front,” *Proc. IEEE* **55**, 57–77 (1967).
48. O. DeLange, “Optical heterodyne detection,” *IEEE Spectr.* **5**, 77–85 (1968).
49. M. Bylina, S. Glagolev, and A. Diubov, “Comparative analysis of direct and coherent detection methods for digital information optical signals. Part 2. Coherent detection,” *Proc. Telecommun. Univ.* **3**, 21–28 (2017).
50. C. Wang, Y. Qu, and Y. P. T. Tang, “IQ quadrature demodulation algorithm used in heterodyne detection,” *Infrared Phys. & Technol.* **72**, 191–194 (2015).
51. R. Bohme and M. Eichin, “Heterodyne receiver with synchronous demodulation for receiving time signals,” (1999). US Patent 5,930,697.
52. Y.-K. Chen, U.-V. Koc, and A. Leven, “Optical heterodyne receiver and method of extracting data from a phase-modulated input optical signal,” (2010). US Patent 7,650,084.
53. Y.-M. Chi, B. Qi, W. Zhu, L. Qian, H.-K. Lo, S.-H. Youn, A. Lvovsky, and L. Tian, “A balanced homodyne detector for high-rate gaussian-modulated coherent-state quantum key distribution,” *New J. Phys.* **13**, 013003 (2011).
54. X. Tang, R. Kumar, S. Ren, A. Wonfor, R. Penty, and I. White, “Performance of continuous variable quantum key distribution system at different detector bandwidth,” *Opt. Commun.* p. 126034 (2020).

55. W. Vogel and J. Grabow, "Statistics of difference events in homodyne detection," *Phys. Rev. A* **47**, 4227 (1993).
56. M. Bina, A. Allevi, M. Bondani, and S. Olivares, "Homodyne-like detection for coherent state-discrimination in the presence of phase noise," *Opt. Express* **25**, 10685–10692 (2017).
57. E. Samsonov, B. Pervushin, A. Ivanova, A. Santev, V. Egorov, S. Kynev, and A. Gleim, "Vacuum-based quantum random number generator using multi-mode coherent states," *Quantum Inf. Process.* **19**, 1–11 (2020).

Quantum random number generator using vacuum fluctuations

B. E. Pervushin¹, M. A. Fadeev^{1,2}, A. V. Zinovev¹, R. K. Goncharov¹, A. A. Santev¹,
A. E. Ivanova^{1,2}, E. O. Samsonov^{1,2}

¹ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia

²Quanttelecom LLC, 6 liniya, Vasilievsky island d.59, korp. 1, lit. B, St. Petersburg, 199178, Russia

borispermushin@itmo.ru, wertsam@itmo.ru, avzinovev15@yandex.ru, rkgoncharov@itmo.ru, aasantev@itmo.ru,
aeivanova@itmo.ru, eosamsonov@itmo.ru

PACS 03.67.-a

DOI 10.17586/2220-8054-2021-12-2-156-160

Experimental implementation of a quantum random number generator based on vacuum fluctuation is presented in this paper. A Y-splitter is used in optical setup of the quantum random number generator. The generation of random numbers in real time with a speed of 300 Mb/s is demonstrated. The conditional minimum entropy is used to estimate the randomness. A cryptographic hashing function is used for post-processing. The resulting sequence has passed DieHard and NIST statistical tests successfully.

Keywords: quantum random number generation, homodyne detection, vacuum fluctuation.

Received: 1 March 2021

Revised: 4 March 2021

1. Introduction

There is a demand for random numbers in many fields of science and technology [1–4]. Existing random number generators (RNG) can be divided into two groups: pseudo-random [5] and physical [6]. Pseudo-random RNGs are based on the use of mathematical algorithms, the output bit sequences of such generators can be predictable. Physical generators using classical physical processes as a source of entropy can also be potentially predictable due to the determinism inherent in classical processes. Such generators can be used in fields that do not require true randomness. However, for certain tasks, more reliable random number generation devices should be used. In particular, the generation of encryption keys in cryptographic systems requires truly random numbers, which can be obtained only by using a quantum random number generator (QRNG). QRNGs are based on quantum processes, which are nondeterministic. Randomness in such generators can be extracted based on the principle of detecting single photons in different optical modes [7], using entangled photons [8], laser phase noise [9], or measuring fluctuations of vacuum [10, 13]. The last type of QRNGs is of the interest due to the simplicity of implementation, relatively compact size, and high speed of random sequence generation. On-chip implementations of the QRNG have been actively developed, due to small dimensions and stability of work [11, 12]. This paper demonstrates the implementation of a quantum random number generator based on vacuum fluctuations using a Y beam splitter. The presented device provides generation of random numbers in real time at a speed of 300 Mb/s. To determine the unpredictability of the output sequence, an estimate of the conditional minimum entropy was employed using the approach described in [15, 16]. The resulting random sequence was tested using the well-known battery of statistical tests DieHard [17] and NIST [18].

2. Quantum randomness generation system

The result of the interference of the reference field, described by Poisson statistics, and the vacuum field on an optical beam splitter with two input and two output ports is described in operator form in [19], these beam splitters were used in the QRNG based on vacuum fluctuations in a number of works [10, 13, 14]. In this work, for the experimental implementation of QRNG based on vacuum fluctuations, the Y-beam splitter is used, the mathematical substantiation of the possibility of using it is presented in [20, 21]. The QRNG scheme based on vacuum fluctuations is shown in Fig. 1.

In the presented QRNG, laser beam (reference field) is mixed with the vacuum field at a polarizing Y beam splitter [22]. A polarization controller is used to fine-tune the division ratio. Thus, two inputs of the balanced detector receive signals containing an amplified vacuum signal as one of its components, which appears as shot noise as a result of detection.

After detection, the differential photocurrent is amplified using a transimpedance amplifier. The resulting voltage, randomly varying in time, is converted into a numerical sequence by an ADC. An extractor is used to extract a truly

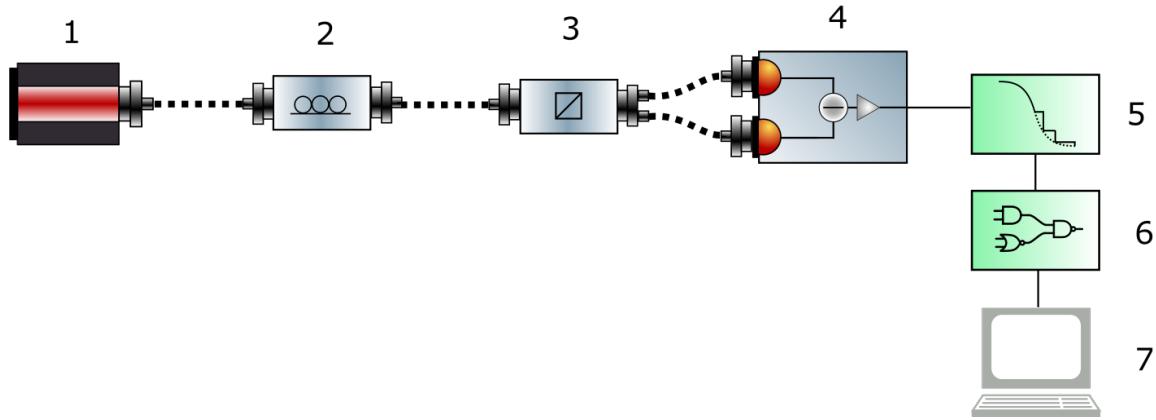


FIG. 1. Scheme of the quantum random number generator based on vacuum fluctuation. 1 – laser; 2 – polarization controller; 3 – Y beam splitter; 4 – balanced detector; 5 – ADC; 6 – FPGA; 7 – computer.

random normally distributed sequence. In particular, to extract a random sequence, an AES-based cryptographic hashing algorithm is used.

3. Experiment

In the proposed experimental implementation, the laser power is set to 40 mW. The reference field is divided on the beam splitter after polarization controller, the total loss of which is 1.06 dB. Two outputs of the Y-splitter are connected to two inputs of a balanced detector, the bandwidth of which is 100 MHz. The electrical signals from the two photodiodes are subtracted and the resulting current is converted to voltage using a transimpedance amplifier. The resulting voltage signal is digitized using a high-speed 8-bit ADC with 100 MHz bandwidth and 150 MHz sampling rate.

The rate of generating a raw sequence of random numbers is:

$$v = \min(\tau^{-1}, 2BW) \cdot n, \quad (1)$$

where τ^{-1} is the ADC measurement frequency, BW is the smallest bandwidth of the analog signal, n is a number of bits per measurement.

From the formula (1) it can be seen that the generation rate is limited by the measurement frequency and the smallest bandwidth in the circuit. Thus, the raw sequence speed is 1200 Mb/s.

Since, in addition to quantum noise, the system contains untrusted electronic noises, it is necessary to estimate the conditional entropy of the source, taking into account that the intruder can control classical noise. For this purpose, the minimum entropy is used, which, in comparison with the Shannon entropy, is a more rigorous estimate and is generally determined by:

$$H_{\min}(M_{dis}) = -\log_2 \left(\max_i p_i \right), \quad (2)$$

where M_{dis} is a measured discrete signal, p_i are probabilities of different measurement outcomes.

When taking into account the eavesdropper, the conditional minimum entropy in our case is [15]:

$$H_{\min}(M_{dis} | E) = -\log_2 \left(\max \left\{ \frac{1}{2} \left[\operatorname{erf} \left(\frac{e_{\max} - R + 3\delta/2}{\sqrt{2}\sigma_q} \right) + 1 \right], \operatorname{erf} \left(\frac{\delta}{2\sqrt{2}\sigma_q} \right) \right\} \right), \quad (3)$$

where R is a half the dynamic range of the ADC, $\delta = R/2^{n-1}$, e_{\max} is a maximum value of the electronic signal, and σ_q is a standard deviation of a quantum signal.

Due to the independence of the quantum and electronic signals, the standard deviation of the quantum signal is defined as:

$$\sigma_m^2 = \sigma_e^2 + \sigma_q^2, \quad (4)$$

where σ_m is a standard deviation of the measured signal (sums of quantum and electronic signals), σ_e is a standard deviation of the electronic signal. In the experimental QRNG system, the minimum entropy of the source was 4.78.

The unpredictability of the resulting bit sequence can be guaranteed by the Leftover Hash Lemma [23]. If the hash function converts k bits to

$$l < k \cdot H_{\min}/n - 2 \log_2(1/\varepsilon), \quad (5)$$

then the output sequence will be ε -close to the uniform distribution. In this case $k = 1024$, $l = 256$, then the security parameter is less than 2^{-177} . A rather strict security parameter was chosen here, since the hashing algorithm used in this work is not universal [15]. The final sequence generation rate is:

$$V = v \text{ Mb/s} \cdot \frac{256}{1024} = 300 \text{ Mb/s}. \quad (6)$$

DieHard and NIST statistical tests were used to check the resulting output sequence. The results are shown in Tables 1 and 2.

TABLE 1. DieHard statistical test results. The obtained p-value for successful passing of the test must lie in the interval $0.025 < \text{p-value} < 0.975$

No.	Test	p-value
1	BIRTHDAY SPACINGS TEST	0.165456
2	THE OVERLAPPING 5-PERMUTATION TEST	0.654752
3	the BINARY RANK TEST for 31x31 matrices BINARY RANK TEST for 32x32 matrices	0.792586
4	BINARY RANK TEST for 6x8 matrices	0.431478
5	THE BITSTREAM TEST	0.437767
6	OPSO	0.427352
	OQSO	0.481557
	DNA	0.482048
7	the COUNT-THE-1's TEST on a stream of bytes	0.095081
8	the COUNT-THE-1's TEST for specific bytes	0.563297
9	THIS IS A PARKING LOT TEST	0.896585
10	THE MINIMUM DISTANCE TEST	0.815571
11	THE 3DSPHERES TEST	0.039996
12	the SQEEZE test	0.134697
13	The OVERLAPPING SUMS test	0.470491
14	the RUNS test	0.290913
15	CRAPS TEST	0.466673

4. Conclusion

The paper describes an experimental implementation of a system for the generation of random numbers in real time, based on vacuum fluctuations. The quantification of unpredictability is determined by the conditional minimum entropy, taking into account the presence of the eavesdropper. The minimum entropy was 4.78. The resulting sequence has successfully passed the NIST and DieHard statistical test batteries. The parameters of the experimental model of the system made it possible to achieve a generation rate of 300 Mb/s.

Conflict of interest

The authors declare no conflicts of interest.

TABLE 2. Results of passing NIST statistical tests. The p-values must be p-value > 0.025 to pass successfully

No.	Test	p-value
1	BIRTHDAY SPACINGS TEST	0.165456
2	THE OVERLAPPING 5-PERMUTATION TEST	0.654752
3	the BINARY RANK TEST for 31x31 matrices BINARY RANK TEST for 32x32 matrices	0.792586
4	BINARY RANK TEST for 6x8 matrices	0.431478
5	THE BITSTREAM TEST	0.437767
6	OPSO	0.427352
	OQSO	0.481557
	DNA	0.482048
7	the COUNT-THE-1's TEST on a stream of bytes	0.095081
8	the COUNT-THE-1's TEST for specific bytes	0.563297
9	THIS IS A PARKING LOT TEST	0.896585
10	THE MINIMUM DISTANCE TEST	0.815571
11	THE 3DSPHERES TEST	0.039996
12	the SQEEZE test	0.134697
13	The OVERLAPPING SUMS test	0.470491
14	the RUNS test.	0.290913
15	CRAPS TEST	0.466673

Acknowledgements

This work was funded by Government of Russian Federation (grant MK-777.2020.8).

References

- [1] Ferrenberg A.M., Landau D.P., et. al. Monte Carlo simulations: Hidden errors from “good” random number generators. *Physical Review Letters*, 1992, **69** (23), 3382.
- [2] Gennaro R. Randomness in cryptography. *IEEE security & privacy*, 2006, **4** (2), P. 64–67.
- [3] Gisin N., Ribordy G., et. al. Quantum cryptography. *Reviews of modern physics*, 2002, **74** (1), 145.
- [4] Metropolis N., Ulam S. The monte carlo method. *Journal of the American statistical association*, 1949, **44** (247), P. 335–341.
- [5] Nisan N., Wigderson A. Hardness vs randomness. *Journal of computer and System Sciences*, 1994, **49** (2), P. 149–167.
- [6] Johnston D. *Random Number Generators – Principles and Practices: A Guide for Engineers and Programmers*. Walter de Gruyter GmbH & Co KG: 2018, 439 p.
- [7] Jennewein T., Achleitner U., et. al. A fast and compact quantum random number generator. *Review of Scientific Instruments*. 2000, **71** (4), P. 1675–1680.
- [8] Pironio S., Acin A., Massar S., et. al. Random numbers certified by Bell’s theorem. *Nature*, 2010, **464** (7291), P. 1021–1024.
- [9] Guo H., Tang W., et. al. Truly random number generation based on measurement of phase noise of a laser. *Physical Review E*, 2010, **81** (5), 051137.
- [10] Shi Y., Chng B., et. al. Random numbers from vacuum fluctuations. *Applied Physics Letters*, 2016, **109** (4), 041101.
- [11] Kiselev F.D., Samsonov E.O., Gleim A.V. Modeling of linear optical controlled-Z quantum gate with dimensional errors of passive components. *Nanosyst.: Phys. Chem. Math.*, 2019, **10** (6), P. 627–631.
- [12] Rappaelli F., et. al. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. *Quantum Science and Technology*, 2018, **3** (2), 025003.
- [13] Gabriel C., Wittmann C., et. al. A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, 2010, **4** (10), P. 711–715.
- [14] Ivanova A.E., Chivilikhin S.A., et. al. How scatter of the experimental parameters affects the statistical characteristics of a quantum random-number generator. *J. Opt. Technol.*, 2014, **81** (8), P. 427–430.

- [15] Haw J.Y., Assad S.M., et. al. Maximization of extractable randomness in a quantum random-number generator. *Physical Review Applied*, 2015, **3** (5), 054004.
- [16] Guo X., Liu R., et. al. Enhancing extractable quantum entropy in vacuum-based quantum random number generator. *Entropy*, 2018, **20** (11), 819.
- [17] Marsaglia G. DIEHARD Test suite, 1998. URL: <http://www.stat.fsu.edu/pub/diehard>.
- [18] Rukhin A., et. al. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. National Institute of Standards & Technology, 2010.
- [19] Grynberg G., et. al. *Introduction to quantum optics: from the semi-classical approach to quantized light*. Cambridge university press, 2010.
- [20] Ivanova A.E., Chivilikhin S.A., Miroshnichenko G.P., Gleim A.V. Fiber quantum random number generator, based on vacuum fluctuations. *Nanosyst.: Phys. Chem. Math.*, 2017, **8** (4), P. 441–446.
- [21] Ivanova A.E., Chivilikhin S.A., Gleim A.V. The use of beam and fiber splitters in quantum random number generators based on vacuum fluctuations. *Nanosyst.: Phys. Chem. Math.*, 2016, **7** (2), P. 378–383.
- [22] Ivanova A.E. Quantum generation of random bit sequences based on vacuum fluctuations in a fiber-optic circuit. PhD Thesis, St. Petersburg, 2017, 121 p.
- [23] Tomamichel M., et. al. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 2011, **57** (8), P. 5524–5535.

Continuous variable measurement-device-independent quantum communication scheme based on subcarrier waves

M. Fadeev^{1,2}, R. Goncharov¹, S. Smirnov^{1,2}, V. Chistyakov¹

¹Laboratory for Quantum Communications, ITMO University, Saint Petersburg, Russia

²Quanttelecom LLC., Saint Petersburg, Russia

Abstract—In this work, we combine the achievements in terms of coherent detection based on the subcarrier wave method and measurement-device-independent approach. For such a scheme we provide a proof-of-principle experiment.

Index Terms—measurement-device-independent, coherent detection, subcarrier wave, continuous variables

I. INTRODUCTION

The need for research in the field of measurement-device-independent quantum key distribution (MDI QKD) is primarily due to noticeable progress in the field of engineering implementation of such systems. However, many questions regarding the practical implementation of the latter remain open. The concept of subcarrier wave (SCW) continuous variable QKD (CV-QKD) studied in this paper is in the context of encoding information at the sidebands of modulated radiation. Such systems can be implemented both in fiber and in free space, on discrete and continuous variables.

II. DESCRIPTION OF THE OPTICAL SETUP

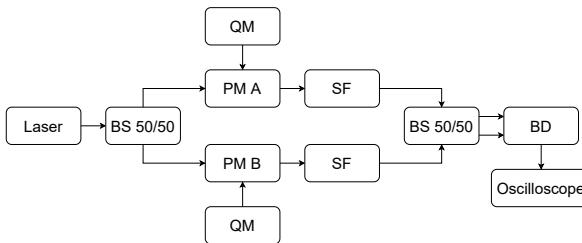


Fig. 1. Optical scheme of the experimental setup. BS is a beam splitter, QM is a quadrature modulator, PM is a phase modulator, SF is a spectral filter, BD is a balanced detector.

The optical scheme of the setup for the experiment is shown in the figure 1. The continuous radiation from the laser is split into a Y (1:2) beam splitter (BS), after which each of the branches (Alice's and Bob's) is subjected to electro-optical phase modulation with a given modulation frequency of 4.8 GHz (a combination of quadrature (QM) and phase modulator (PM)). In this case, the phases in the branches are chosen independently and randomly, as if it were in a QKD protocol. In this experiment, it was decided to fix one of the phases, while discretely or almost continuously changing the second. That is, it is assumed that the phase set by Alice on the "PM A"

modulator remains unchanged. Further, the resulting radiation in both branches pass spectral filtering (SF) and, after mixing on a 50/50 beam splitter, go to the arms of a balanced detector (BD).

III. RESULTS

The experiment can be described as follows. Alice sends 4 different states by applying different phase shifts $\{0, \pi/2, \pi, 3\pi/2\}$. Duration of these states is 80 ns and frequency of phase shifting is 100 MHz. On the other hand, Bob chooses only one state with zero phase shift. Interference between signals from Alice and Bob is detected by BD. Also BDs can replace two avalanche single photon detectors that are used in MDI schemes. The output of it is shown in Figure 2. This waveform demonstrates that the outcome voltage has a dependence of phase shifts chosen by Alice and Bob. In cases where the output of balanced detectors is fluctuating around zero, the basis of Alice does not match Bob's one and those results should be extracted from key in QKD protocol by using analog-to-digital converter.



Fig. 2. Outcome waveform from balanced detector with 4 states encoding.

IV. CONCLUSION

In this work, we have demonstrated the principal possibility of implementing the MDI CV-QKD scheme based on SCW method. Further research will be aimed at assembling a complete scheme of the QKD protocol.

ACKNOWLEDGMENT

This work was supported by grant "Fundamental and Applied Problems of Photonics" No. 621317 of ITMO University.

Conference materials

UDC 535.14

DOI: <https://doi.org/10.18721/JPM.173.145>

Influence of optical feedback on an optical pulse shape of a semiconductor laser

M.V. Boltanskii^{1, 3}, E.I. Maksimova¹, M.A. Fadeev^{4, 5}, R.A. Shakhovoy^{1, 2, 6}✉

¹ Limited Liability Company "QRate", Moscow, Russia;

² Moscow Technical University of Communications and Informatics, Moscow, Russia;

³ Peoples' Friendship University of Russia, Moscow, Russia;

⁴ Russian Quantum Center, Skolkovo, Moscow, Russia;

⁵ ITMO University, St. Petersburg, Russia;

⁶ NTI Center for Quantum Communications, National University of Science and Technology MISIS, Moscow, Russia

✉ m.boltanskiy@goqrate.com

Abstract. Gain-switched semiconductor lasers can produce pulses with naturally randomized phase, which makes them a convenient light source for quantum key distribution and random number generation. Nevertheless, semiconductor lasers are vulnerable to external optical feedback, a phenomenon, characterized by injection of a certain part of laser radiation into the laser's diode cavity. Although optical feedback may be used to decrease relaxation oscillations and chirp, it may have negative effect on laser pulses. Here, we study the influence of optical feedback on the pulse shape of a gain-switched laser.

Keywords: gain-switched laser, optical feedback, laser pulse interference

Citation: Boltanskii M.V., Maximova E.I., Fadeev M.A., Shakhovoy R.A., Influence of optical feedback on an optical pulse shape of a semiconductor laser, St. Petersburg State Polytechnical University Journal. Physics and Mathematics. 17 (3.1) (2024) 224–228. DOI: <https://doi.org/10.18721/JPM.173.145>

This is an open access article under the CC BY-NC 4.0 license (<https://creativecommons.org/licenses/by-nc/4.0/>)

Материалы конференции

УДК 535.14

DOI: <https://doi.org/10.18721/JPM.173.145>

Влияние оптической обратной связи на форму оптических импульсов полупроводникового лазера

М.В. Болтанский^{1, 3}, Е.И. Максимова¹, М.А. Фадеев^{4, 5}, Р.А. Шаховой^{1, 2, 6}✉

¹ ООО «КуРЭйт», Москва, Россия;

² Московский технический университет связи и информатики, Москва, Россия;

³ Российский университет дружбы народов, Москва, Россия;

⁴ Российский квантовый центр, Сколково, Москва, Россия;

⁵ Университет ИТМО, Санкт-Петербург, Россия;

⁶ Центр компетенций НТИ «Квантовые коммуникации» НИТУ МИСИС, Москва, Россия;

✉ m.boltanskiy@goqrate.com

Аннотация. Полупроводниковые лазеры в режиме усиления способны излучать импульсы со случайной относительной фазой, что делает их надежным источником энтропии для квантового распределения ключа и генерации случайности. Тем не менее, полупроводниковые лазеры уязвимы перед влиянием оптической обратной связи — явления, характеризуемого инжекции определенной доли лазерного излучения обратно в



полость лазерного диода. Хотя оптическая обратная связь может быть использована для подавления релаксационных колебаний и чирпа, она может иметь серьезный негативный эффект на лазерные импульсы. В этой работе мы изучаем влияние оптической обратной связи на форму импульса лазера в режиме переключения усиления.

Ключевые слова: лазер в режиме переключения усиления, оптическая обратная связь, интерференция лазерных импульсов

Ссылка при цитировании: Болтанский М.В., Максимова Е.И., Фадеев М.А., Шаховой Р.А., Влияние оптической обратной связи на форму оптических импульсов полупроводникового лазера // Научно-технические ведомости СПбГПУ. Физико-математические науки. 2024. Т. 17. № 3.1. С. 224–228. DOI: <https://doi.org/10.18721/JPM.173.145>

Статья открытого доступа, распространяемая по лицензии CC BY-NC 4.0 (<https://creativecommons.org/licenses/by-nc/4.0/>)

Introduction

External optical feedback (EOF) is known to have positive effect on a pulsed laser, e.g., it can reduce frequency chirp [1] and suppress relaxation oscillations [2], which can be useful in telecommunications. It also finds applications in range and velocity measurements [3]. However, optical feedback often causes certain unwanted effects, e.g. chaos dynamics [4] or increase of turn-on delay jitter [5]. In general, influence of EOF is stronger on lasers operating in continuous mode, meanwhile modulated lasers might avoid being impacted by EOF in case feedback radiation comes into a laser's cavity between modulation pulses [6]. Nevertheless, under certain circumstances, modulated laser pulses can be significantly affected by EOF as well [7]. Thereby, laser modules are often equipped with an optical isolator to prevent unwanted feedback. In this work, we studied the influence of optical feedback on a shape of optical pulses in a gain-switched distributed feedback (DFB) semiconductor laser.

Materials and Methods

The fiber-optic experimental scheme used to demonstrate the effect of optical feedback on a laser signal is shown in Fig. 1. It consisted of a semiconductor 1550 nm DFB laser diode (model SWLD-1554.94-FC/PC-05-PM) controlled by a laser driver based on a Texas Instruments ONET1151L chip, and a ring mirror (a looped beam splitter). The optical variable delay line (VDL) was installed in front of the mirror to control the length of the external cavity.

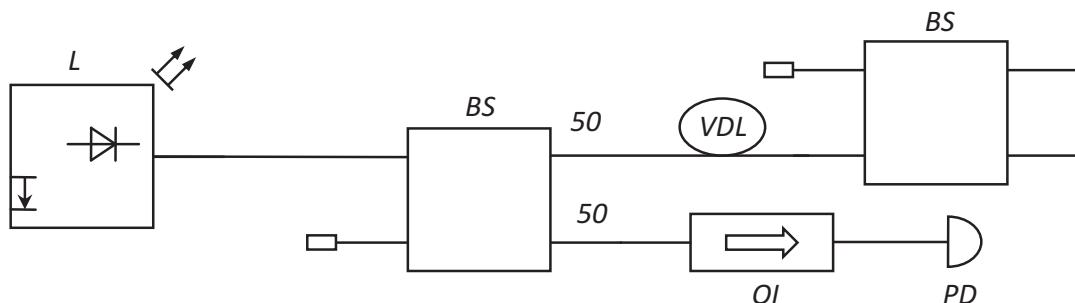


Fig. 1. The experimental scheme. *L* – laser module, *BS* – beam splitter, *OI* – optical isolator, *VDL* – variable optical delay line, *PD* – photodetector

The experiment was conducted using a pulse train with pulses of duration 400 ps, pulse repetition rate of 1.25 GHz and average laser output power of 2.7 mW. During the experiment, we varied the delay line to change the length of the external resonator.

Results and Discussion

Figure 2 shows the waveforms of laser pulses at different VDL values. Each waveform in the figure is accompanied by a value of the delay introduced by the VDL in picoseconds modulo the pulse repetition period, where a 0 ps delay would mean that a reflected pulse completely overlaps a generated one. Hence, delay values describe a measure of time shifts of reflected pulses relative to generated ones. One can see that at positive delay values right parts of laser pulses are barely distorted, meanwhile first relaxation peaks are not changed at all. As we move on to the negative values, we can observe well-pronounced suppression of relaxation oscillations.

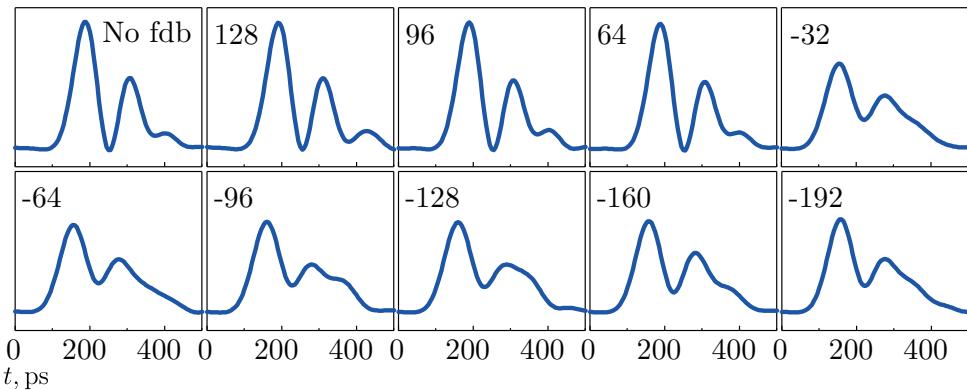


Fig. 2. Experimental laser pulse shapes at various optical feedback delay

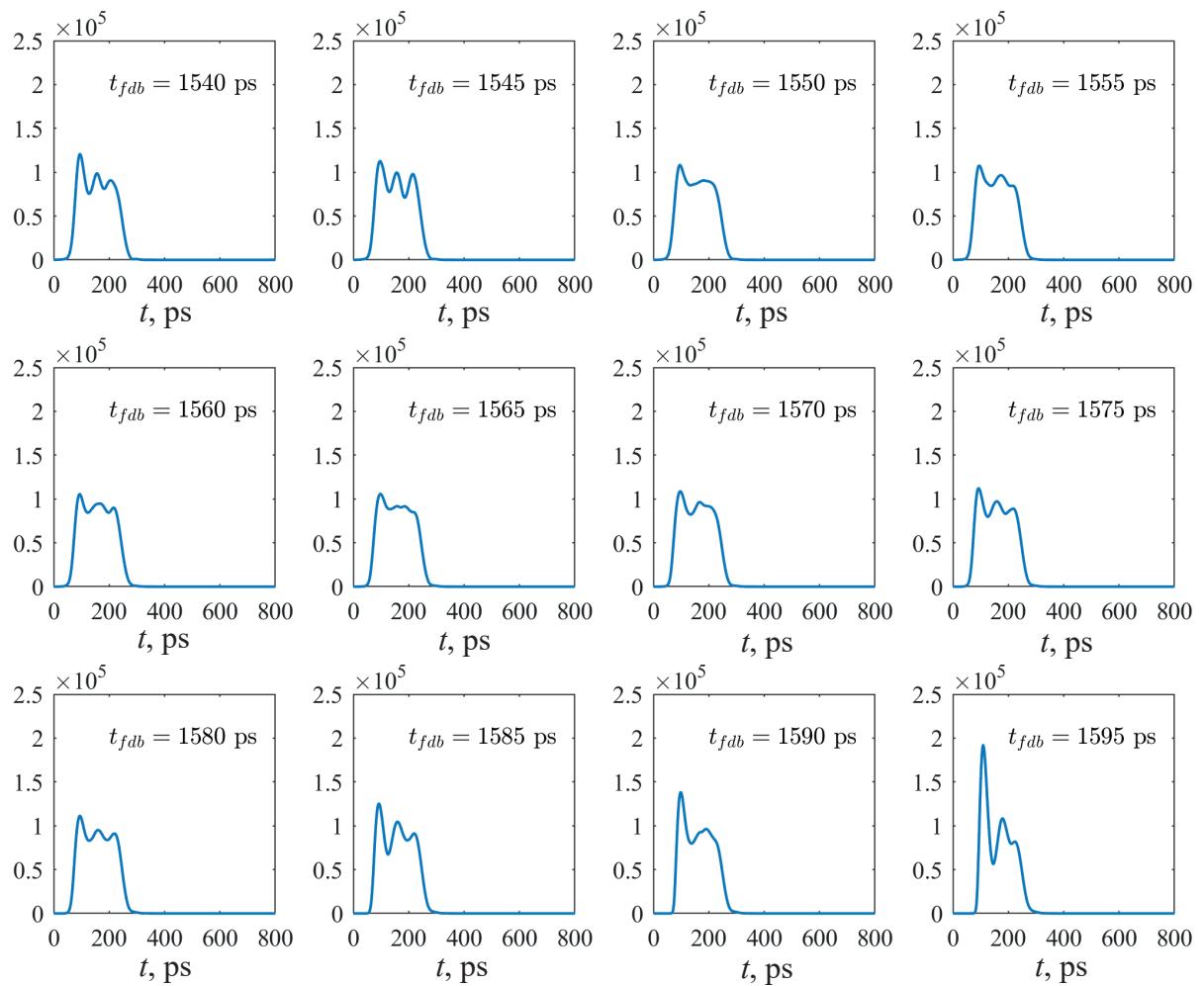


Fig. 3. Simulations of laser pulse shapes at various optical feedback delay

Figure 3 represents the results of computer simulations of a semiconductor laser diode with optical feedback, conducted with the commonly used rate equation model [8]. Simulation parameters are presented in Table. Simulations show that the influence of optical feedback on the waveform of laser pulses strongly depends on the arrival time of the reflected pulse. In particular, suppression of relaxation oscillations is more pronounced when the onset of lasing occurs under the quasi-stationary part of the reflected pulse, i.e. when the reflected pulse returns into the resonator earlier than the new pulse appears.

Table
Simulation parameters

Parameters	Values
Bias current I_b , mA	6.0
Carrier lifetime τ_e , ns	1.0
Pulse width ω , ns	0.4
Central optical frequency ω_0 , THz	193.548
Pulse repetition rate f_p , GHz	1.25
Confinement factor Γ	0.12
Threshold carrier number N_{th}	$5.5 \cdot 10^7$
Transparency carrier number N_{tr}	$4 \cdot 10^7$
Spontaneous emission factor C_{sp}	10^{-5}
Quantum differential output ϵ	0.3
Henry factor α	5
Feedback coupling factor κ_{fdb} , GHz	5

Conclusion

We performed an experimental and theoretical analysis to study the influence of optical feedback on an optical pulse shape of a gain-switched laser. It was shown that laser radiation reflected into the semiconductor laser diode's cavity may significantly change the pulse waveform at certain delay values, which is presented by our simulations, which are in a good agreement with the experimental results.

REFERENCES

1. Lang R., Kobayashi K., Suppression of the Relaxation Oscillation in the Modulated Output of Semiconductor Lasers, IEEE Journal of quantum electronics. (12) (1976) 194–199.
2. Grillot F., Provost J., Kechaou K., Thedrez B., Erasme D., Frequency Chirp Stabilization in Semiconductor Distributed Feedback Lasers with External Control, Optics Express. (20) (2012) 26062–26074.
3. De Groot J.P., Applications of optical feedback in laser diodes, Laser-Diode Technology and Applications. (1219) (1990) 457–467.
4. Al Bayati B., Ahmad A., Al Naimee K., Influence of optical feedback strength and semiconductor laser coherence on chaos communications, Journal of the Optical Society of America B. (35) (2018) 918–925.
5. Langley L.N., Shore K.A., The effect of external optical feedback on timing jitter in modulated laser diodes, Journal of Lightwave Technology. (11) (1993) 434–441.
6. Ryan A., Agrawal G., Gray G., Gage E., Optical-feedback-induced chaos and its control in multimode semiconductor lasers, IEEE Journal of Quantum Electronics. (30) (1994) 668–679.
7. Clarke B., The effect of reflections on the system performance of intensity modulated laser diodes, Journal of Lightwave Technology. (9) (1991) 741–749.
8. Shakhovoy R.A., Semiconductor laser dynamics, ELS «Лань», Saint-Petersburg. (404) (2024).

THE AUTHORS

BOLTANSKII Matvei V.
m.boltanskiy@goqrate.com

SHAKHOVOY Roman A.
r.shakhovoy@goqrate.com

MAXIMOVA Elizaveta I.
e.maksimova@goqrate.com

FADEEV Maxim A.
mfadeev2022@gmail.com

Received 04.07.2024. Approved after reviewing 31.07.2024. Accepted 31.07.2024.

Hybrid quantum communication protocol for fiber and atmosphere channel

Ilnur Z. Latypov^{1,a}, Vladimir V. Chistyakov^{2,3,b}, Maxim A. Fadeev^{2,4,c}, Danil V. Sulimov^{2,d}, Alexey K. Khalturinsky^{3,e}, Sergey M. Kynev^{2,3,f}, Vladimir I. Egorov^{2,3,g}

¹FRC Kazan Scientific Center of the Russian Academy of Sciences, Kazan, 420111, Russia

²ITMO University, Kronverkskiy, 197101, Russia

³Quanttelecom LLC., St. Petersburg, 199178, Russia

⁴Russian Quantum Center, Skolkovo, Moscow 121205, Russia

^abibidey@mail.ru, ^bv_chistyakov@itmo.ru, ^cwertsam@itmo.ru, ^ddvsulimov@itmo.ru,

^ea.halturinsky@quanttelecom.ru, ^fsergey.kynev@itmo.ru, ^gviegorov@itmo.ru

Corresponding author: I. Z. Latypov, bibidey@mail.ru

PACS 03.67.-a, 42.50.-p

ABSTRACT In this paper, we explore a hybrid quantum communication protocol that operates concurrently over fiber optic and atmospheric channels. This new protocol addresses challenges in urban settings where laying optical fiber may be impractical or costly. By integrating the subcarrier wave (SCW) quantum key distribution (QKD) with phase coding, our approach enhances the flexibility and reliability of quantum communication systems. We have developed and tested an atmospheric optical module equipped with an auto-tuning system to ensure precise optical axis alignment, crucial for minimizing signal loss in turbulent environments. Experimental results demonstrate stable sifted key rates and low quantum bit error rate (QBER) across various channel lengths, confirming the efficacy of our hybrid protocol in securing communication over diverse transmission environments.

KEYWORDS free-space optics, quantum communication, quantum key distribution, atmosphere channel.

ACKNOWLEDGEMENTS Atmospheric channel experiments were done by IZL, MAF, DVS, and AKK with the support of the government assignment for the FRC Kazan Scientific Center of RAS. The analytical work of VVC, SMK is supported by a grant from the Russian Science Foundation (project No. 24-29-00786).

FOR CITATION Latypov I.Z., Chistyakov V.V., Fadeev M.A., Sulimov D.V., Khalturinsky A.K., Kynev S.M., Egorov V.I. Hybrid quantum communication protocol for fiber and atmosphere channel. *Nanosystems: Phys. Chem. Math.*, 2024, **15** (5), 654–657.

1. Introduction

Protocols for quantum key distribution (QKD) are being developed for both fiber optic networks [1,2] and atmospheric links [3–5]. However, integrating fiber optic and atmospheric links to overcome challenges requiring the flexibility and reliability of both transmission media remains a key need. Atmospheric links are actively being developed for both traditional communication tasks within Internet networking and quantum cryptography. Atmospheric laser communication lines are effectively used at short and medium distances (up to 1 km), where laying fiber lines or radio frequency channels is technically or economically impractical. Modern atmospheric quantum communication systems are usually designed for long distances (ranging from 50 to 150 km) using ground-to-satellite or ground-satellite-ground configurations.

This paper presents a quantum communication system utilizing a universal “hybrid” protocol that generates a quantum key simultaneously in both the fiber and atmospheric channels. This scheme’s relevance stems from the specific requirements of constructing quantum telecommunication networks in urban environments, where areas often exist where laying fiber lines is impossible or economically unfeasible. This issue is known as the “last mile” problem [6,7]. A hybrid scheme is feasible when the sites are within the line of sight of each other. Subcarrier wave (SCW) quantum communication systems adopt a different approach to coding quantum states, avoiding issues prevalent in polarization coding systems.

2. Quantum key distribution in a hybrid communication channel

The scheme of the SCW QKD protocol with phase coding in free space is shown in Fig. 1 [8]. According to the scheme, the source of coherent radiation emits monochromatic light with frequency ω . After phase modulation with an electrical signal with low modulating frequency Ω and phase ϕ_A , the modulated signal passes through an attenuator and enters the quantum channel (atmosphere), where it undergoes attenuation.

After passing through the second electro-optic modulator with the same modulating frequency Ω and phase ϕ_B , the amplitudes of the sidebands increase (taking part of the energy from the carrier mode in the case $\phi_A = \phi_B$) or decrease (energy flows to the carrier mode). The narrowband spectral filter passes only the sidebands, and then the signal is detected by a single photon detector.

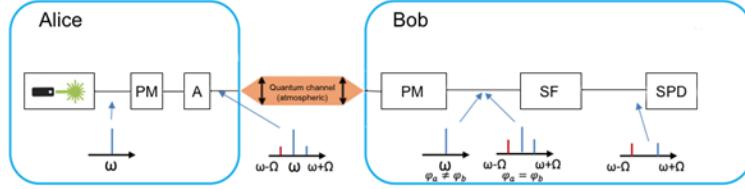


FIG. 1. Experimental setup of free-space subcarrier wave quantum communication system. PM is the phase modulator, A is the optical attenuator, SF is the spectral filter, and SPD is the single photon detector

TABLE 1. Statistics of optical line operation under typical turbulence conditions

Optical line	optical losses, average value, dB	optical loss, average deviation, dB	optical losses, minimum value, dB	optical losses, maximum value, dB	time
20 m	9,78	2,54	7,65	15,43	134 min

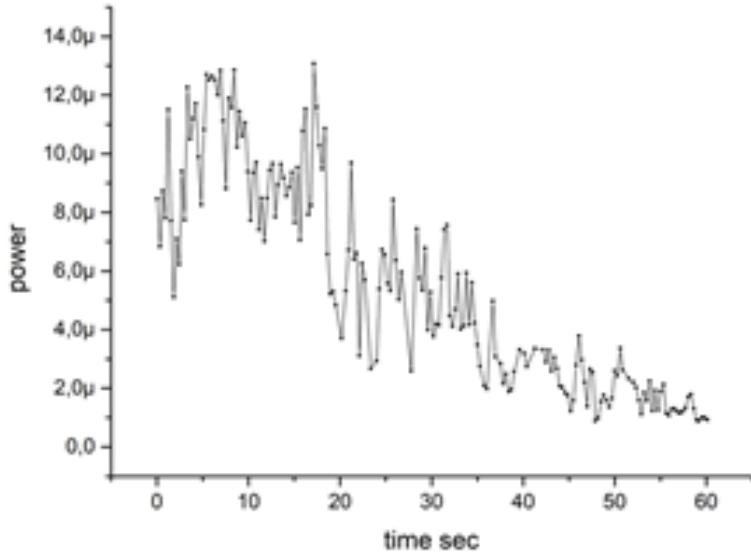


FIG. 2. The power of the laser radiation transmitted through the atmospheric line without auto-tuning system

To create a stable atmospheric channel, we developed transmitting and receiving optical modules equipped with an auto-tuning system. For the optical line to operate reliably, it is crucial to keep the optical axes of the receiver and the transmitter aligned with the accuracy of just a few microradians. When the length of the optical line increases from 5 to 100 meters, the losses in the optical signal remain relatively stable and range from 6 to 10 dB. The main part of the losses is associated with the deformation of the energy profile of the beam in a turbulent atmosphere. The automatic tuning system is based on the use of reference radiation of an optical diode at a wavelength of 900 nm, which is coaxially aligned with the optical axis of the quantum channel. The coordinates of the reference radiation are determined by a CCD matrix that generates a signal for a mirror controlled by four electromagnets. Thus, the auto-tuning system always maintains the alignment of the transmitter and receiver.

In the absence of an auto-tuning system, misalignment of the optical axes can occur within one minute. Fig. 2 shows an example of the dependence of the power of laser radiation at a wavelength of 1550 nm transmitted through an atmospheric line without an auto-tuning system.

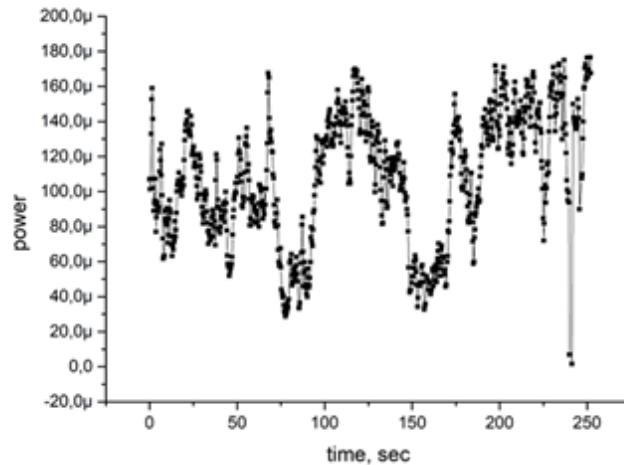


FIG. 3. The power of the laser radiation transmitted through the atmospheric line. Deviation from the maximum value is associated with the influence of turbulence

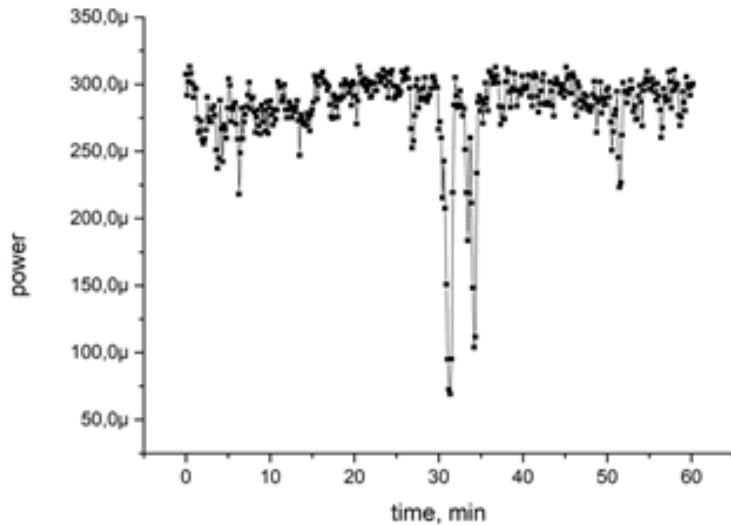


FIG. 4. The power dependence of the signal transmitted through the optical line on time. The operation of the auto-tracking system for a long time is demonstrated

Fig. 3 shows an example of the effect of turbulence on losses in the optical channel. The magnitude and nature of turbulence depend on the location of the optical line, the speed of movement of air masses, and the temperature gradient. Fig. 4 shows the effectiveness of the auto-tracking system over a long time. The accuracy of our track system was 7 microradian, which made it possible to keep the optical signal at the level of 1 dB.

After setting up the optical and QKD systems, we measured the performance of the systems over different channel lengths: 25 meters, 40 meters, and 50 meters. For all optical channels, the optical loss was 6.5 dB, and the sifted key generation rate was 1.45 KB/s, with a quantum bit error rate (QBER) of 6%. Losses at the output and input into the optical fiber determined losses in the optical line. An optical beam with an aperture of 80 mm has a low diffraction divergence, thus at a distance of 15, 25, and 40 meters, we get the same key generation rate.

3. Conclusion

Measurements of the key rate in a hybrid communication protocol including fiber optic and atmospheric sections have been carried out. The atmospheric link was implemented using the developed transceivers equipped with an auto-tuning system. The results show that the SCW QKD protocol functions effectively in the atmospheric link, and the key generation rate depends solely on the optical loss. In the future, it is planned to improve the persistence of the protocol by detailed theoretical analysis of the possibility of using turbulence to obtain information accessible by an intruder (Eve).

References

- [1] Honjo T., Nam S.W., Takesue H., Zhang Y., Hadfield R.H., Dardy H.H., and Yamamoto Y. Long-distance entanglement-based quantum key distribution over optical fiber. *Optics Express*, 2008, **16**(23), P. 19118–19126.
- [2] Rosenberg D., Harrington J.W., Rice P.R., Hiskett P.A., Peterson C.G., Hughes R.J., Lita A.E., Nam S.W., and Nordholt J.E. Long-distance decoy-state quantum key distribution in optical fiber. *Physical Review Letters*, 2007, **98**(1), P. 010503.
- [3] Cao Y., Li Z., Zhang W., You Z., Zhang X., Wang Z., Huang C., Li H.W., and Guo G.C. Long-distance free-space measurement-device-independent quantum key distribution. *Physical Review Letters*, 2020, **125**(26), P. 260503.
- [4] Pirandola S. Limits and security of free-space quantum communications. *Physical Review Research*, 2021, **3**(1), P. 013279.
- [5] Schmitt-Manderbach T., Weier H., Fuerst M., Ursin R., Tiefenbacher F., Scheidl T., Perdigues J., Sodnik Z., Kurtsiefer C., and Weinfurter H. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 2007, **98**(1), P. 010504.
- [6] Cao Y., Zhang Z., Xu B., You L., Wang Z., and Li H. W. The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Communications Surveys & Tutorials*, 2022, **24**(2), P. 839–894.
- [7] Techateerawat P. Simulating Network Management System for Quantum Key Distribution based on rural and remote broadband in Thailand. *PBRU Science Journal*, 2023, **20**(1), P. 97–110.
- [8] Kynev S.M., Chistyakov V.V., Fadeev M.A., and Latypov I.Z. Free-space subcarrier wave quantum communication. *Journal of Physics: Conference Series*. IOP Publishing, 2017, **917**(5), P. 052003.

Submitted 9 September 2024; revised 22 September 2024; accepted 23 September 2024

Information about the authors:

Ilnur Z. Latypov – FRC Kazan Scientific Center of the Russian Academy of Sciences, ul. Lobachevskogo, 2/31, POB 261, Kazan, 420111, Russia; ORCID 0000-0003-2990-249X; bibidey@mail.ru

Vladimir V. Chistyakov – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; Quanttelecom LLC., 6 Line, 59, St. Petersburg, 199178, Russia; ORCID 0000-0002-2414-3490; v_chistyakov@itmo.ru

Maxim A. Fadeev – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; Russian Quantum Center, Skolkovo, Moscow 121205, Russia; ORCID 0000-0003-4290-4852; wertsam@itmo.ru

Daniel V. Sulimov – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; ORCID 0000-0002-7964-0697; dvsulimov@itmo.ru

Alexey K. Khalturinsky – Quanttelecom LLC., 6 Line, 59, St. Petersburg, 199178, Russia; a.halturinsky@quanttelecom.ru

Sergey M. Kynev – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; Quanttelecom LLC., 6 Line, 59, St. Petersburg, 199178, Russia; ORCID 0000-0001-8698-1804; sergey.kynev@itmo.ru

Vladimir I. Egorov – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; Quanttelecom LLC., 6 Line, 59, St. Petersburg, 199178, Russia; ORCID 0000-0003-0767-0261; viegorov@itmo.ru

Conflict of interest: the authors declare no conflict of interest.

Secure laser source for QKD systems

M. Fadeev^{1,2}, A.A. Ponomova¹, A. Huang³, R. Shakhovoy^{4,5,6}, V. Makarov^{1,5,7}

¹ Russian Quantum Center, Skolkovo, Moscow 121205, Russia

² ITMO University, St. Petersburg, 197101, Russia

³ National University of Defense Technology, Changsha 410073, People's Republic of China

⁴ QRate, Skolkovo, Russia

⁵ NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia

⁶ Moscow Technical University of Communications and Informatics, Moscow, Russia

⁷ University of Science and Technology of China, Shanghai 201315, People's Republic of China

mfadeev2022@gmail.com

Abstract—In practical quantum key distribution systems, single photon sources take laser-seeding attacks. Typically, some amount of isolation is recommended as the countermeasure against these attacks. Here, we demonstrate a new approach of QKD system protection against laser seeding based on internally seeded photon source scheme, resilient to external perturbations.

Index Terms—single photon source, QKD, laser-seeding attack, quantum hacking, countermeasure

I. INTRODUCTION

Practical QKD systems use strongly attenuated laser pulses from semiconductor laser diodes (LD) rather than true single-photon sources due to the lasts do not enable practical key rates. However, as LDs are very sensitive to external perturbations, there are several laser-seeding attacks which open up back doors for Eve. Previous study has shown that an injection power of 100 nW could be enough to control the intensity of Alice's pulses [1] and about 1 nW might be enough to partially control the phase [2]. Here, we investigate an internally seeded photon source configuration under external laser-seeding attack.

II. EXPERIMENT

We implemented an optical injection-locked light source proposed by L.C.Comandar et al. [3]. It includes the master laser diode that injects pulses into the slave laser diode via a fiber-optic circulator. Both LDs' temperature and time of drive electric pulses were matched well to provide injection locking and chirpless bell-shaped laser pulses. The source operates at 10.035 MHz repetition rate with pulse duration of about 850 ps. To investigate resilience of the source, the attacker's CW seed laser emission is inserted into the source through the third circulator port (Alice's output). Our experimental setup allow Eve's laser power from 100 mW to 1.1 W and spectral tunability of about several nanometers near to 1550 nm. Due to losses in the circulator for Eve's light, the maximum Eve's laser power is about 1.3 μW at the slave entrance (in comparison, the average power of the master LD at the slave entrance is 7 μW). The average power, spectra, pulse shapes, pulse intensity stability and statistic of interference of two following each other pulses are characterized before and under attack using different Eve's laser wavelengths.

III. RESULTS

The source under attack shows high stability of its spectral and amplitude-time characteristics. However, we found an increase in average output power by 7.5%. According to data analysis, it results from amplification of Eve's emission in the slave LD. Figure 1 shows output spectra for different seed laser wavelengths. It can be seen that amplification is the most notable when Eve's wavelength differs from Alice's one. While Eve might conduct a wavelength-dependent attack using DWDM to obtain additional information about the secure key, this attack might be easily closed using a narrowband spectral filter.

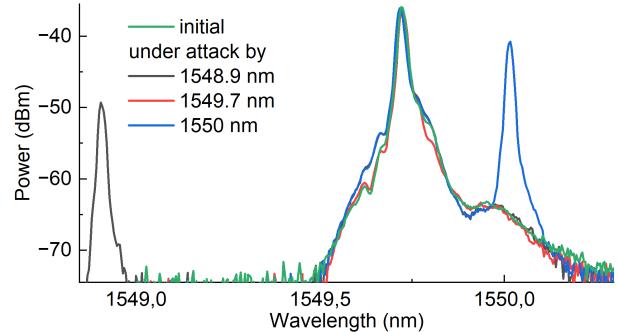


Fig. 1. QKD source output spectra when seeding power at the slave entrance is about 700 nW. (The spectra of reflected Eve's emission are rejected from the measured output spectra.)

IV. SUMMARY

We show experimentally that the injection-locked source is resilient against laser-seeding attacks and might be used as an effective countermeasure in QKD sources.

REFERENCES

- [1] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser-seeding attack in quantum key distribution," *Phys. Rev. Appl.*, vol. 12, pp. 064043, 2019.
- [2] V. Lovic, D.G. Marangon, P.R. Smith, R.I. Woodward, and A.J. Shields, "Quantified effects of the laser-seeding attack in quantum key distribution," *Phys. Rev. Appl.*, Vol. 20, pp. 044005, 2023.
- [3] L.C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, Z.L. Yuan, and A.J. Shields, "Near perfect mode overlap between independently seeded, gain-switched lasers," *Opt. Express.* vol. 24, pp. 17849–17859, 2016.

Laser-pumping attack on QKD sources

M. Fadeev^{1,2}, A.A. Ponosova¹, R. Shakhovoy^{3,4,5}, V. Makarov^{1,5,6}

¹Russian Quantum Center, Skolkovo, Moscow 121205, Russia

²ITMO University, St. Petersburg, 197101, Russia

³QRate, Skolkovo, Russia

⁴NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia

⁵Moscow Technical University of Communications and Informatics, Moscow, Russia

⁶University of Science and Technology of China, Shanghai 201315, People's Republic of China

mfadeev2022@gmail.com

Abstract—For the first time, we demonstrate a new type of attack on QKD systems based on laser pumping of a photon source. It includes injection of cw-laser emission into a source at a wavelength shorter than the system operating one. In particular, we show that laser emission at 1310 nm induces an increase in photon number at 1550 nm, changes in pulse shape and width. The QKD risk evaluation due to laser-pumping attack is presented.

Index Terms—QKD source loopholes, vulnerabilities, laser-pumping attack, quantum hacking

I. INTRODUCTION

Semiconductor distributed-feedback laser diodes used in QKD systems have electrical pumping, where an electrical current generates electron-hole pairs, afterward, theirs relaxation results in photons emitting. However, some semiconductor materials might also be pumped optically. Typically, optical pumping is possible at a somewhat shorter wavelength than the operating one. While the most producers do not disclose information about semiconductor composition, more often, for lasers in 1300 and 1550 nm wavelength range, the active material is InGaAsP-based quaternary compound [1], which might be pumped optically [2]. Our study is focused on risk evaluation in presence of laser-pumping attack on semiconductor diodes of QKD systems.

II. EXPERIMENT

To simulate a quantum hacking scenario, we have implemented a simple experimental setup in which 1310-nm Eve's light injects into a target photon source via a fiber-optic circulator and, next, output characteristics at 1550 nm of a source are measured at the third circulator port. As Alice source, we used semiconductor LD without internal isolator. It generates 510-ps optical pulses with a repetition rate of 10 MHz. Eve's LD at 1310 nm operates in the continuous-wave regime. Its power at the entrance of the source under test ranges from 1.17 μ W to 2.98 mW. The pulse envelope and spectra are measured under different injection powers. The pulse energy is then calculated by integrating the recorded pulse envelope. To better understand, we have also studied the watt-ampere characteristic of 1550-nm LD in the CW mode when pumped by 1310-nm emission.

Identify applicable funding agency here. If none, delete this.

III. RESULTS

We observe changes in spectral, power and amplitude-time characteristics (Fig. 1). Each of them might be used by Eve to obtain additional information about the secret key. However, the increase in pulse energy is the most likely due to the unnoticed increase in intensity that can compromise the security of QKD, as was theoretically shown [2] for the prepare-and-measure decoy-state BB84 and MDI QKD protocols. We show the maximum magnification of 1.4 at the pump power of about 2.98 mW. To prevent the attack, adequate isolation should be provided throughout the spectral range.

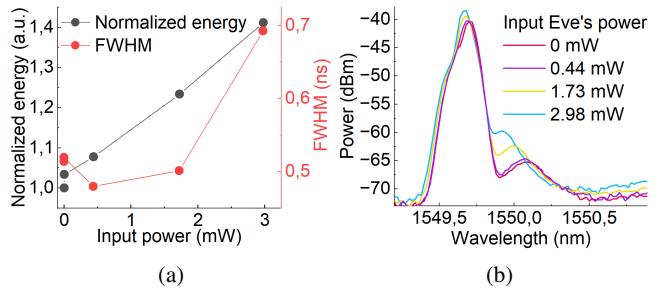


Fig. 1: Changes in photon source characteristics depending on 1310-nm injection power: normalized pulse energy and pulse width (a); output spectra (b).

IV. SUMMARY

We have shown that a practical source based on a semiconductor laser diode is vulnerable to a laser-pumping attack, in which light at a somewhat shorter wavelength injected from the communication line into the QKD source results in an increase of the intensities of the prepared states.

REFERENCES

- [1] Z. Fang, H. Cai, G. Chen, R. Qu, Single Frequency Semiconductor Lasers, 1st ed. Springer Singapore, 2017.
- [2] H. Temkin, G.J. Dolan, and R.A. Logan, "Optically pumped In-GaAsP/InP distributed feedback lasers." J. Appl. Phys., vol. 56, pp. 2183–2186, 1984.
- [3] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser-seeding attack in quantum key distribution," Phys. Rev. Appl., vol. 12, pp. 064043, 2019.

¹ Контактные данные автора, ответственного за связь с редакцией

² Фадеев Максим Алексеевич

³ Университет ИТМО, 197101, г. Санкт-Петербург, Кронверкский пр., 49

⁴ мобильный телефон +7 999 206-94-13

⁵ e-mail: wertsam2011@gmail.com

6 УДК 681.7

7 **Гетеродинное детектирование для системы квантового распре-**
8 **деления ключа на боковых частотах**

9 *M.A. Фадеев^{1,3}, П.А. Морозова¹, С.В. Смирнов^{1,2}, А.Е. Иванова^{1,2},*

10 *С.М. Кынев^{1,2}, В.В. Чистяков¹*

11 ¹ Университет ИТМО 197101, Россия, г. Санкт-Петербург, Кронверкский пр, д. 49;

12 ²ООО «СМАРТС-Кванттелеком» 199178, Россия, г. Санкт-Петербург, Б.О., 6 линия

13 д.59, корп. 1, лит. Б;

14 ³ Российский Квантовый Центр 21205, г. Москва, Территория Инновационного Цен-
15 тра «Сколково», Большой бульвар, д. 30, стр. 1

16 Одним из способов улучшения характеристик системы квантовой коммуникации на
17 боковых частотах является изменение принципов детектирования. В настоящей статье
18 в качестве альтернативы детектору одиночных фотонов, рассматривается гетеродинное
19 детектирование с использованием балансного фотодетектора. В рамках работы реали-
20 зована схема гетеродинного детектирования для системы квантового распределения
21 ключа на боковых частотах, продемонстрирована экспериментальная работа данной
22 схемы и проведены измерения фазового сдвига, которым возможно кодировать инфор-
23 мацию.

²⁴ **Heterodyne detection for subcarrier-wave quantum key distribution**

²⁵ **system**

²⁶ *M. A. Fadeev, R. K. Goncharov, P. A. Morozova, S. V. Smirnov, A. E. Ivanova S. M.*

²⁷ *Kynev, V. V. Chistyakov*

²⁸ One way to improve the performance of a quantum communication system at side
²⁹ frequencies is to change the detection principles. In this article, as an alternative to a single
³⁰ photon detector, heterodyne detection using a balanced photodetector is considered. As part
³¹ of the work, a heterodyne detection circuit was implemented for a quantum key distribution
³² system at side frequencies; the experimental operation of this circuit was demonstrated, and
³³ measurements of the phase shift, which can be used to encode information, were carried out.

³⁴

³⁵ Здесь желательно указать перевод специальных терминов, часто использующихся

³⁶ в статье, на английский язык:

³⁷ квантовое распределение ключа - quantum key distribution гетеродинное детектирова-
³⁸ ние - heterodyne detection боковые частоты - subcarrier waves балансный детектор -
³⁹ balanced detector КРКБЧ - SCWQKD Гомодинное детектирование - homodyne detection
⁴⁰ Локальный осциллятор - Local Oscillator Быстрое Преобразование Фурье - Fast Fourier
⁴¹ Transform Дискретные переменные - Discrete Variables Непрерывные переменны - Continuous
⁴² Variables КРКНП - CV-QKD

⁴³ ВВЕДЕНИЕ

⁴⁴ Современные системы передачи данных невозможны без систем шифрования и выра-
⁴⁵ ботки ключей. Однако развитие квантовых компьютеров является существенным вызо-
⁴⁶ вом для существующих протоколов шифрования [1]. Одним из решений этой проблемы
⁴⁷ являются системы квантового распределения ключа (КРК), построенные на физиче-
⁴⁸ ских принципах защиты информации. Криптографическая стойкость КРК обеспечива-
⁴⁹ ется за счет использования одиночных фотонов или ослабленного (до уровня кванто-
⁵⁰ вого сигнала) когерентного излучения в качестве носителей информации и достигается
⁵¹ следующими свойствами: теорема о запрете клонирования, разрушение фотона при из-
⁵² мерении [2, 3, 4]. На практике в системах КРК чаще применяются так называемые
⁵³ ослабленные когерентные состояния света из-за сложностей реализации однофотонных
⁵⁴ схем [5]. Тем не менее, для таких систем также обоснована криптографическая стой-
⁵⁵ кость [6, 7, 8].

⁵⁶ В мировой литературе существует следующая классификация протоколов КРК: на
⁵⁷ дискретных переменных [4], где в блоке получателя используются детекторы одиноч-
⁵⁸ ных фотонов на основе сверхпроводников или лавинных диодов; и на непрерывных
⁵⁹ переменных [9, 10], где на приемной стороне приготовленный сигнал смешивается на
⁶⁰ сбалансированном светоделителе с так называемым локальным осциллятором — мощ-
⁶¹ ным опорным излучением. Результат интерференции этих сигналов будет зависеть от
⁶² разности фаз между локальным осциллятором и информационным сигналом. Резуль-
⁶³ тат регистрируется с помощью балансного детектора, который состоит из классических
⁶⁴ фотодиодов и вычитающей схемы, поэтому выходные фототоки вычитываются для умень-
⁶⁵ шения шумов и увеличения чувствительности.

⁶⁶ В настоящей работе рассматривается система КРК на непрерывных переменных с
⁶⁷ передачей по волоконному каналу локального осциллятора совместно с информацион-

68 ным сигналом. Разностная частота (между локальным осциллятором и сигналом) на-
69 блюдается на выходе балансного детектора и в случае кодирования информации в боко-
70 вых частотах модулированного излучения является модулирующей частотой электро-
71 оптического модулятора в блоке отправителя. Одним из подходов к реализации прото-
72 колов КРК является КРК на боковых частотах (КРКБЧ) [11, 12, 13], конвенциональная
73 схема которого отражена на рисунке 1. Данный подход позволяет генерировать ослаб-
74 ленные когерентные состояния на боковых частотах, которые появляются в оптическом
75 спектре после фазовой модуляции синусоидальным сигналом. Такая реализация позво-
76 ляет более эффективно использовать технику частотного мультиплексирования (Dense
77 Wavelength Division Multiplexing) [14], а также успешно компенсировать поляризаци-
78 онные искажения линии пассивным методом. [15, 16] Дополнительно существует воз-
79 можность производить сеансы квантовой коммуникации по открытому пространству,
80 используя КРКБЧ [17].

81 Типичный протокол КРКБЧ работает следующим образом. Лазерное излучение от
82 непрерывного лазера попадает на фазовый модулятор, на радиочастотный вход кото-
83 рого подается синусоидальный сигнал. Для генерации модулирующего сигнала и вне-
84 сения фазового сдвига в него используется квадратурный модулятор. В результате на
85 выходе оптического фазового модулятора в оптическом спектре формируется много-
86 модовый (в смысле частотных мод) сигнал. Рассматривают три значимые моды: моду
87 на центральной частоте, являющуюся несущей модой. две боковые моды, отстоящие
88 от несущей, которые соответствуют сумме и разности частот лазера и модулирующего
89 сигнала. Остальными же модами пренебрегают вследствие малой глубины модуляции.
90 Полученный спектр излучения ослабляется с помощью перестраиваемого аттенюатора
91 так, чтобы мощность боковых компонент была на уровне квантового сигнала.

92 После этого полученное излучение передается по оптическому волокну на сторону

93 приемника. На приемной стороне подготовленное Алисой состояние подвергается по-
94 второй модуляции на той же частоте, что и на стороне отправителя. При этом Боб
95 вносит в свой модулирующий сигнал фазовый сдвиг. В результате повторной модуля-
96 ции на боковых частотах наблюдается интерференция, которая зависит от разности
97 фаз, выбранных Алисой и Бобом. Далее установлен спектральный фильтр на основе
98 Брэгговской решетки, который отражает сигнал на несущей частоте, поскольку он не
99 несет информации, а боковые компоненты проходят без изменений. Регистрация резуль-
100 тата интерференции происходит с помощью детектора одиночных фотонов. Количество
101 отсчетов, формируемых детектором, будет зависеть от результата интерференции.

102 Однако описанная выше схема обладает следующими недостатками: необходимость
103 согласования базисов измерений состояния фотонов, низкая эффективность детектора
104 одиночных фотонов и необходимость его охлаждения до температур порядка -40°C .

105 Ограничения системы КРК с детектором одиночных фотонов на основе лавинного
106 фотодиода возможно преодолеть, используя концепцию КРК на непрерывных пере-
107 менных (КРКНП) и когерентное детектирование, которое основано на использовании
108 балансного детектора для регистрации излучения. В литературе уже было предложено
109 несколько вариантов реализации [18, 19], тем не менее такие схемы сталкиваются со
110 сложностями по части экспериментальной схемы.

111 **1 Гетеродинное детектирование в системе квантовой 112 коммуникации на боковых частотах**

113 Одним из методов реализации когерентного приема является гетеродинное детектиро-
114 вание. Данный метод изначально был предложен в радиотехнике для приема высокоча-
115 стотных модулированных сигналов. Суть данного детектирования в переносе частоты

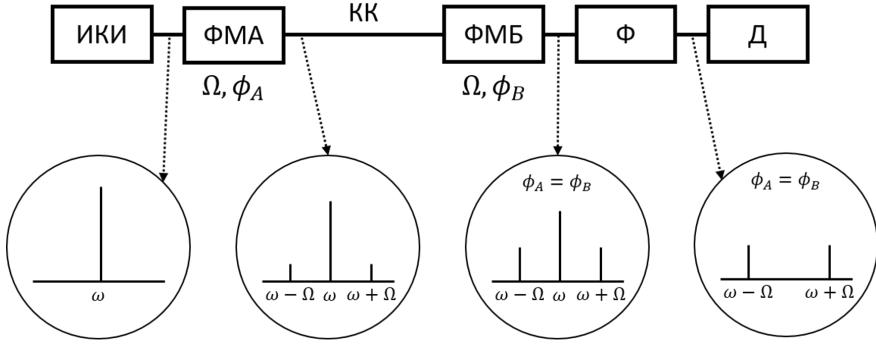


Рис. 1: Оптическая схема (упрощенная) системы КРКБЧ. Источник когерентного излучения ИКИ испускает слабый монохроматический свет (сигнал), в спектре которого после фазовой модуляции в электрооптическом модуляторе ФМА, к которому приложен осциллирующий электрический сигнал с частотой Ω порядка нескольких ГГц и фазой ϕ_A , появляются боковые частоты (на схеме показаны только первые боковые частоты). Далее модулированный сигнал проходит через квантовый канал КК (оптическое волокно), где претерпевает затухание. После сигнала проходит второй электрооптический модулятор, к которому также приложен осциллирующий электрический сигнал с частотой Ω и фазой ϕ_B . В зависимости от разности фаз между ϕ_A и ϕ_B амплитуды боковых мод увеличиваются (забирая часть энергии с центральной частоты в случае $\phi_A = \phi_B$) или уменьшаются (энергия перетекает на центральную частоту). Узкополосный фильтр Ф пропускает только боковые частоты (и малую часть центральной частоты), далее происходит регистрация сигнала с помощью детектора одиночных фотонов.

116 из полосы высоких частот в полосу более низких частот, где обработка и усиление сиг-
 117 налов упрощены [20, 21, 22]. Достигается это за счет интерференции сигналов: опорного
 118 (локального осциллятора) и принятого информационного на нелинейном элементе [23].
 119 В результате принятый сигнал переносится в полосу более низких частот, по сравнению
 120 с частотой исходного сигнала. При этом информация, закодированная в фазе исходного
 121 сигнала, сохраняется.
 122 В настоящей работе по аналогии с [18, 19] рассматривается аналог такого подхода

123 в контексте КРКБЧ. Тем не менее, как описано выше, предыдущие варианты сложно
124 реализовать на практике. Особенno это касается гетеродинного детектирования из [19],
125 который так и не был полноценно реализован. Следует отметить, что в работе [24],
126 несмотря на общее название, рассматривается аналог гомодинного детектирования с
127 регистрацией только одной квадратурной компоненты. Представленную там схему сле-
128 дует называть аналогом по той причине, что в качестве локального осциллятора там
129 используется энергия, перенесенная с несущей моды в боковые в результате повторной
130 модуляции. Теоретическое описание схемы было приведено в работе [25], а в работе
131 [26] на примере протокола GG02 было показано падение эффективности относительно
132 конвенционального гомодинирования.

133 В настоящей же работе осуществляется гетеродинированием с детектированием на
134 радиочастоте, что позволяет регистрировать сразу две квадратурные компоненты без
135 необходимости использования двух балансных детекторов. Это можно рассматривать
136 как альтернативный подход в контексте когерентного детектирования для систем кван-
137 товых коммуникаций на боковых частотах.

138 Протокол работает следующим образом:

- 139 1. Алиса готовит квантовые состояния, кодируя информацию в фазовый свиг излу-
140 чения на боковых частотах ослабленного лазерного излучения, и передает их.
- 141 2. Боб измеряет пришедшие квантовые состояния с помощью гетеродинного детек-
142 тирования.
- 143 3. Выходной сигнал балансного детектора оцифровывается и обрабатывается с по-
144 мощью алгоритма Быстрого Преобразования Фурье.
- 145 4. Измеряется частота и фаза нужной гармоники из полученного мгновенного спек-
146 тра.

147 5. Оценивается соотношение сигнал/шум.

148 6. Проводится процедура исправления ошибок с помощью соответствующих кодов.

149 В конечном счете, оценивается т.н. просеянный ключ без учета присутствия нарушителя в канале. Т.е. процедура усиления стойкости не выполняется и оставлена на будущие работы с полноценным доказательством стойкости.

152 **2 Математическая модель гетеродинного приема для** 153 **системы квантовой коммуникации на боковых ча-** 154 **стотах**

155 Излучение лазера может быть представлено следующим образом:

$$F(t) = A_0 * \sin(\omega_0 t + \phi_0), \quad (1)$$

156 где A_0 – амплитуда сигнала, ω_0 – частота лазерного излучения, ϕ_0 – начальная фаза

157 излучения. Модулирующий сигнал:

$$S(t) = (1 + m \sin(\Omega t + \phi(t))), \quad (2)$$

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

159 Лазерное излучение после модуляции выглядит следующим образом:

$$\begin{aligned} F_s(t) &= F(t) * S(t) = A_0 * \sin(\omega_0 t + \phi_0) + \frac{A_0 * m}{2} * (\cos((\omega_0 + \Omega)t + (\phi_0 + \phi(t))) - \\ &- \frac{A_0 * m}{2} * (\cos((\omega_0 - \Omega)t + (\phi_0 - \phi(t)))), \end{aligned} \quad (3)$$

160 Результат квадратичного детектирования сигнала, полученного в выражении (3)

161 будет выглядеть следующим образом:

$$\begin{aligned} F_d(t) &= F(t)^2 * S(t)^2 = (A_0 * \sin(\omega_0 t + \phi_0))^2 * (1 + m * \sin(\Omega t + \phi_0 + \phi(t)))^2 = \\ &= \frac{1}{8} \left\{ 4A_0^2 + 2A_0^2 * m^2 - 4A_0^2 \cos(2\omega t + 2\phi_0) - 2A_0^2 * m^2 \cos(2\omega t + 2\phi_0) - \right. \\ &\quad - 2A_0^2 * m^2 \cos(2\Omega t + 2\phi(t)) + A_0^2 * m^2 \cos(2\omega t - 2\Omega t + 2\phi_0 - 2\phi(t)) + \\ &\quad + A_0^2 * m^2 \cos(2\omega t + 2\Omega t + 2\phi_0 + 2\phi(t)) + 8A_0^2 m \sin(\Omega t + 2\phi(t)) + \\ &\quad \left. + 4A_0^2 m \sin(2\omega t - \Omega t + 2\phi_0 - \phi(t)) - 4A_0^2 m \sin(2\omega t + \Omega t + 2\phi_0 + \phi(t)) \right\}, \quad (4) \end{aligned}$$

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

$$I = R(\lambda) GCF_d, \quad (5)$$

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

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

170 **3 Экспериментальная реализация гетеродинного при- 171 ема для системы квантовой коммуникации на боко- 172 вых частотах**

173 Схема экспериментальной установки (см. рисунок 2). Она состоит из лазера Teraxion
174 PureSpectrum со следующими параметрами: центральная длина волны 1550 нм, ширина
175 полосы излучения менее 1 МГц, излучаемая мощность до 40 мВт. После него установ-
176 лен светоделитель с 1 входом и 2 выходами, излучение между которыми разделяется

177 50 на 50. Один из выходов подключен к фазовому модулятору производства EOSpace
178 со следующими характеристиками: вносимые потери 4 дБ, полоса пропускания 20 ГГц,
179 рабочая длина волны 1550 нм. Второй же выход светоделителя использовался в каче-
180 стве контрольного для измерения выходной мощности. В качестве генератора сигна-
181 ла использовался генератор Tektronix AFG3022C. Параметры модулирующего сигнала:
182 Частота сигнала 100 МГц, его амплитуда 0.8 В со смещением на 1 В, вносимый фазовый
183 свдиг от 0 до 360 градусов, индекс модуляции при этом составлял 0.05. В результате
184 мощность на боковых частотах составляла 200 нВт, во всем спектре - 40 мкВт. Модули-
185 рованный сигнал лазера, в котором наблюдаются 3 гармоники: несущая и две боковые
186 частоты, попадает на светоделитель с 2 входами и 2 выходами. Один из входов не
187 использовался. Сигнал между выходными портами делится пополам и попадают на ба-
188 лансный детектор. Данный детектор обладает следующими характеристиками: полоса
189 пропускания 200 МГц, чувствительность фотодиодов 0,7 А/Вт, коэффициент усиления
190 $4 \cdot 10^3$

191 В качестве измерительного оборудования выступал осциллограф Tektonix DPO70604C
192 с полосой пропускания 6 ГГц.

193 4 Результаты проведенного эксперимента

194 На рисунках 3 и 4 представлены осциллограммы на выходе балансного детектора. На
195 рисунке 3 отображается синусоидальный сигнал на частоте модуляции в 100 МГц с
196 фазовым сдвигом равным 0 градусов. Данный сигнал необходимо фильтровать от соб-
197 ственных шумов детектора и шумов от прохождения волоконной линии связи.

198 Для этого лучше всего подойдет полосовой фильтр, центральная частота которо-
199 го будет согласована с частотой модуляции. На рисунке 4 отображен синусоидальный
200 сигнал, который был отфильтрован с помощью цифрового фильтра для устранения

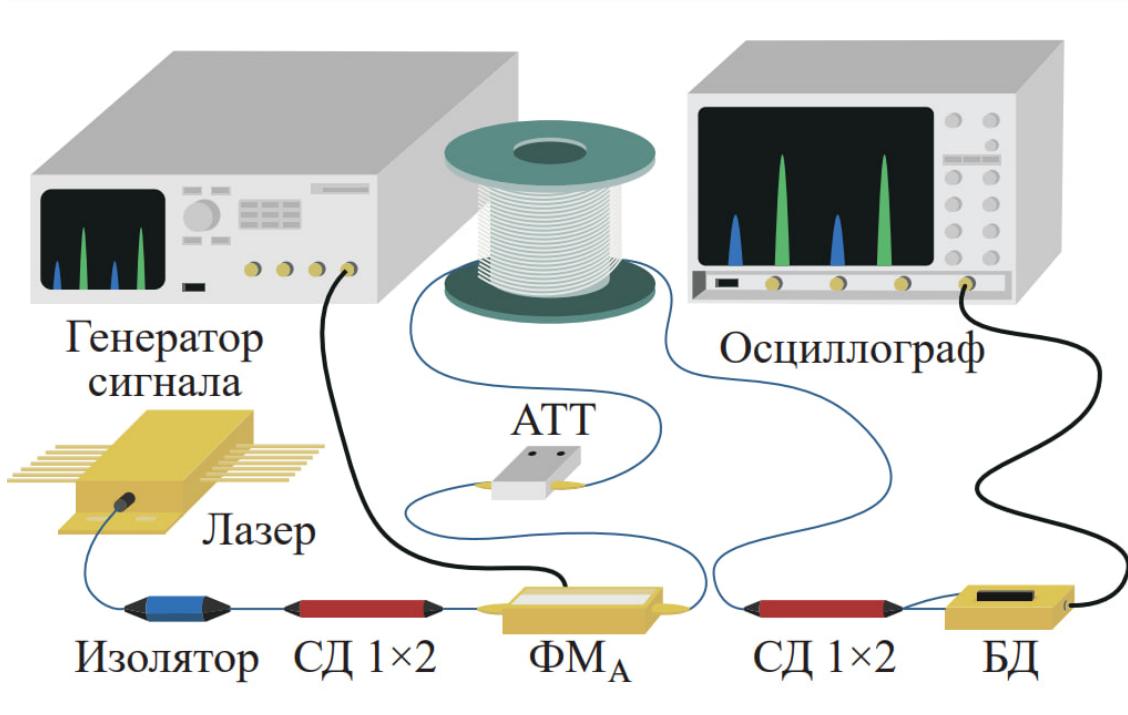


Рис. 2: Схема эксперимента гетеродинного приема

шумов. Частота сигнала на выходе балансного детектора равна частоте модуляции и несет в себе фазовый сдвиг, который кодируется на стороне отправителя. На рисунке 5 отображен спектр полученного сигнала. Она получена путем применением Быстрого Преобразования Фурье (БПФ) к данным с осциллографа, отображенных на рисунке 3. В результате были построены амплитудно-частотный спектр сигнала на выходе балансного детектора, он отображен на рисунке 5.

Как можно увидеть, в спектре наблюдается только одна гармоника на частоте модуляции. Для передачи информации в сигнал модуляции вносились фазовые сдвиги от 0 до 360 градусов с шагом 90, что соответствует QPSK типу модуляции. Результат измерений представлен на рисунке 6. Эти результаты получены с помощью БПФ, примененного к набору измерений для каждого фазового сдвига. В результате был получен фазово-частотный и амплитудно-частотный спектр, из которых извлекалась фаза и амплитуда гармоники соответственно. Дополнительно все амплитуды сигналов были нормированы. В результате получается набор сдвигов фаз, которым соответствует

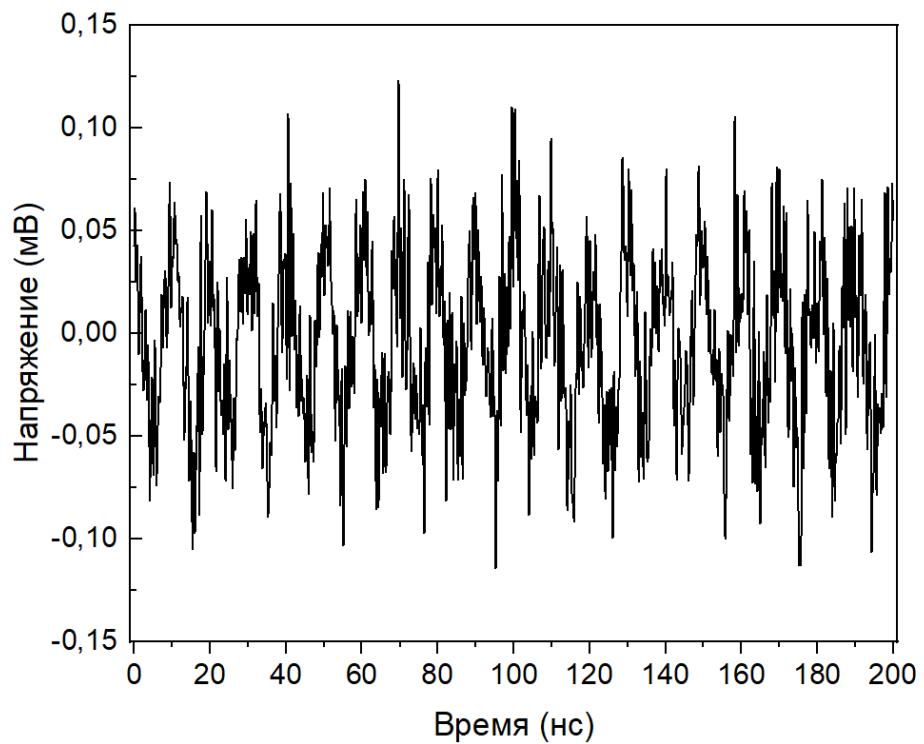


Рис. 3: Осциллографма выхода балансного детектора без фильтрации

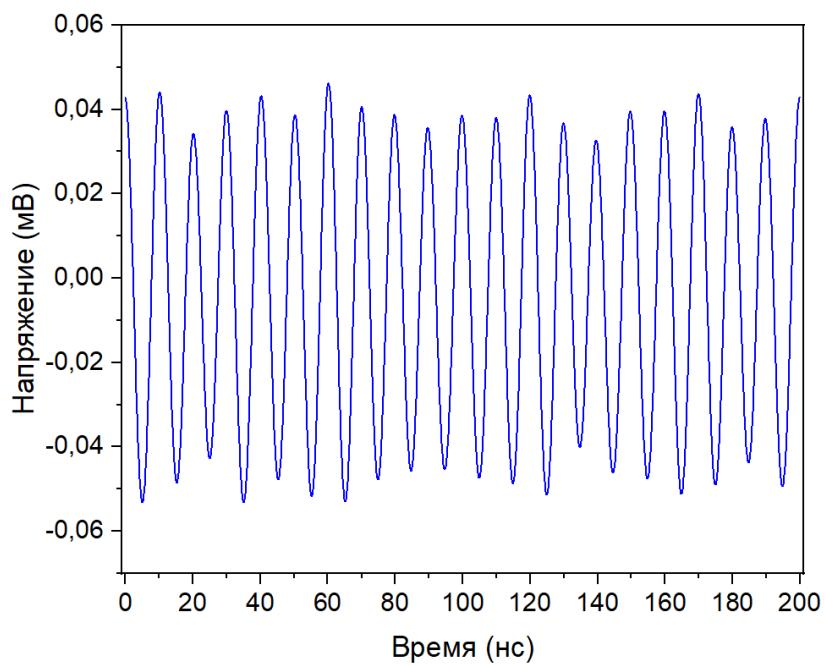


Рис. 4: Осциллографма выхода балансного детектора после фильтрации

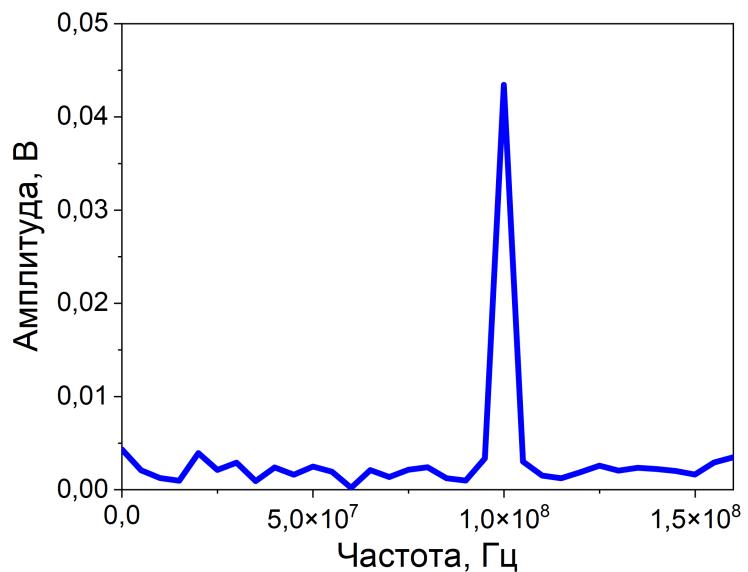


Рис. 5: Спектр сигнала на выходе балансного детектора

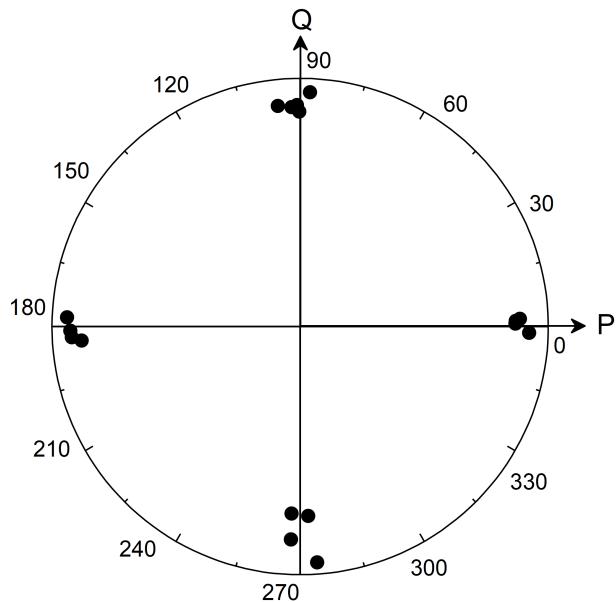


Рис. 6: Измеренные значения фазовых сдвигов

²¹⁵ двухбитовое значение информации [00, 01, 10, 11], передаваемое излучением на сторону

²¹⁶ приемника.

₂₁₇ **5 Заключение**

₂₁₈ Используя локальный осциллятор, переданный вместе с информационным сигналом,
₂₁₉ возможно детектировать информацию, закодированную в фазовом сдвиге, не прибегая
₂₂₀ к повторной модуляции. такой способ детектирования позволяет переносить сигнал с
₂₂₁ любым типом модуляции из оптической полосы частот в радиочастотную, где методы
₂₂₂ ее демодуляции отработаны и упрощены, что может существенно улучшить характе-
₂₂₃ ристики систем КРК и повысить их устойчивость к определенным типам атак. При
₂₂₄ регистрации непосредственно слабых когерентных состояний форма сигнала, сформи-
₂₂₅ рованного на балансном детекторе не изменится, однако существенно уменьшается его
₂₂₆ амплитуда, что потребует дополнительной постобработки для выделения сигнала из
₂₂₇ шумов, помимо предложенной в нашей работе цифровой фильтрации. Анализ в тер-
₂₂₈ минах квантовой оптики описан в работе [27], а работа [19] подтверждает сходимость
₂₂₉ моделей по результатам. Современные системы с гетеродинным детектированием поз-
₂₃₀ воляют передавать информацию на расстояния до 100 км, что позволит улучшить за-
₂₃₁ щищенность передаваемых объемов данных. Для данного эксперимента удалось рас-
₂₃₂пределить ключ на расстояние в 10 км при потерях 2 дБ. Масштабируемость данного
₂₃₃ эксперимента доказана предыдущими исследованиями. Это позволяет сделать вывод о
₂₃₄ том, что эффективность данного протокола будет ниже на 10 процентов относительно
₂₃₅ конвенциональных систем КРКНП, что будет компенсироваться гибкостью протокола и
₂₃₆ дополнительными возможностями.

₂₃₇ **6 Благодарности**

₂₃₈ Авторы статьи выражают благодарность Гончарову Роману Константиновичу за ак-
₂₃₉тивные консультации по работе. Исследование выполнено за счет гранта Российского

²⁴⁰ научного фонда (проект № 24-29-00786).

241 Список литературы

- 242 [1] T. Folger, The quantum hack, *Scientific American* 314 (2) (2016) 48–55.
- 243 [2] C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin
244 tossing, in: Proc. of IEEE Int. Conf. on Comp., Syst. and Signal Proc., Bangalore, India,
245 Dec. 10-12, 1984, 1984.
- 246 [3] P. W. Shor, J. Preskill, Simple proof of security of the bb84 quantum key distribution
247 protocol, *Physical review letters* 85 (2) (2000) 441.
- 248 [4] M. A. Nielsen, I. Chuang, *Quantum computation and quantum information* (2002).
- 249 [5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck,
250 D. Englund, T. Gehring, C. Lupo, C. Ottaviani, et al., Advances in quantum
251 cryptography, *Advances in optics and photonics* 12 (4) (2020) 1012–1236.
- 252 [6] X. Ma, B. Qi, Y. Zhao, H.-K. Lo, Practical decoy state for quantum key distribution,
253 *Physical Review A* 72 (1) (2005) 012326.
- 254 [7] L. Liu, Y. Wang, E. Lavie, C. Wang, A. Ricou, F. Z. Guo, C. C. W. Lim, Practical
255 quantum key distribution with non-phase-randomized coherent states, *Physical Review*
256 *Applied* 12 (2) (2019) 024048.
- 257 [8] A. Gaidash, G. Miroshnichenko, A. Kozubov, Subcarrier wave quantum key distribution
258 with leaky and flawed devices, *JOSA B* 39 (2) (2022) 577–585.
- 259 [9] E. Diamanti, A. Leverrier, Distributing secret keys with quantum continuous variables:
260 principle, security and implementations, *Entropy* 17 (9) (2015) 6072–6092.

- 261 [10] R. Goncharov, I. Vorontsova, D. Kirichenko, I. Filipov, I. Adam, V. Chistiakov,
262 S. Smirnov, B. Nasedkin, B. Pervushin, D. Kargina, et al., The rationale for the optimal
263 continuous-variable quantum key distribution protocol, Optics 3 (4) (2022) 338–351.
- 264 [11] Gleim, A. V., et al. "Secure polarization-independent subcarrier quantum key
265 distribution in optical fiber channel using BB84 protocol with a strong reference."Optics
266 express 24.3 (2016): 2619-2633.
- 267 [12] G. Miroshnichenko, A. Kozubov, A. Gaidash, A. Gleim, D. Horoshko, Security of
268 subcarrier wave quantum key distribution against the collective beam-splitting attack,
269 Optics express 26 (9) (2018) 11292–11308.
- 270 [13] Кынев, С. М., Чистяков В.В., Иночкин М.В, и др. "Перспективы построения систем
271 квантовой коммуникации на боковых частотах на отечественной компонентной ба-
272 зе Известия вузов. Радиофизика. 1 (67) (2024) 43–57.
- 273 [14] J. Mora, A. Ruiz-Alba, W. Amaya, A. Martínez, V. García-Muñoz, D. Calvo,
274 J. Capmany, Experimental demonstration of subcarrier multiplexed quantum key
275 distribution system, Optics letters 37 (11) (2012) 2031–2033.
- 276 [15] A. Bahrami, A. Lord, T. Spiller, Quantum key distribution integration with optical
277 dense wavelength division multiplexing: a review, IET Quantum Communication 1 (1)
278 (2020) 9–15.
- 279 [16] R. Kumar, H. Qin, R. Alléaume, Coexistence of continuous variable qkd with intense
280 dwdm classical channels, New Journal of Physics 17 (4) (2015) 043027.
- 281 [17] S. Kynev, V. Chistyakov, S. Smirnov, K. Volkova, V. Egorov, A. Gleim, Free-space
282 subcarrier wave quantum communication, in: Journal of Physics: Conference Series,
283 Vol. 917, IOP Publishing, 2017, p. 052003.

- 284 [18] E. Samsonov, R. Goncharov, A. Gaidash, A. Kozubov, V. Egorov, A. Gleim,
285 Subcarrier wave continuous variable quantum key distribution with discrete modulation:
286 mathematical model and finite-key analysis, *Scientific Reports* 10 (1) (2020) 10034.
- 287 [19] E. Samsonov, R. Goncharov, M. Fadeev, A. Zinoviev, D. Kirichenko, B. Nasedkin,
288 A. Kiselev, V. Egorov, Coherent detection schemes for subcarrier wave continuous
289 variable quantum key distribution, *JOSA B* 38 (7) (2021) 2215–2222.
- 290 [20] I. Suleiman, J. A. H. Nielsen, X. Guo, N. Jain, J. Neergaard-Nielsen, T. Gehring,
291 U. L. Andersen, 40 km fiber transmission of squeezed light measured with a real local
292 oscillator, *Quantum Science and Technology* 7 (4) (2022) 045003.
- 293 [21] S. Kleis, M. Rueckmann, C. G. Schaeffer, Continuous variable quantum key distribution
294 with a real local oscillator using simultaneous pilot signals, *Optics letters* 42 (8) (2017)
295 1588–1591.
- 296 [22] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola,
297 T. B. Pedersen, M. Kolb, B. Ömer, et al., Practical continuous-variable quantum key
298 distribution with composable security, *Nature communications* 13 (1) (2022) 4740.
- 299 [23] B. Qi, P. Lougovski, R. Pooser, W. Grice, M. Bobrek, Generating the local oscillator
300 “locally” in continuous-variable quantum key distribution based on coherent detection,
301 *Physical Review X* 5 (4) (2015) 041009.
- 302 [24] K. S. Mel’nik, N. M. Arslanov, O. I. Bannik, L. R. Gilyazov, V. I. Egorov, A. V. Gleim,
303 S. A. Moiseev, Using a Heterodyne Detection Scheme in a Subcarrier Wave Quantum
304 Communication System, *Bulletin of the Russian Academy of Sciences: Physics* 82 (8)
305 (2018) 1038–41.

- 306 [25] E. Samsonov, R. Goncharov, A. Gaidash, A. Kozubov, V. Egorov, A. Gleim,
307 Subcarrier wave continuous variable quantum key distribution with discrete modulation:
308 mathematical model and finite-key analysis, Scientific Reports. 10 (2020).
- 309 [26] R. Goncharov, E. Samsonov, A.D. Kiselev, Subcarrier wave quantum key distribution
310 system with gaussian modulation, Journal of Physics: Conference Series. 2103 (2021)
311 012169.
- 312 [27] Samsonov, E., Goncharov, R., Gaidash, A. et al. Subcarrier wave continuous variable
313 quantum key distribution with discrete modulation: mathematical model and finite-key
314 analysis. Sci Rep 10, 10034 (2020).

Optical-pumping attack on a quantum key distribution laser source

Maxim Fadeev,^{1,2,*} Anastasiya Ponosova,^{1,3} Qingquan Peng,⁴
Anqi Huang,⁴ Roman Shakhovoy,^{3,5} and Vadim Makarov^{1,6,3}

¹*Russian Quantum Center, Skolkovo, Moscow 121205, Russia*

²*ITMO University, St. Petersburg 197101, Russia*

³*NTI Center for Quantum Communications, National University of Science and Technology MISIS, Moscow 119049, Russia*

⁴*College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, People's Republic of China*

⁵*QRate, Moscow 143026, Russia*

⁶*Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain*

(Dated: September 8, 2025)

We report a new type of vulnerability based on a physical principle that has not been previously exploited in quantum hacking—optical pumping of a laser in practical implementations of quantum key distribution (QKD) systems. We show that it is possible to increase the pulse energy of a source laser diode not only by injection-locking it with external light near its emission wavelength of 1550 nm, but also by optically pumping it at a much shorter wavelength. We experimentally demonstrate a 10% increase in pulse energy when exposing the laser diode to continuous-wave (cw) laser light at 1310 nm with a power of 1.6 mW via its fiber pigtail. This effect may allow an eavesdropper to steal the secret key. A possible countermeasure is to install broadband optical filters and isolators at the source output and to characterise them during security certification.

I. INTRODUCTION

Quantum key distribution (QKD) is a technology to generate a true random secret key by remote users using single photons [1, 2]. The impossibility of compromising QKD protocols via direct measurement of single photons and independence of its security on computation algorithms make QKD an attractive cryptographic tool, especially with the rise of computational technologies. However, attempts at cryptanalysis of practical QKD implementations reveal many imperfections in their hardware. Active quantum-hacking strategies have been proposed that create vulnerabilities in a “healthy” system imperceptible for its legitimate users [3–7] or can exploit technical imperfections [8]. To meet hard requirements on cryptographic resistance, practical QKD implementations are studied and countermeasures to ensure physical security of the system hardware are developed and improved.

One of the imperfect devices in practical QKD systems is a photon source. Today, strongly attenuated laser pulses from semiconductor laser diodes (LDs) are used instead of true single-photon sources. In several studies, vulnerabilities in QKD are created by seeding Alice’s LD by Eve’s light injected through the quantum channel [9–11]. The attackers use laser light at about 1550 nm, which is near the LD operating wavelength. Injected power in the range of 100–160 nW can be sufficient to control the intensity of Alice’s pulses [9, 10]. Power as low as 1 nW might be enough to partially control the phase of Alice’s pulses [11].

In this paper, we investigate the effects of optical

pumping [12–14] of the QKD source of coherent radiation by 1310-nm illumination from the attacker Eve. This wavelength a particular case of a broad wavelength band that is absorbed by InGaAsP crystal within the laser [15]. Here, we select a wavelength of 1310 nm due to its prevalence and accessibility, which consequently increases the potential risks of the attack. We demonstrate that QKD source based on a 1550-nm gain-switched laser diode is vulnerable to an optical-pumping attack, which results in increase of the energy of pulses emitted by Alice and might compromise the security of the key.

Our study indicates that the sufficient attenuation of Eve’s light entirely mitigates the optical-pumping attack. However, QKD systems may be vulnerable to it due to the spectral selectivity of their passive countermeasures. The analysis of an industrial QKD system [7] reveals that active-state-preparation Alice modules may already be immune to this attack. Conversely, passive state-preparation QKD systems without modulators [16–18] are at greater risk due to the weaker requirements for passive countermeasures. But here we demonstrated the attack in principle at a single wavelength, while an adversary could exploit the entire absorption spectrum of the laser diode material. Effectiveness of the attack at different wavelengths will depend significantly on the practical implementation of a QKD system, including its LD architecture. Thus, comprehensive testing and evaluation are essential to certify QKD systems against this novel attack across the entire LD absorption band.

II. EXPERIMENTAL SETUP

Our experimental setup (Fig. 1) simulates a hacking scenario when Eve injects light into QKD source at a wavelength significantly shorter than the QKD operating

* mfadeev2022@gmail.com

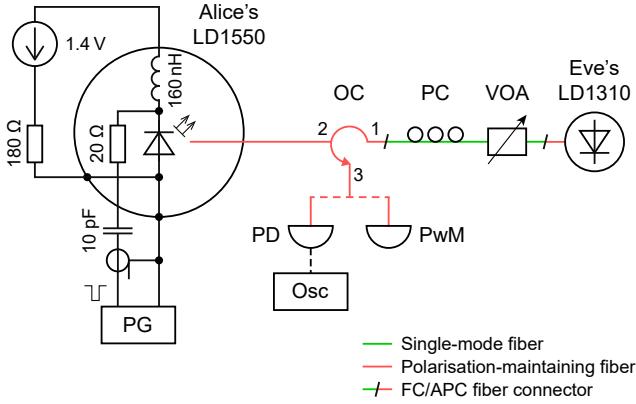


FIG. 1. Scheme of experiment. LD, laser diode; PG, pulse generator; OC, optical circulator; PD, photodiode; Osc, oscilloscope; PwM, power meter; PC, polarisation controller; VOA, variable optical attenuator. External electrical connections of LD1550 for pulsed operation are shown. Port 3 of OC is interchangeably connected to either PD or PwM.

one. A 1550-nm laser diode (LD1550; Agilecom WSL5-934010C4124-82) mimics Alice. However, contrary to the usual industry practice, it lacks a built-in isolator, in order to demonstrate effects using low-power attacker's source (otherwise the isolator would add about 10 dB attenuation at 1310 nm). We conduct measurements of QKD source characteristics in both cw and pulsed regimes. In cw regime, LD1550 is powered only by a laboratory power supply (Keysight E3648A). For operating in a gain-switching pulsed mode [19], the bias current provided by the power supply is 3 mA, and pulses from the pulse generator (Highland Technology P400) are applied at 10 MHz repetition rate. In this regime, LD1550 produces 700-ps-wide optical pulses, and has an average power of $14 \pm 0.1 \mu\text{W}$.

As an attacker, we use a 1310-nm laser diode (LD1310; Nolatex FPL-FBG-1310-14BF) in cw regime. Its emission is injected into LD1550 via a fiber-optic circulator. The output power is controlled with a variable optical attenuator (VOA; OZ Optics BB-100) in a range from 23 nW to 1.6 mW at port 2 of the optical circulator OC. This power is limited by the available maximum power of LD1310. A polarisation controller PC is adjusted to maximise Eve's power at port 2 of OC.

We investigate several characteristics of LD1550 under optical pumping by LD1310: its light-current characteristic and differential quantum efficiency in cw mode, pulse area and shape, and average power in the pulsed regime. The average optical power is measured using an optical power meter (Thorlabs PM400 with a photodiode sensor S154C). The backreflected light at 1310 nm makes a contribution to 1550-nm average power measurements at port 3 of OC. We correct for this by measuring the reflected power with LD1550 switched off and subtracting it from the total measured power in each experiment. This correction is stable and is of the same order of mag-

nitude or less than the effects observed. Pulse shape is recorded by a p-i-n photodiode (Laserscom PDI35-10G, 10 GHz bandwidth) connected to an oscilloscope (LeCroy 735Zi, 3.5 GHz bandwidth).

First, all the characteristics of LD1550 are measured before exposure. Then, they are characterised under exposure to a constant power level of LD1310 emission. In the experiments conducted on the cw 1550-nm LD, we gradually reduce Eve's injected power, beginning from its maximum value. We terminate the experiment when we observe several instances of unchanged characteristics in the 1550-nm LD operation under exposure. Conversely, in the tests of Alice's pulsed source, we gradually increase the 1310-nm power, starting from its minimum value.

III. EXPERIMENTAL RESULTS

We demonstrate how Eve can manipulate the characteristics of Alice's laser by 1310 nm wavelength radiation of different powers. We quantify the influence of Eve's pumping via differential quantum efficiency [20, 21]. It indicates how efficiently a laser medium converts injected electron-hole pairs into emitted photons. The theoretical limit for this coefficient is 1. Here we explore how additional optical pumping changes this efficiency.

Figure 2 demonstrates differential quantum efficiency of LD1550 depending on the pump power injected through its fiber pigtail. For thus, we measure the output power of LD1550 in cw regime depending on current under different power levels of pumping illumination (inset in Fig. 2). We extract the experimental value of optical power – current slope. We then calculate the differential quantum efficiency

$$\eta = \frac{2e}{\hbar\omega} \frac{dP}{dI}, \quad (1)$$

where e is the elementary charge, \hbar is the reduced Planck's constant, ω is the laser frequency, and dP/dI is the power–current slope averaged over 7 to 25 mA range.

Our data confirms that, at a fixed bias current, Alice's diode emits higher power under optical pumping. However, the change in the differential quantum efficiency is less than 1% in the investigated range of pumping power. With a decrease in pump power from 1.6 to 0.6 mW, the differential quantum efficiency decreases linearly, and then, under the lower pumping power of 140 μW and less, it becomes constant and remains the same even immediately after exposure but higher comparing to the pre-exposure level. It recovers to the initial value within a day. Both pre- and after-exposure levels are marked with dashed lines in Fig. 2. Additional research is required for an explanation of this effect.

This behaviour might result in an increase of the mean photon number emitted by Alice. To estimate the effect of optical pumping on QKD security, we measure LD1550's output characteristics in the pulsed regime in the presence of attack. Figure 3 shows the increase in

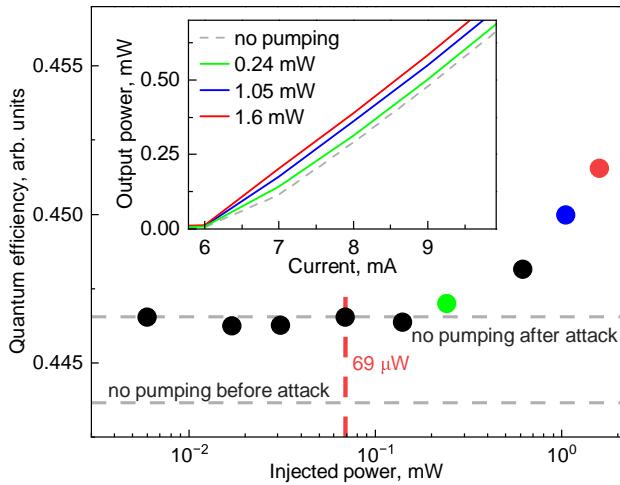


FIG. 2. Dependence of differential quantum efficiency on the injected cw power of Eve. “No pumping after attack” shows the level of differential quantum efficiency immediately after exposure. The inset shows measured light-current characteristics of LD1550 in cw regime.

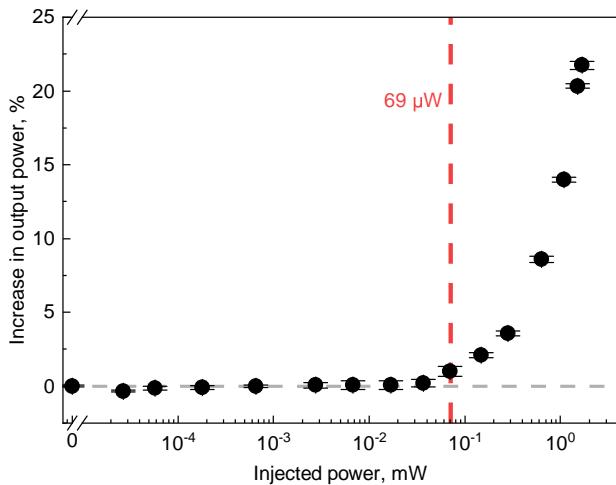


FIG. 3. Average output power of pulsed LD1550 under exposure to 1310-nm light. Standard deviation is less than 1%.

the average output power of Alice’s laser when injecting a different amount of power at 1310 nm. A notable and stable increase takes place when Eve’s pump power reaches 69 μ W. With a further pump power increase, the LD1550’s power rises linearly. It reaches 21.7% at pump power of 1.6 mW.

We also measure the shape of pulses emitted by Alice under Eve’s illumination. For each experimental point, we record 200k pulses, calculate the mean pulse area and its standard deviation, and draw a normalised pulse energy as the pulse area under exposure divided by the initial pulse area before exposure. The result is shown in Fig. 4. Here, the maximum increase in pulse energy is about 10% at the maximum LD1310 power. A sta-

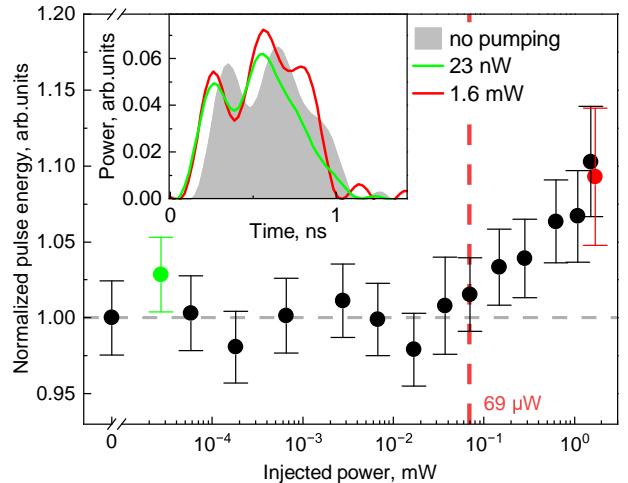


FIG. 4. Pulse energy of LD1550’s pulses under Eve’s illumination, normalised to their energy without pumping. Error bars present the standard deviation. Inset shows typical single-shot pulse shapes before exposure and under exposure to the minimum and maximum 1310-nm laser powers. The pulses change shape. Their mean timing, however, does not change; the time shift visible in the plot is the result of a random jitter of individual pulses.

ble increase in the pulse energy is observed starting from 140 μ W pump power. However, the pulse shape changes even under the lowest applied pump power of just 23 nW (inset in Fig. 4). The observed shifting of pulses under attack by about 75 ps is an order of measurement accuracy.

The behaviour of the pulse energy differs quantitatively from that of the average output power. In Fig. 4, even a decrease of the pulse energy is observed. This discrepancy may be caused by spontaneous luminescence of LD1550 under continuous pumping by LD1310, which cannot be distinguished in our measurements.

In summary, our experimental results show that just about 23 nW of 1310-nm light might change characteristics of Alice’s pulses, while about 140 μ W should reach her laser diode to induce an increase in its pulse energy.

IV. DISCUSSION

As shown in Sec. III, optical pumping induces an increase of both the average power and pulse energy. Let us discuss the implications of each for QKD security.

Increase of average power. In our experiment done at a low duty cycle, we notice that the increase in average power under pumping is higher than the increase in pulse energy. The difference reaches 10% under the highest attacker’s power. This can be explained by an emission of LD1550 between signal pulses, induced by the optical pumping. However, the emission power between the pulses is about 1000 times lower than in the pulses. It

might be difficult for Eve to exploit.

Increase of pulse energy. This increases the mean photon number emitted. Its effect on the security of different QKD protocols is well-studied, particularly for the standard decoy-state BB84 and MDI QKD protocols [9]. For instance, in a typical BB84 system [22], an unaccounted increase of the pulse energy by 10% leads to an overestimate of the secret key rate by 11% at the distance of 40 km of fiber [9], which makes the QKD system insecure. Hereinafter, we present calculations indicating that the attack can be entirely mitigated by employing sufficient attenuation of the eavesdropper's light. With the implemented countermeasure, this attack will not increase Alice's pulse intensity and affect the secret key rate.

Countermeasures. To prevent the optical-pumping attack, different known techniques might be considered. They include real-time calibration of Alice's intensity using variable optical attenuators with feedback, monitoring incoming light from the quantum channel, using optical power limiting devices [11, 23, 24], and providing a sufficiently high total isolation [25] to suppress the injected light from the quantum channel to a safe level.

In our experiment, the 1310-nm pump power required to observe a stable increase of both differential quantum efficiency and 1550-nm pulse energy is about 140 μW (-8.5 dBm). It is several orders of magnitude higher comparing to the laser-seeding attacks [9–11]. Therefore, the optical-pumping attack should be easily preventable by a proper isolation level.

A major limiting factor for Eve is the power-handling ability of the quantum channel and of the last component in the QKD source setup. Owing to the lack of experimental and theoretical data on this, we assume that the last component in the QKD source is a fiber-optic isolator and its damage threshold at 1310 nm equals that at 1550 nm, which is on order of 4 W (36 dBm) [25]. Then, Alice needs isolation at 1310 nm just above 44.5 dB to prevent the optical-pumping attack. Meanwhile, a Raman fiber laser based on a standard single-mode fiber (OFS SMBD0980B) of about 250 W cw power at 1310 nm is reported in [26]. In this case, the required isolation is 62.5 dB.

The estimated safe isolation boundaries are significantly lower than the typical isolation at 1550 nm of practical active-state-preparation Alice modules in their backward direction [7, 27, 28]. Unfortunately, systems might be vulnerable to the optical-pumping attack owing to the spectral dependency of the isolation of an optical scheme. Some of the passive elements used to prevent attacks, such as fiber-optic isolators and dense-wavelength-division multiplexers (DWDMs), often have vulnerabilities at wavelengths differing from their operating one [29–31]. Figure 5 shows typical wavelength-dependence of loss of 1550-nm telecommunication fiber-optic isolators and DWDM near 1310 nm. At 1550 nm, a typical single-stage isolator provides isolation of about 30 dB [25] and dual-stage isolator of about 50 dB. At 1310 nm, they

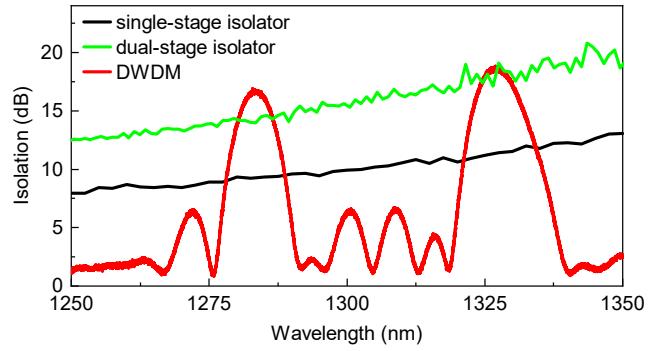


FIG. 5. Spectral characteristics near 1310 nm of typical 1550-nm fiber-optic isolators in backward direction and a dense-wavelength-division multiplexer (DWDM; Pointech DWDM-1T-MOD777-34) measured from its common port to the port of channel 34.

provide isolation of only about 10 and 15 dB. DWDM filters also have the same issue with the lack of isolation outside their operating range, as shown in Fig. 5. Their isolation at 1310 nm between the common input and channel output fluctuates around a few decibel. So, the spectral dependence of the system components might open a loophole for Eve to conduct the optical-pumping attack and should be considered in the system design.

However, if the QKD system lacks modulators, it is not susceptible to the light-injection attacks and might not have enough isolation installed, such as passive-state-preparation schemes [16, 22, 33–37]. Then it's important to ensure it is protected against the optical-pumping attack.

V. RISK EVALUATION FOR A PRACTICAL QKD IMPLEMENTATION

We estimate the success of the optical-pumping attack on an industrial-prototype prepare-and-measure QKD system, on the example of a real optical scheme of Alice produced by QRate [38] that is analysed in detail in [7]. Figure 6 shows it. Alice uses intensity and phase modulators IM and PM1 to prepare her states, and isolators Iso1 and Iso2 to protect them against the Trojan-horse attack. Laser diode LD1 emits signal pulses and is the target of our attack. The following calculations consider the optical path of Eve's light to it. The total isolation at 1310 nm is calculated as a sum of loss in backward direction of each component, and is

$$\alpha_{1310} = \alpha_{\text{Iso2}} + \alpha_{\text{Iso1}} + \alpha_{\text{DWDM2}} + \alpha_{\text{Att}} + \alpha_{\text{VOA1}} + \alpha_{\text{DWDM1}} + \alpha_{\text{BS}} + \alpha_{\text{PM1}} + \alpha_{\text{IM}} + \alpha_{\text{LD1}}, \quad (2)$$

where α_{Iso} is the isolation value of the optical isolator at 1310 nm wavelength, α_{LD1} is the isolation of LD1's built-in isolator, α_{DWDM} , α_{Att} , α_{VOA1} , α_{BS} , α_{PM1} , and α_{IM} are insertion losses of components in Fig. 6.

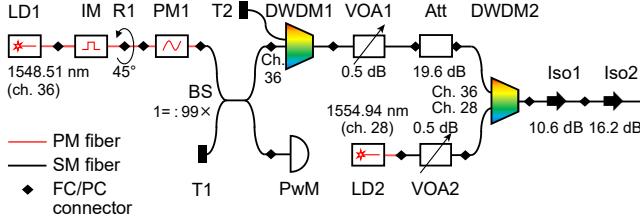


FIG. 6. Optical scheme of a commercial QKD transmitter [7]. LD, laser diode; IM, intensity modulator; R, FC/PC connector with 45° rotation; PM, phase modulator; T, optical terminator; BS, beamsplitter; DWDM, dense-wavelength-division multiplexer; Ch., DWDM channel number; VOA, variable optical attenuator; PwM, power meter; Att, fixed attenuator; Iso, polarisation-independent isolator.

The isolation values at 1310 nm used for the calculation in Eq. (2) are listed in Table I. To estimate Alice’s setup isolation at 1310 nm, we measure insertion loss of components similar to those listed in [7]. We cannot disclose model numbers for most of them, owing to our confidentiality agreements with QKD system manufacturers. They are standard off-the-shelf fiber-optic products. Fixed attenuator (Thorlabs FA20T) and fiber-optic 99:1 beamsplitter (Thorlabs TW1550R1A2) specify loss at 1310 nm in their data sheets. A phase modulator based on Ti-diffused lithium niobate is characterised using our PwM and LD1310. Insertion loss of IM is assumed to be the same as that of PM. All the other components are characterised using a broadband light source and optical spectrum analyser (Hewlett-Packard 70004A), using methodology from Appendix E of [7]. The isolation of LD1’s built-in isolator is assumed to be the same as that of the single-stage isolator.

The total calculated isolation at 1310 nm is 97.6 dB, which is higher comparing to our maximum required value of 62.5 dB. Thus, the system is resilient against

TABLE I. Insertion loss of components similar to those from the QKD system [7] measured at 1310 nm. The variable optical attenuator can be set anywhere in the range 0.5–30 dB, of which the worst case of 0.5 dB is assumed here.

Element	Symbol	Loss, dB
Isolator 2	α_{Iso2}	16.2
Isolator 1	α_{Iso1}	10.6
DWDM2	α_{DWMD2}	3.0
Fixed attenuator	α_{Att}	19.6
Variable optical attenuator	α_{VOA1}	0.5
DWDM1	α_{DWMD1}	4.1
Beamsplitter	α_{BS}	24.0
Phase modulator	α_{PM1}	4.5
Intensity modulator	α_{IM}	4.5
LD1’s built-in isolator	α_{LD1}	10.6

the optical-pumping attack at 1310 nm. However, to ensure its security, both the efficiency of optical pumping and insertion loss of the source components must be characterised in a very wide spectral range [7?].

VI. CONCLUSION

We have proposed a new kind of attack on real QKD systems—the optical-pumping attack on the transmitter. It allows the eavesdropper to increase the intensity of the prepared states by injecting light into Alice at a wavelength corresponding to a semiconductor absorption band of her laser source. We experimentally demonstrate 10% increase in pulse energy of 1550-nm Alice’s source using Eve’s injected power of 1.6 mW at 1310 nm.

Our study shows that the power required for the success of this attack is at least three orders of magnitude higher than that of the laser-seeding attack. At the same time, characteristics of passive countermeasures in practical QKD systems are wavelength-dependent and might be ineffective against this type of attack in a wide spectral range. Thus, the optical-pumping attack should be considered a possible threat to QKD security. As part of the certification process, QKD systems must be tested to confirm their countermeasures effectively mitigate this attack.

Finally, we analyse the risk of this attack on the example of the industrial QKD system [7, 38]. The analysis indicates that systems with proper protection against the light-injection attacks may be resilient against the optical-pumping attack with existing countermeasures. Therefore, the latter should be strongly considered in QKD systems that do not require protection against the light-injection attacks, such as the systems using passive state preparation [16–18, 22, 33–37].

Funding: Russian Science Foundation (grant 21-42-00040). Q.P. and A.H. acknowledge funding from the National Natural Science Foundation of China (grant 62371459) and the Innovation Program for Quantum Science and Technology (grant 2021ZD0300704). V.M. acknowledges funding from the Galician Regional Government (consolidation of research units: atlanttic and own funding through the “Planes Complementarios de I+D+I con las Comunidades Autónomas” in Quantum Communication), MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1), and the “Hub Nacional de Excelencia en Comunicaciones Cuánticas” funded by the Spanish Ministry for Digital Transformation and the Public Service and the European Union NextGenerationEU.

Author contributions: R.S., A.H., and Q.P. assisted in planning the experiment. M.F. and A.P. conducted the experiment. R.S. and V.M. supervised the study. All authors analysed the results and contributed to writing the manuscript.

Disclosures: The authors declare no conflicts of interest.

Data availability: Data underlying the results presented in this paper are not publicly available at this time, but may be obtained from the authors upon reasonable request.

Appendix A: Supplementary materials

Distributed feedback (DFB) laser diodes are widely used in quantum key distribution (QKD) systems because they offer low noise, high-frequency stability, and a narrow linewidth. The DFB laser achieves high-performance emission by combining an active medium (gain semiconductor) with a diffraction grating along the entire length of the cavity. This design allows for precise selection of the wavelength.

An injection current transfers carriers to the active region of LD. When this current reaches a sufficient level to create a population inversion, lasing—or stimulated emission—occurs as a result of carrier recombination: electrons from the conduction band recombine with holes in the valence band. Optical pumping excites electrons from the valence band into the conduction band inside the active region of LD. Figure A.1 provides a schematic illustration of the conduction and valence bands. For a detailed explanation of the actual band structure in InGaAsP materials typically applied in 1550-nm laser diodes, refer to [39].

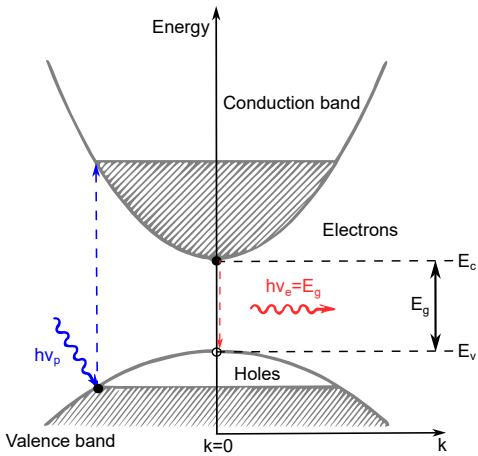


FIG. A.1. Schematic view of the conduction and valence bands in semiconductor material. The pump light is in blue, and the emission light is in red. E_c represents the energy level at the bottom of the conduction band, and E_v the energy level at the top of the valence band.

In the presence of injection current alone, the laser rate equation for the carrier number N is expressed as follows:

$$\dot{N} = I/e - N/\tau_e - QG/(\Gamma\tau_{ph}) \quad (\text{A.1})$$

The effect of continuous optical pumping at a wavelength of 1310 nm is reduced to the addition of the optical pumping rate R_{opt} to the right hand side of the laser rate equation for the carrier number N . The system of rate equations can thus be written as follows:

$$\begin{aligned} \dot{N} &= I/e + R_{\text{opt}} - N/\tau_e - QG/(\Gamma\tau_{ph}), \\ \dot{Q} &= (G - 1)Q/\tau_{ph} + C_{\text{sp}}N/\tau_e, \end{aligned} \quad (\text{A.2})$$

where Q is the normalized electric field intensity corresponding to the photon number inside the laser cavity and related to the output power by $P = Q\eta\hbar\omega_0/(2\Gamma\tau_{ph})$, where $\hbar\omega$ is the photon energy (ω is the central angular frequency of the 1550-nm laser), η is the differential quantum output, Γ is the confinement factor, τ_{ph} is the photon lifetime inside the cavity, and the factor 1/2 takes into account that the output power is measured only from one facet. Onwards, I is the pump current, e is the absolute value of the electron charge, τ_e is the effective lifetime of the electron, the factor C_{sp} corresponds to the fraction of spontaneously emitted photons that end up in the active mode, and the dimensionless gain G is defined by

$$G = \frac{N - N_0}{N_{\text{th}} - N_0} \frac{1}{\sqrt{1 + 2\gamma_Q Q}}, \quad (\text{A.3})$$

where N_0 and N_{th} are the carrier numbers at transparency and threshold, respectively, and γ_Q is the dimensionless gain compression factor. The optical pumping rate, in turn, can be written as

$$R_{\text{opt}} = \epsilon_{\text{opt}} \frac{P_{1310}}{\hbar\omega_{1310}}, \quad (\text{A.4})$$

where ϵ_{opt} — is the pumping efficiency, P_{1310} is the optical pumping power, and $\hbar\omega_{1310}$ is the corresponding photon energy.

The actual characteristics of laser diodes required for near-practical simulation, such as the absorption cross-sections of the semiconductor, the material properties, and the coupling efficiency with optical fibre, are unknown because manufacturers keep this information confidential. For simulations we have used laser and pump current parameters listed in Table A.1. Simulations of the output signal with and without optical pumping are shown in Fig. A.2. It was assumed that the pump current is a sequence of rectangular pulses and can be written as $I(t) = I_b + I_p(t)$, where I_b is the bias current, and the modulation current $I_p(t)$ varied from 0 to I_p^{\max} (the peak-to-peak value of the modulation current).

[1] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin, Experimental quantum cryptography, *J. Cryptology* **5**, 3 (1992).

tology **5**, 3 (1992).

TABLE A.1. Simulation parameters.

Parameter	Value
Bias current I_b , mA	6.0
Maximum pump current I_p^{\max} , mA	20.0
Carrier timelife τ_e , ns	1.0
Photon timelife τ_{ph} , ps	3.0
Pump current pulse width, ns	0.2
Pulse repetition rate, GHz	2.5
Confinement factor Γ	0.12
Threshold carrier number N_{th}	6.5×10^7
Transparency level N_0	5.5×10^7
Spontaneous emissions fraction C_{sp}	10^{-5}
Gain compression factor γ_Q	1.0×10^{-6}
Pumping efficiency ϵ_{opt}	0.1

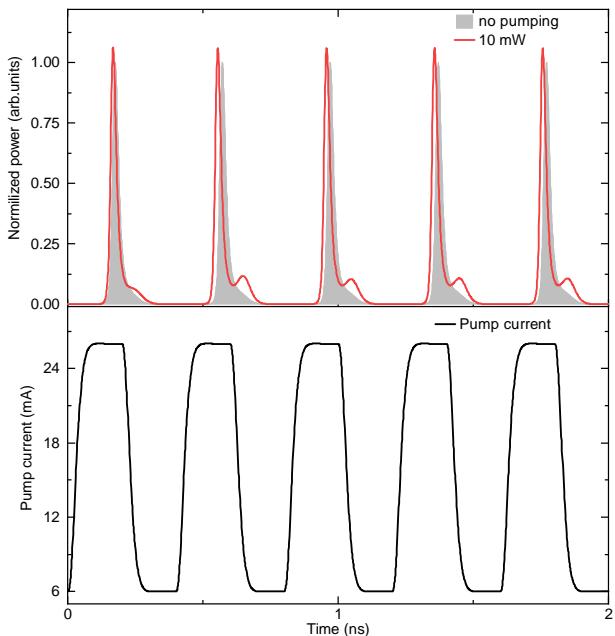


FIG. A.2. Simulations of the output signal with and without optical pumping.

- [2] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, Quantum key distribution based on private states: Unconditional security over untrusted channels with zero quantum capacity, *IEEE Trans. Inf. Theory* **54**, 2604 (2008).
- [3] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, *Nat. Photonics* **8**, 595 (2014).
- [4] A. Dixon, J. Dynes, M. Lucamarini, B. Fröhlich, A. Sharpe, A. Plews, W. Tam, Z. Yuan, Y. Tanizawa, H. Sato, *et al.*, Quantum key distribution with hacking countermeasures and long term field trial, *Sci. Rep.* **7**, 1978 (2017).
- [5] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev.*

- Mod. Phys. **92**, 025002 (2020).
- [6] S. Sun and A. Huang, A review of security evaluation of practical quantum key distribution system, *Entropy* **24**, 260 (2022).
- [7] V. Makarov, A. Abrikosov, P. Chaiwongkhot, A. K. Fedorov, A. Huang, E. Kiktenko, M. Petrov, A. Ponosova, D. Ruzhitskaya, A. Tayduganov, D. Trefilov, and K. Zaitsev, Preparing a commercial quantum key distribution system for certification against implementation loop-holes, *Phys. Rev. Appl.* **22**, 044076 (2024).
- [8] A. Gnanapandithan, L. Qian, and H.-K. Lo, Hidden multidimensional modulation side channels in quantum protocols, *Phys. Rev. Lett.* **134**, 130802 (2025).
- [9] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Laser-seeding attack in quantum key distribution, *Phys. Rev. Appl.* **12**, 064043 (2019).
- [10] X.-L. Pang, A.-L. Yang, C.-N. Zhang, J.-P. Dou, H. Li, J. Gao, and X.-M. Jin, Hacking quantum key distribution via injection locking, *Phys. Rev. Appl.* **13**, 034008 (2020).
- [11] V. Lovic, D. G. Marangon, P. R. Smith, R. I. Woodward, and A. J. Shields, Quantified effects of the laser-seeding attack in quantum key distribution, *Phys. Rev. Appl.* **20**, 044005 (2023).
- [12] O. Svelto, Pumping processes, in *Principles of Lasers* (Springer US, Boston, MA, 1998) pp. 201–248.
- [13] T. Okamoto, N. Nunoya, Y. Onodera, T. Yamazaki, S. Tamura, and S. Arai, Optically pumped membrane BH-DFB lasers for low-threshold and single-mode operation, *IEEE J. Sel. Top. Quantum Electron.* **9**, 1361 (2003).
- [14] M. Guina, A. Rantamäki, and A. Häkkinen, Optically pumped VECSELs: review of technology and progress, *J. Phys. D: Appl. Phys.* **50**, 383001 (2017).
- [15] M. Levinshtein, S. Rumyantsev, and M. Shur, *Handbook Series on Semiconductor Parameters, Vol. 2: Ternary and Quaternary A_3B_5 Semiconductors* (World Scientific Publishing, Singapore, 1999).
- [16] V. Zapatero, W. Wang, and M. Curty, A fully passive transmitter for decoy-state quantum key distribution, *Quantum Sci. Technol.* **8**, 025014 (2023).
- [17] C. Hu, W. Wang, K.-S. Chan, Z. Yuan, and H.-K. Lo, Proof-of-principle demonstration of fully passive quantum key distribution, *Phys. Rev. Lett.* **131**, 110801 (2023).
- [18] F.-Y. Lu, Z.-H. Wang, V. Zapatero, J.-L. Chen, S. Wang, Z.-Q. Yin, M. Curty, D.-Y. He, R. Wang, W. Chen, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, Experimental demonstration of fully passive quantum key distribution, *Phys. Rev. Lett.* **131**, 110802 (2023).
- [19] O. Svelto, Transient laser behavior, in *Principles of Lasers* (Springer US, Boston, MA, 2010) pp. 313–373.
- [20] D. T. Cassidy, Differential quantum efficiency of a homogeneously broadened injection laser, *Appl. Opt.* **23**, 2870 (1984).
- [21] T. Tomiyasu, T. Hiratani, D. Inoue, N. Nakamura, K. Fukuda, T. Uryu, T. Amemiya, N. Nishiyama, and S. Arai, High-differential quantum efficiency operation of GaInAsP/InP membrane distributed-reflector laser on Si, *Appl. Phys. Express* **10**, 062702 (2017).
- [22] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, Quantum cryptography with-

- out detector vulnerabilities using optically-seeded lasers, *Nat. Photonics* **10**, 312 (2016).
- [23] G. Zhang, I. W. Primaatmaja, J. Y. Haw, X. Gong, C. Wang, and C. C. W. Lim, Securing practical quantum communication systems with optical power limiters, *PRX Quantum* **2**, 030304 (2021).
- [24] Q. Peng, B. Gao, D. Wang, Q. Liao, Z. Zuo, H. Zhong, A. Huang, and Y. Guo, Defending against a laser-seeding attack on continuous-variable quantum key distribution using an improved optical power limiter, *Phys. Rev. A* **108**, 052616 (2023).
- [25] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, Protecting fiber-optic quantum key distribution sources against light-injection attacks, *PRX Quantum* **3**, 040307 (2022).
- [26] A. Grimes, A. Hariharan, I. Sun, and J. W. Nicholson, High-power, high-efficiency, semi-random Raman fiber lasers, in *Proc. SPIE 11981, Fiber Lasers XIX: Technology and Systems* (2022) p. 119810J.
- [27] H. Tan, W. Li, L. Zhang, K. Wei, and F. Xu, Chip-based quantum key distribution against trojan-horse attack, *Phys. Rev. Appl.* **15**, 064038 (2021).
- [28] S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, and V. Makarov, An approach for security evaluation and certification of a complete quantum communication system, *Sci. Rep.* **11**, 5110 (2021).
- [29] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Risk analysis of Trojan-horse attacks on practical quantum key distribution systems, *IEEE J. Sel. Top. Quantum Electron.* **21**, 6600710 (2015).
- [30] B. A. Nasedkin, I. M. Filipov, A. O. Ismagilov, V. V. Chistiakov, F. D. Kiselev, A. N. Tsyplkin, and V. I. Egorov, Analyzing transmission spectra of fiber-optic elements in the near IR range to improve the security of quantum key distribution systems, *Bull. Russ. Acad. Sci.: Phys.* **86**, 1164 (2022).
- [31] A. V. Borisova, B. D. Garmaev, I. B. Bobrov, S. S. Negodyaev, and I. V. Sinil'shchikov, Risk analysis of countermeasures against the Trojan-horse attacks on quantum key distribution systems in 1260–1650 nm spectral range, *Opt. Spectrosc.* **128**, 1892 (2020).
- [32] H. Tan, M. Petrov, W. Zhang, L. Han, S.-K. Liao, V. Makarov, F. Xu, and J.-W. Pan, Wide-spectrum security against attacks in quantum key distribution (2024), unpublished.
- [33] Z. L. Yuan, B. Fröhlich, M. Lucamarini, G. L. Roberts, J. F. Dynes, and A. J. Shields, Directly phase-modulated light source, *Phys. Rev. X* **6**, 031044 (2016).
- [34] G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, and A. J. Shields, A direct GHz-coded phase and intensity modulated transmitter applied to quantum key distribution, *Quantum Sci. Technol.* **3**, 045010 (2018).
- [35] T. K. Paraïso, I. D. Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, A modulator-free quantum key distribution transmitter chip, *npj Quantum Inf.* **5**, 42 (2019).
- [36] W. Wang, R. Wang, C. Hu, V. Zapatero, L. Qian, B. Qi, M. Curty, and H.-K. Lo, Fully passive quantum key distribution, *Phys. Rev. Lett.* **130**, 220801 (2023).
- [37] Y. Kurochkin, M. Papadovasilakis, A. Trushechkin, R. Piera, and J. A. Grieve, A practical transmitter device for passive state BB84 quantum key distribution, arXiv (2024), arXiv:2405.08481 [quant-ph].
- [38] Qrate QKD312, Hardware and software system for quantum key distribution (QKD), https://goqrate.com/projects/qrate_qkd312/, visited 10 August 2025.
- [39] Y. A. Goldberg and N. M. Schmidt, Gallium indium arsenide phosphide ($\text{Ga}_x\text{In}_{1-x}\text{As}_y\text{P}_{1-y}$), in *Handbook Series on Semiconductor Parameters*, Vol. 2, edited by M. Levinshtein, S. Rumyantsev, and M. Shur (World Scientific, London, 1999) Chap. 7, pp. 153–179.