МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА

На правах рукописи

Сущев Иван Сергеевич

Исследование комбинированных атак на волоконные системы квантового распределения ключей

Специальность 1.3.19. Лазерная физика

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата физико-математических наук

Москва — 2026

Диссертация подготовлена на кафедре квантовой электроники физического факультета МГУ имени М. В. Ломоносова.

Научный руководитель: **Молотков Сергей Николаевич,**
доктор физико-математических наук

Официальные оппоненты: **Арсеев Петр Иварович,**
доктор физико-математических наук, профессор, член-корреспондент РАН, Физический институт им. П. Н. Лебедева Российской академии наук, отделение теоретической физики им. И. Е. Тамма, главный научный сотрудник

Калачев Алексей Алексеевич,
доктор физико-математических наук, доцент, член-корреспондент РАН, Федеральный исследовательский центр «Казанский научный центр Российской академии наук», дирекция, директор

Махлин Юрий Генрихович,
доктор физико-математических наук, доцент, член-корреспондент РАН, Национальный исследовательский университет «Высшая школа экономики», Международная лаборатория физики конденсированного состояния, заведующий лабораторией

Защита состоится «21» октября 2026 г. в 16 часов 30 минут на заседании диссертационного совета МГУ.013.4 Московского государственного университета имени М. В. Ломоносова по адресу: 119991, Москва, Ленинские горы, д. 1, стр. 62, корпус нелинейной оптики, аудитория им. С.А. Ахманова.

E-mail: diss.sov.31@physics.msu.ru.

С диссертацией можно ознакомиться в отделе диссертаций Научной библиотеки МГУ имени М.В. Ломоносова (Ломоносовский просп., д. 27) и на портале: https://dissovet.msu.ru/dissertation/4043.

Автореферат разослан « » сентября 2026 года.

Ученый секретарь
диссертационного совета МГУ.013.4
кандидат физико-математических наук Коновко А. А.

Общая характеристика работы

Квантовая криптография позволяет решить проблему безопасного обмена информацией путем квантового распределения ключей (КРК) между двумя сторонами (Алисой и Бобом), открывая возможность для применения симметричного шифрования. Секретность ключей обеспечивается фундаментальными законами квантовой физики и не требует дополнительных допущений о вычислительных возможностях нарушителя (Евы), в отличие от ассиметричной схемы шифрования, уязвимой к алгоритмам взлома с использованием квантового вычислителя [1; 2]. В 1949 году К. Шенноном было определено, что для абсолютной криптографической стойкости, криптосистема должны удовлетворять следующим принципам [3]:

1. секретный ключ должен представлять собой истинно случайную последовательность;
2. длина ключа должна быть не меньше размера шифруемого сообщения;
3. каждый секретный ключ должен использоваться лишь единожды.

Следование этим правилам ставит сразу две физические проблемы: необходимость в источниках истинно случайных последовательностей и способе быстрого и надежного распределения ключей между пользователями. Как выяснилось, квантовая физика решает обе эти проблемы. Во-первых, единственным источником истинной случайности служат именно квантовые системы. В отличие от классических систем, подчиняющихся детерминистическим уравнениям (например, уравнениям Гамильтона), квантовые системы имеют принципиально стохастическую природу. Любое возникновение вероятностных величин в классической теории обуславливается недостатком знаний о параметрах системы или сложностью точного решения систем уравнений. Квантовая теория постулирует существование систем, полное описание которых не исключает неопределенность исхода измерения над ними. Отсутствие так называемых скрытых параметров, предписывающих детерминированный результат измерений, в такого рода системах многократно экспериментально подтверждалось при помощи проверки нарушения неравенств Белла [4]. Так, Алану Аспе в 2022 году была присуждена Нобелевская премия по физике за экспериментальное установление нарушений неравенств Белла [5; 6].

Во-вторых, квантовые состояния являются идеальным средством защищенной передачи информации, благодаря таким свойствам, как невозможность скопировать неизвестное квантовое состояние, выраженное в теореме о «запрете клонирования» [7], и невозможность достоверно различить неортогональные квантовые состояния. Воспользовавшись этими свойствами квантовых систем, Чарльз Беннет и Жиль Брассар в 1984 году предложили первый в истории протокол квантового распределения ключей

BB84 [8], положив начало квантовой криптографии. Биты ключа кодировались состояниями поляризации фотона в двух взаимно неортогональных базисах. Распределение ключей осуществлялось путем распространения фотонов от источника Алисы к измерительной станции Боба.

В последующие годы квантовая криптография стало интенсивно развиваться. Основной вклад в ее развитие внесло значительное усовершенствование элементной базы, необходимой для построения линий квантовой связи. Можно выделить улучшение характеристик и распространение оптоволоконных каналов, служащих средой для распространения оптических импульсов, прогресс в области детекторов одиночных фотонов (детекторы на базе лавинных фотодиодов стали настольным прибором в любой квантово-оптической лаборатории, а также появились новые сверхчувствительные сверхпроводниковые детекторы с предельно низким уровнем шума) и достижения в области генерации одиночных фотонов и лазерных импульсов. На сегодняшний день квантовая криптография заняла свою нишу в отрасли информационной безопасности, коммерческие системы КРК распространяются по всему миру. Системы КРК производятся в том числе и в России. В 2022 году российская квантово-криптографическая система выработки и распределения ключей впервые получила сертификат регулятора в области криптографической защиты информации.

Актуальность темы. Несмотря на безусловную криптографическую стойкость, заявляемую квантово-криптографическими протоколами, техническая реализация систем КРК может быть связана с рядом недостатков, что открывает нарушителю возможности по проведению различных атак. Исследования в области безопасности КРК, или квантового «хакинга», являются одним из важнейших направлений в современной квантовой криптографии. Атаки на системы КРК и меры противодействия им являются предметом множества научных работ, рассмотренных, например в обзорах [9—11]. В связи с появлением большого числа различных систем КРК остро встает вопрос практического анализа их безопасности. Для оценки реальных рисков безопасности КРК, такой анализ должен охватывать все возможные уязвимости исследуемой системы в совокупности.

Степень разработанности темы является достаточно высокой. Вопросы практической безопасности систем КРК начали исследоваться практически сразу, при первой экспериментальной демонстрации сеанса выработки квантового ключа в 1992 году [12]. В последующие годы ряд работ был посвящен доказательству стойкости протоколов КРК, а также обеспечению безопасности КРК при наличии несовершенств технической реализации. Однако, опубликованные работы были посвящены исследованию безопасности лабораторных или учебных систем КРК с точки зрения отдельных уязвимостей. В настоящей работе упор сделан на исследование

безопасности реальных систем КРК при совокупном рассмотрении уязвимостей.

Целью настоящей работы является разработка методов практического анализа рисков безопасности волоконных систем КРК в условиях проведения нарушителем комбинированных атак, а также применение разработанных методов к реальной волоконной системе КРК.

Для достижения поставленной цели были сформулированы следующие **задачи**:

1. Анализ влияния побочных каналов утечки информации произвольного вида на выполнение условия секретности КРК и выделение параметров, характеризующих данное влияние.
2. Разработка экспериментальных способов определения значений выделенных параметров побочных каналов утечки информации в системах КРК.
3. Применение разработанных теоретических и экспериментальных методов анализа побочных каналов утечки информации к реальной волоконной системе КРК.
4. Анализ влияния изменения параметров системы КРК на выполнение условия секретности КРК, в частности, при увеличении интенсивности легитимного излучения при проведении атаки с лазерным повреждением.
5. Анализ безопасности систем КРК в условиях увеличении интенсивности легитимного излучения с учетом реальных возможностей нарушителя.

Объектом исследования являются системы квантового распределения ключей. **Предметом исследования** являются способы практического анализа безопасности систем квантового распределения ключей при наличии несовершенств технической реализации.

Научная новизна:

1. Получен способ вычисления верхней границы информации, доступной нарушителю, при комбинировании унитарной коллективной атаки с атаками по побочным каналам с учетом произвольного вида квантовых состояний в побочных каналах.
2. Предложен способ измерения спектров пропускания волоконно-оптических компонентов в спектральном диапазоне 1100—1800 нм с динамическим диапазоном, превышающим 100 дБ.
3. Разработан широкополосный оптический рефлектометр, позволяющий проводить рефлектометрию волоконно-оптических схем в спектральном диапазоне 1100—1800 нм.
4. Проведен практический анализ безопасности реальной системы КРК в условиях комбинирования коллективной атаки с атакой активного оптического зондирования.

5. Рассмотрены атаки на многофотонную компоненту при увеличении интенсивности легитимного излучения, направленные на системы КРК, использующие метод «decoy state».
6. Построены атаки с безошибочными измерениями при увеличении интенсивности легитимного излучения, направленные на системы КРК, использующие метод «decoy state», реализуемые с использованием существующих технологий.

Научная и практическая значимость обусловлена возможностью использования результатов настоящей работы при разработке и создании систем КРК, а также при проведении сертификационных исследований систем КРК.

Методология научного исследования основана на широко используемых и испытанных методах выполнения эксперимента, проведения аналитических и численных расчетов. Аналитические расчеты были проведены с использованием опубликованных доказанных теорем, а также путем прямого вычисления. Численные расчеты для решения уравнений и минимизации параметров проводились с использованием методов численного перебора, а также методом золотого сечения. Для проведения экспериментальных исследований использовалось коммерческое оборудование, а именно, суперконтинуумный лазер с шириной спектра, превышающей спектральный диапазон 1100—1800 нм, акустооптические фильтры с шириной полосы 10 нм, управляемые с персонального компьютера, детектор одиночных фотонов на базе лавинного InGaAs-фотодиода с диапазоном чувствительности 1100—1800 нм, временно́й коррелятор электрических сигналов с разрешением до 100 пс, а также стандартные волоконно-оптические компоненты. Также использовалась коммерческая система КРК с возможностью извлечения отдельных составных частей. Управление экспериментальным стендом велось при помощи специализированного программного обеспечения с персонального компьютера. Система КРК исследовалась в выключенном состоянии.

Основные положения, выносимые на защиту:

1. Защищенность системы КРК, использующей протокол BB84, при наличии побочных каналов утечки информации достигается путем сокращения выработанного ключа на этапе усилении секретности на величину, равную максимальному значению утечки информации для протокола BB84, возникающей при комбинировании нарушителем унитарной коллективной атаки с атаками по побочным каналам. Данная величина может быть вычислена для заданной вероятности ошибочного измерения на приемной стороне как функция от интенсивностей излучения в каждом из побочных каналов без определения явного вида квантовых состояний в побочных каналах.

2. Измерение спектров пропускания пассивных волоконно-оптических элементов с использованием источника суперконтинуума, перестраиваемых фильтров и детектора одиночных фотонов в совокупности с проведением широкополосной рефлектометрии с использованием источника суперконтинуума, перестраиваемых фильтров, временно́го коррелятора электрических сигналов и детектора одиночных фотонов позволяют определить интенсивность излучения в активном оптическом побочном канале для волоконных систем КРК в спектральном диапазоне 1100—1800 нм и вычислить максимальное значение утечки информации по побочным каналам в данном диапазоне.
3. Применение метода «decoy state» обеспечивает защищенность системы КРК, использующей протокол BB84, от атак с безошибочными измерениями, основанными на различении закодированных состояний при помощи оборудования, эквивалентного приемнику КРК с пассивным выбором базиса. При несанкционированном увеличении интенсивности излучения передатчика КРК в некоторое число раз защищенность системы сохраняется вплоть до достижения порогового значения, определяемого параметрами метода «decoy state». Для типичных параметров метода «decoy state» при использовании нарушителем идеальных детекторов, данные пороговые значения лежат в диапазоне 10—20 дБ, что отвечает ранее продемонстрированным значениям степени просветления оптических аттенюаторов под действием мощного излучения. При увеличении интенсивности на большее значение нарушителю становится доступен весь выработанный ключ.
4. Применение метода «decoy state», статистического мониторинга темпов отсчетов и темпов двойных срабатываний для информационных состояний и состояний-ловушек обеспечивает защищенность системы КРК, использующей протокол BB84, от атаки с безошибочными измерениями и дополнительным измерением с псевдоразличением числа фотонов. При несанкционированном увеличении интенсивности излучения передатчика КРК в некоторое число раз защищенность системы сохраняется вплоть до достижения порогового значения, определяемого параметрами метода «decoy state», потерями в канале между легитимными пользователями, квантовой эффективностью детекторов нарушителя и вероятностью темновых отсчетов на детекторах приемника КРК. При увеличении интенсивности на большее значение нарушителю становится доступен весь выработанный ключ.

Достоверность полученных результатов обеспечивается использованием современных оптических компонентов, поверенного и корректно откалиброванного измерительного оборудования. Воспроизводимость

экспериментальных данных подтверждается многократным повторением измерений и устойчивостью наблюдаемых характеристик. Полученные зависимости согласуются с теоретически ожидаемым поведением и данными независимых исследований, опубликованных в научной литературе. Численные расчёты выполнены с применением проверенных программных средств и алгоритмов. Представленные результаты обсуждались на российских и международных конференциях и прошли рецензирование в научных журналах.

Апробация работы. Основные результаты работы докладывались на следующих конференциях:

1. РусКрипто 2021, Солнечногорск, Россия, 2021 год
2. 6th International Conference on Quantum Technologies (ICQT2021), Москва, Россия, 2021 год
3. SPIE Security + Defence 2021, Мадрид, Испания, 2021 год
4. Рускрипто 2022, Солнечногорск, Россия, 2022 год
5. SPIE Quantum Technologies 2022, Страсбург, Франция, 2022 год
6. 20th International Conference Laser Optics (ICLO 2022), Санкт-Петербург, Россия, 2022 год
7. РусКрипто 2023, Солнечногорск, Россия, 2023 год
8. Диановская конференция по волоконной оптике (ВКВО-2023), Пермь, Россия, 2023 год
9. Невская фотоника—2023, Санкт-Петербург, Россия, 2023 год
10. 21st International Conference Laser Optics (ICLO 2024), Санкт-Петербург, Россия, 2024 год
11. ХОЛОЭКСПО 2025, Уфа, Россия, 2025 год

Личный вклад. Все результаты работы получены автором лично или при непосредственном участии. Автор принимал участие в разработке, сборке, настройке и отладке экспериментальных схем, проведении экспериментов, обработке результатов измерений, выводе аналитических формул и проведении численных симуляций.

Публикации. Основные результаты по теме диссертации изложены в 4 научных статьях, опубликованных в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ по специальности и отрасли наук.

Объем и структура работы. Диссертация состоит из введения, 3 глав, заключения. Полный объем диссертации составляет 138 страниц текста с 22 рисунками и 1 таблицей. Список литературы содержит 156 наименований.

Основное содержание работы

В **первой главе** проведен обзор литературы. Сперва формулируется критерий секретности в квантовой криптографии с использованием

следового расстояния между матрицами плотности для идеальной и реальной ситуации [13]. Приводится операциональный смысл параметра ϵ, входящего в формулу критерия секретности. Далее приводится набор определений, необходимых для введения достаточного условия секретности с использованием гладкой условной min-энтропии, которая, в свою очередь, записывается через условную энтропию фон Неймана. В следующем разделе рассматривается вопрос доказательства секретности протоколов квантового распределения ключей (КРК) путем их сведения к ЭПР-версии. Приводятся энтропийные соотношения неопределенности, позволяющие оценить условную энтропию фон Неймана, входящую в достаточное условие секретности, через наблюдаемые параметры. Рассматривается случай использования самого распространенного квантово-криптографического протокола BB84 [8] с ослабленными когерентными состояниями: приводится явный вид достаточного условия секретности для данного случая. Подробно описывается способ оценки каждого параметра, входящего в формулу достаточного условия секретности, а именно, величины классической утечки, доли однофотонной компоненты и вероятности ошибки в однофотонной компоненте. Описывается широко применимый метод состояний-ловушек (метод «decoy state») для оценки параметров с использованием вспомогательных когерентных состояний с уменьшенной интенсивностью.

Также в первой главе рассматриваются атаки на системы КРК. Сперва описывается унитарная коллективная атака, являющаяся оптимальной для нарушителя, в случае использования протокола BB84. Выписан явный вид квантового состояния для системы Алиса—Боб—Ева при проведении коллективной атаки. Показано, что доля секретных бит при проведении коллективной атаки совпадает с границей, установленной достаточным условием секретности при использовании энтропийных соотношений неопределенности. Далее рассматривается класс атак, связанных с использованием ослабленных когерентных состояний вместо строго однофотонных— атак на многофотонную компоненту. Описаны атаки со светоделителем («Beam Splitting», BS), атаки с расщеплением по числу фотонов («Photon Number Splitting», PNS) и атаки с однозначным различением состояний («Unambiguous State Discrimination», USD). Делается вывод о том, что представленные в настоящий момент схемы атак на многофотонную компоненту являются чрезмерно ресурсозатратными и тяжело выполнимыми в реальных условиях. Также отмечается, что при выработке ключа на однофотонной компоненте (например, при штатном использовании метода «decoy state») протокол BB84 может считаться защищенным от атак такого рода.

Следующий раздел первой главы посвящен влиянию несовершенств технической реализации на безопасность КРК. Показано, что при наличии

неточности приготовления и измерения квантовых состояний, достаточное условие секретности необходимо модифицировать путем добавления в него параметров, отвечающих за близость реальных процедур измерения и приготовления к идеальным. Далее рассматриваются атаки на техническую реализацию систем КРК. Данные атаки связаны с несовершенствами аппаратуры, которые могут дать возможность нарушителю осуществить взаимодействие с легитимными пользователями, не воздействуя на квантовые состояния в канале (или воздействуя не только на них), в результате которого криптографическая стойкость полученных ключей будет понижена. Выделены следующие классы атак на техническую реализацию:

– атаки по побочным каналам утечки информации;
– атаки навязывания (атаки «fake-state»);
– изменение свойств системы внешним воздействием.

Далее каждый из классов рассматривается подробно. В разделе, посвященному побочным каналам утечки информации, перечисляются побочные каналы различной природы, среди которых выделяются оптические побочные каналы. К ним относятся активный оптический побочный канал (атака «Trojan Horse», THA), связанный с наличием паразитных отражений от внутренностей установки легитимного пользователя при введении зондирующего излучения нарушителем, и пассивный оптический побочный канал (атака «Backflash», BFA), связанным с паразитным эффектом переизлучения однофотонных детекторов на приемной стороне. Показано, что при использовании модельных соображений о состояниях в побочном канале (в частности, в литературе рассматривается случай когерентных состояний), можно дополнить матрицу плотности системы Алиса—Боб—Ева, ранее включавшей лишь коллективную атаку. Вычисление условной энтропии для модифицированной матрицы плотности позволяет обновить достаточное условие секретности с учетом утечки по побочным каналам. Данное вычисление проводится на примере активного оптического побочного канала.

В следующей части рассматриваются атаки навязывания, к которым относятся такие атаки, как атака с рассогласованием квантовых эффективностей детекторов во времени, атака с ослеплением детекторов («Detector Blinding Attack», DBA) атака на спаде строба («After-Gate Attack», AGA). Показано, что меры защиты от данных атак представляют собой либо модификации протоколов КРК, исключающие возможность проведения атак такого рода, либо добавление технических средств мониторинга попыток проведения атак навязывания. При надлежащей реализации мер защиты от атак навязывания модификация достаточного условия секретности не требуется.

Наконец, рассматривается изменение параметров системы КРК при внешнем воздействии со стороны нарушителя. В частности, отмечается, что нарушитель способен увеличить среднее число фотонов в легитимных

посылках, воздействуя на оптические элементы внутри схемы передатчика. Так, рассмотрена атака с лазерным повреждением («Laser Damage Attack», LDA), атака с затравочным излучением («Laser Seeding Attack», LSA) и атака с вынужденной фоторефракцией («Induced Photorefraction Attack», IPA). Успешное осуществление данных атак может позволить нарушителю выявить часть ключа при дальнейшем проведении атак на многофотонную компоненту.

В конце главы раскрывается понятие комбинированной атаки на систему КРК. Под комбинированной атакой предлагается понимать одновременное проведение двух или более атак на систему КРК в целях получения информации о секретном ключе, превышающем совокупную информацию, получаемую нарушителем при проведении данных атак по отдельности. На основе проведенного литературного обзора делается вывод о том, что для обеспечения безопасности систем КРК необходимо рассматривать комбинирование коллективных атак, атак на многофотонную компоненту, атак по побочным каналам и атак навязывания в условиях изменения свойств системы внешним воздействием нарушителя.

Вторая глава посвящена теоретическому и экспериментальному анализу побочных каналов утечки информации в системах КРК. В отличие от подходов, требующих задания конкретного вида состояний в побочном канале, в диссертации состояние побочного канала характеризуется степенью перекрытия состояний (фиделити), соответствующих различным значениям закодированного бита.

Рассмотрение проводится на примере протокола BB84 при комбинировании коллективной атаки с атакой по активному оптическому побочному каналу. Для двух значений закодированного бита состояния полной квантовой системы Евы записываются в виде

$$\rho_E^0 = \rho_Q^0 \otimes \rho_{\text{THA}}^0, \qquad \rho_E^1 = \rho_Q^1 \otimes \rho_{\text{THA}}^1, \tag{1}$$

где ρ_Q^0 и ρ_Q^1 описывают вспомогательную квантовую систему Евы, связанную с коллективной атакой, а ρ_{THA}^0 и ρ_{THA}^1 — состояния в активном побочном канале. После взятия частичного следа по подсистеме Боба матрица плотности системы Алиса—Ева имеет квантово-классический вид

$$\rho_{XE} = \frac{1}{2}|0\rangle_X\langle 0| \otimes \rho_E^0 + \frac{1}{2}|1\rangle_X\langle 1| \otimes \rho_E^1. \tag{2}$$

Для состояний такого вида условная энтропия системы Алиса—Ева выражается через величину Холево:

$$H(X|E) = 1 - \chi_E, \tag{3}$$

где

$$\chi_E = S(\rho_E) - \frac{1}{2}S(\rho_E^0) - \frac{1}{2}S(\rho_E^1), \qquad \rho_E = \frac{1}{2}\rho_E^0 + \frac{1}{2}\rho_E^1, \tag{4}$$

а S обозначает энтропию фон Неймана.

Прямое вычисление величины Холево для произвольных смешанных состояний может быть затруднено, поэтому используется верхняя граница через фиделити Ульмана:

$$\chi_E \leq \overline{\chi}_E \equiv h\left(\frac{1-\sqrt{\mathcal{F}}}{2}\right) \equiv -\frac{1+\sqrt{\mathcal{F}}}{2}\log\frac{1+\sqrt{\mathcal{F}}}{2} - \frac{1-\sqrt{\mathcal{F}}}{2}\log\frac{1-\sqrt{\mathcal{F}}}{2}, \tag{5}$$

где фиделити Ульмана $\mathcal{F}$ определяется как

$$\mathcal{F}(\rho_E^0, \rho_E^1) = \left(\mathrm{tr}\sqrt{\sqrt{\rho_E^0}\rho_E^1\sqrt{\rho_E^0}}\right)^2. \tag{6}$$

Благодаря мультипликативности фиделити вклад коллективной атаки и побочного канала учитывается совместно:

$$H(X|E) \geq 1 - h\left(\frac{1-\eta(1-2E_1)}{2}\right), \tag{7}$$

где E_1 — вероятность ошибки для однофотонной компоненты, а

$$\eta = \sqrt{\mathcal{F}(\rho_{\mathrm{THA}}^0, \rho_{\mathrm{THA}}^1)} \tag{8}$$

— степень перекрытия состояний в побочном канале. Формула (7) показывает, что вклад коллективной атаки и побочного канала не является аддитивным.

Для применения формулы (7) параметр η необходимо связать со средним числом фотонов μ_{THA} в состоянии, возвращающемся к нарушителю. Показано, что вероятность вакуумной компоненты p_0 удовлетворяет неравенству

$$p_0 \geq 1 - \mu. \tag{9}$$

С использованием данного соотношения получены оценки для поляризационного кодирования

$$\eta \geq 1 - \mu_{\mathrm{THA}}, \tag{10}$$

и для фазового кодирования:

$$\eta \geq 1 - 2\mu_{\mathrm{THA}}. \tag{11}$$

Таким образом, достаточное условие секретности выражается через экспериментально измеряемую величину.

Далее описывается экспериментальный способ определения μ_{THA}. При проведении THA Ева вводит в передатчик Алисы интенсивный оптический импульс, который проходит через пассивные волоконные элементы защиты, отражается от внутренних элементов схемы и возвращается к нарушителю. Среднее число фотонов в возвращающемся импульсе выражается как

$$\mu_{\text{THA}}(\lambda) = \frac{P_{\text{THA}}(\lambda)\lambda}{f_{\text{THA}}hc}, \tag{12}$$

где $P_{\text{THA}}(\lambda)$ — мощность возвращающегося излучения на длине волны атаки λ, f_{THA} — частота повторения атакующих импульсов, h — постоянная Планка, c — скорость света в вакууме. Мощность P_{THA} определяется выражением

$$P_{\text{THA}} = P_{\max}[\text{дБм}] + T[\text{дБ}] + R[\text{дБ}]. \tag{13}$$

Экспериментальные исследования проводились на коммерческой системе КРК и включали измерение спектров пропускания защитных элементов и широкополосную рефлектометрию передатчика.

Для измерения спектров пропускания была разработана установка, схема которой приведена на рисунке 1. В качестве источника использовался суперконтинуумный лазер, перестраиваемый фильтр выделял узкую спектральную полосу, а регистрация осуществлялась однофотонным лавинным фотодиодом на базе InGaAs. Установка позволила проводить измерения в диапазоне 1100—1800 нм с динамическим диапазоном до 120 дБ.

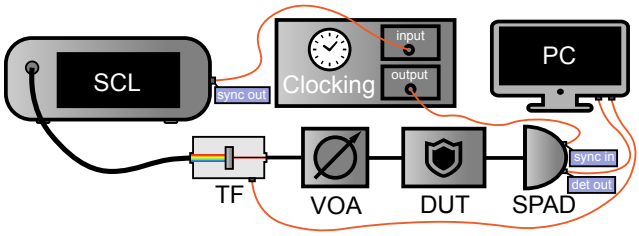

Рисунок 1 — Схема экспериментальной установки для измерения спектра пропускания: SCL — суперконтинуумный лазер, TF — перестраиваемый фильтр, VOA — переменный оптический аттенюатор, DUT — тестируемое устройство, SPAD — однофотонный ЛФД, Clocking — временной коррелятор электрических сигналов, PC — персональный компьютер

Были измерены спектры пропускания основных элементов защиты исследуемой системы КРК: оптического изолятора, оптического циркулятора с зеркалом, WDM-фильтра с постоянным аттенюатором и

переменного оптического аттенюатора. Результаты приведены на рисунке 2.

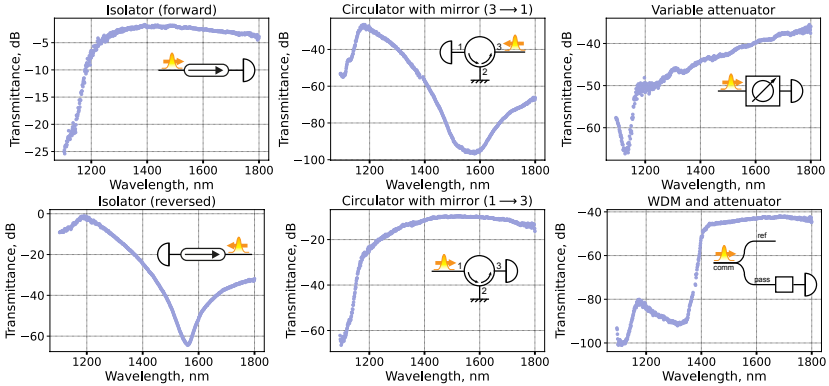

Рисунок 2 — Измеренные спектры пропускания элементов защиты из состава исследуемой системы КРК: оптический изолятор в прямом и обратном подключении, оптический циркулятор с зеркалом в направлениях $1 \to 3$ и $3 \to 1$, переменный аттенюатор, а также WDM-фильтр с постоянным аттенюатором

Измерения показали, что спектральные характеристики элементов существенно изменяются вне рабочей длины волны протокола. Высокий динамический диапазон установки позволил измерить области, где потери превышают 80—100 дБ.

Для определения отражений внутри передатчика был впервые разработан широкополосный однофотонный рефлектометр с разрешением по времени (ν—OTDR), схема которого приведена на рисунке 3. Отраженное излучение через циркулятор направляется на однофотонный детектор, а временной коррелятор регистрирует задержку прихода импульсов и позволяет восстановить распределение отражений по длине схемы.

Рефлектограмма передатчика на длине волны 1325 нм приведена на рисунке 4. На ней видны пики, соответствующие фазовому модулятору, поляризатору и интерферометру Маха—Цандера.

Рефлектометрия системы КРК впервые была выполнена во всем диапазоне 1100—1800 нм. Шаг перестроцки составил 25 нм. Тепловая карта отражений изображена на рисунке 5. Максимальный пик наблюдался в области торцов интерферометра Маха—Цандера.

На основе измерений была вычислена зависимость среднего числа фотонов μ_{THA} от длины волны атаки. При расчете использовались максимальная мощность зондирования, ограниченная порогом лазерного

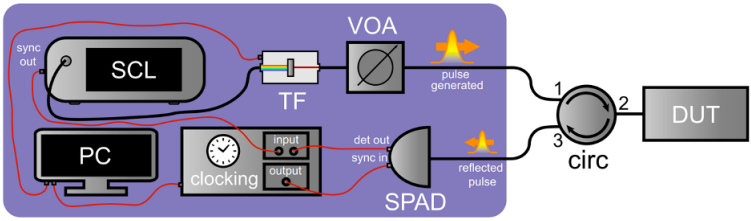

Рисунок 3 — Широкополосный ν-OTDR рефлектометр: SCL — суперконтинуумный лазер, TF — перестраиваемый фильтр, VOA — переменный оптический аттенюатор, circ — оптический циркулятор, DUT — исследуемое устройство, SPAD — однофотонный ЛФД, Clocking — временной коррелятор электрических сигналов, PC — персональный компьютер

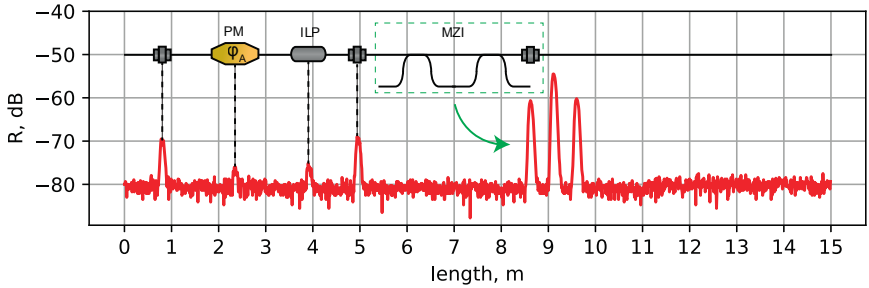

Рисунок 4 — Рефлектограмма передатчика исследуемой системы КРК на длине волны 1325 нм с расшифровкой пиков: PM — фазовый модулятор, ILP — поляризатор, MZI — интерферометр Маха—Цандера

повреждения волоконных компонентов (около 10 Вт), и частота повторения атакующих импульсов $f_{\text{THA}} = 1$ кГц. Результат приведен на рисунке 6.

Максимальное значение интенсивности оказалось порядка $\mu_{\text{THA}} \approx 10^{-8}$ и достигается в области длины волны 1410 нм. На легитимной длине волны 1550 нм величина μ_{THA} оказывается более чем на пять порядков меньше. Это показывает, что анализ только на рабочей длине волны протокола может существенно занизить оценку утечки информации.

Для фазового кодирования минимальная степень перекрытия состояний Евы при максимальном значении μ_{THA} равна

$$\eta_{\text{THA}} = 1 - 2\mu_{\text{THA}} = 0{,}99999998. \tag{14}$$

Если положить $E_1 = 0$, то верхняя граница величины Холево, отвечающая только утечке по THA-каналу, составляет

$$\overline{\chi}_E = h\left(\frac{1-\eta_{\text{THA}}}{2}\right) = h(\mu_{\text{THA}}) \approx 2{,}8 \cdot 10^{-7}. \tag{15}$$

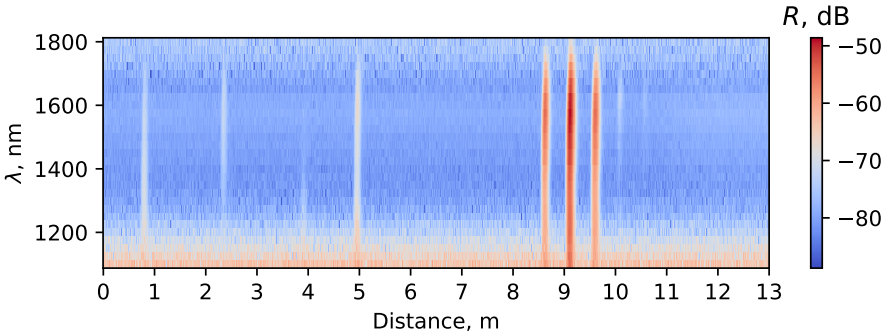

Рисунок 5 — Тепловая карта отражений, полученная при широкополосной рефлектометрии передатчика исследуемой системы КРК в диапазоне 1100—1800 нм

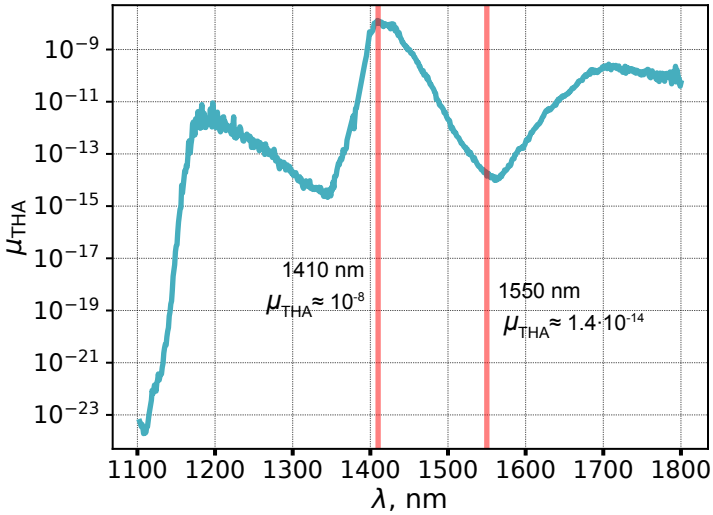

Рисунок 6 — Зависимость среднего числа фотонов μ_{THA} в возвращающемся к нарушителю импульсе от длины волны атакующего излучения.

Полученные результаты показывают, что в исследованной системе активный оптический побочный канал эффективно подавляется, а предложенная методика позволяет учитывать остаточную утечку при расчете длины секретного ключа.

В заключительной части главы рассмотрено обобщение на несколько побочных каналов. Если нарушителю доступны состояния в N независимых побочных каналах, то итоговая степень перекрытия состояний Евы

равна произведению вкладов отдельных каналов:

$$\eta = \eta_{\mathrm{SC}_1} \cdot \eta_{\mathrm{SC}_2} \cdot \ldots \cdot \eta_{\mathrm{SC}_N}. \tag{16}$$

Это позволяет использовать единую схему оценки для THA, BFA и других побочных каналов. Каждый канал характеризуется своим параметром перекрытия, после чего все вклады подставляются в формулу (7). Таким образом, во второй главе предложен способ анализа комбинированных атак по побочным каналам, связывающий измеряемые параметры с информацией нарушителя и длиной секретного ключа.

В **третьей главе** проведен анализ рисков, возникающих при изменении параметров системы КРК внешним воздействием. В отличие от побочных каналов, влияние которых может быть учтено через параметры различимости состояний, изменение параметров системы требует отдельного анализа.

Основное внимание уделено увеличению интенсивности легитимного излучения в системе КРК, использующей протокол BB84 и метод «decoy state» (метод состояний-ловушек). Такое увеличение может возникнуть в результате атаки с лазерным повреждением или атаки с затравочным излучением. Пусть в штатном режиме средние числа фотонов информационного и слабого состояния-ловушки равны μ и ν, где $\nu < \mu$, а вакуумное состояние-ловушка имеет интенсивность 0. При внешнем воздействии реальные интенсивности изменяются как

$$\mu \longrightarrow \tilde{\mu} = \kappa\mu, \tag{17}$$

$$\nu \longrightarrow \tilde{\nu} = \kappa\nu, \tag{18}$$

где κ — степень увеличения интенсивности излучения. При этом Алиса и Боб продолжают использовать в формулах метода «decoy state» исходные значения μ и ν. Это несоответствие может привести к завышенной оценке доли однофотонной компоненты и компрометации секретного ключа.

Сначала рассмотрена атака с расщеплением по числу фотонов (PNS-атака). В идеализированном случае Ева выполняет неразрушающее измерение числа фотонов, блокирует все посылки, кроме двухфотонных, сохраняет один фотон, а второй отправляет Бобу. После раскрытия базисов она измеряет сохраненный фотон в правильном базисе и получает бит ключа без внесения ошибки. Показано, что метод «decoy state» в этом случае ошибочно оценивает долю однофотонной компоненты как ненулевую при любом $\kappa > 1$. Следовательно, в идеализированной модели двухфотонная PNS-атака приводит к полной компрометации ключа уже при сколь угодно малом увеличении интенсивности, однако требует нереалистичных на сегодняшний день технологий.

Далее рассмотрена PNS-атака без долгосрочной квантовой памяти. В этом случае Ева должна измерять отщепленные фотоны до раскрытия базисов. Чтобы получить весь ключ, она может использовать трехфотонную

компоненту: два фотона измеряются в двух сопряженных базисах, а третий отправляется Бобу. Показано, что метод «decoy state» начинает давать положительную оценку доли однофотонной компоненты при

$$\kappa > \kappa_{3\text{ph}} = 1 + \frac{1}{\mu - \nu} \ln \frac{\mu}{\nu}. \tag{19}$$

Затем рассмотрены USD-атаки, то есть атаки с однозначным различением состояний. В отличие от PNS-атак, они не требуют ни долгосрочной квантовой памяти, ни неразрушающего измерения числа фотонов. Для BB84 с поляризационным кодированием такая атака реализуется установкой, эквивалентной приемнику КРК с пассивным выбором базиса (рисунок 7). При одновременном срабатывании трех детекторов нарушитель может однозначно определить верный базис и закодированное состояние, после чего отправить Бобу состояние с той же поляризацией.

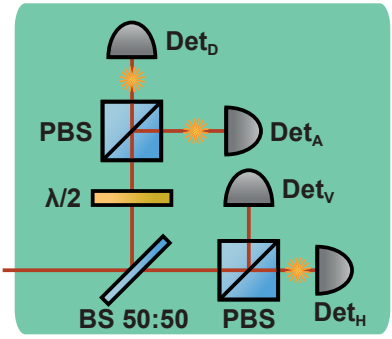

Рисунок 7 — Установка для проведения USD-измерений для протокола BB84 с поляризационным кодированием: BS 50:50 — полупрозрачное зеркало, $\lambda/2$ — полуволновая пластинка для поворота поляризации на 45°, PBS — поляризационный светоделитель, $\text{Det}_{\text{H,V,D,A}}$ — однофотонные детекторы для горизонтально, вертикально, диагонально и антидиагонально поляризованных состояний

Порог степени увеличения интенсивности для такой атаки приближенно равен

$$\kappa_{\text{USD}} \approx 2 + \frac{2}{\mu - \nu} \ln \frac{\mu}{\nu} = 2\kappa_{3\text{ph}}. \tag{20}$$

Таким образом, порог USD-атаки примерно вдвое выше порога трехфотонной PNS-атаки.

Численно была найдена доля однофотонной компоненты, оцениваемая методом «decoy state», для различных параметров легитимных

сигналов в зависимости от κ (рисунок 8). Для типичных параметров пороги лежат в диапазоне от 10 до 20 дБ. После превышения порога оценка однофотонного вклада быстро возрастает, и Ева может подобрать значение κ, соответствующее нормальной работе системы.

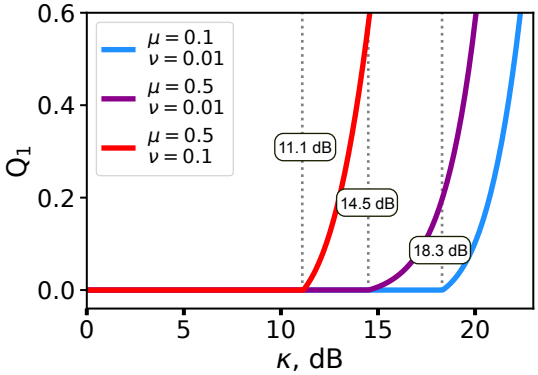

Рисунок 8 — Результат моделирования зависимости оценки доли однофотонной компоненты Q_1 от степени увеличения интенсивности излучения κ при проведении USD-атаки для различных параметров «decoy state»

Далее строится модифицированная USD-атака, схема которой показана на рисунке 9. Перед установкой однозначного различения состояний добавляется асимметричный светоделитель с коэффициентом пропускания T. Отраженная часть направляется на детектор «лишних» фотонов: при его срабатывании Ева блокирует посылку, а в противном случае выполняет стандартное USD-измерение. Это позволяет исключать события, происходящие из более чем трехфотонной компоненты.

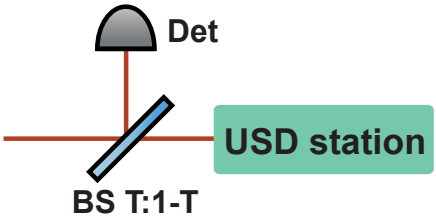

Рисунок 9 — Установка для модифицированной USD-атаки: Det — однофотонный детектор для обнаружения «лишних» фотонов, BS T:1-T — асимметричный светоделитель с коэффициентом пропускания T, USD station — установка для USD-измерений из рисунка 7

Для порога такой атаки получено приближенное выражение

$$\kappa_T = \frac{2}{2-T}\left(1 + \frac{1}{\mu-\nu}\ln\frac{\mu}{\nu}\right) = \frac{2\kappa_{3\text{ph}}}{2-T}. \tag{21}$$

При $T \to 0$ этот порог стремится к пределу трехфотонной PNS-атаки. Однако уменьшение T снижает темпы отсчетов у Боба, поэтому для сохранения скрытности Еве требуется компромиссный выбор коэффициента пропускания.

В следующем разделе рассмотрена USD-атака с псевдоразличением числа фотонов (PPNR USD-атака), предназначенная для имитации темпов отсчетов и темпов двойных срабатываний для информационных состояний и состояний-ловушек. Схема установки Евы приведена на рисунке 10. Перед USD-установкой размещен блок псевдоразличения числа фотонов на светоделителях и однофотонных детекторах. По числу сработавших детекторов Ева делает предположение о типе состояния и выбирает дальнейшее действие. Ее передающая станция может отправлять Бобу одиночный фотон или лазерный импульс заданной интенсивности.

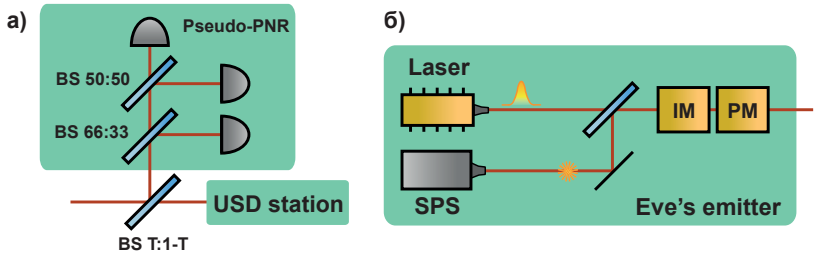

Рисунок 10 — а) Установка Евы для PPNR USD-измерений: BS — светоделитель, USD station — установка для USD-измерений из рисунка 7; б) передатчик Евы: Laser — источник лазерных импульсов, SPS — источник одиночных фотонов, IM/PM — модулятор интенсивности/поляризации

Для каждого значения потерь в канале между Алисой и Бобом выполнялся поиск оптимального T, минимизирующего пороговое значение κ. Атака считалась реализуемой, если найденные вероятности и интенсивности оставались физически допустимыми, а относительная невязка для имитируемых темпов отсчета не превышала $\varepsilon = 10\%$.

Результат моделирования приведен на рисунке 11: показаны оптимальное значение коэффициента пропускания T_o и порог κ_{PPNR} в зависимости от пропускания канала η. В идеальном случае $\eta_E = 1$, $p_{\text{dcr}} = 0$ порог уменьшается при росте потерь в канале и приближается к порогу стандартной USD-атаки.

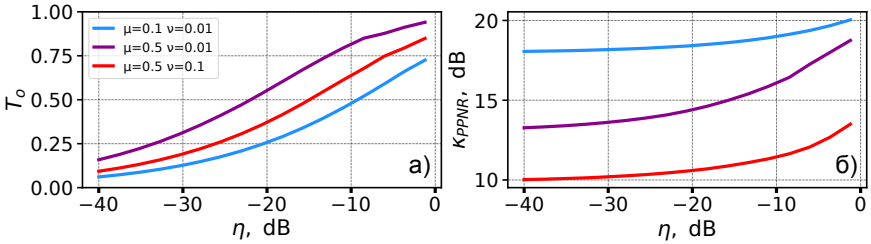

Рисунок 11 — а) Зависимость оптимального значения коэффициента пропускания светоделителя T_o от пропускания канала η; б) зависимость κ_{PPNR} от пропускания канала η для различных параметров «decoy state»

Далее исследовано влияние темновых отсчетов Боба и квантовой эффективности детекторов Евы (рисунок 12). При увеличении вероятности темновых отсчетов p_{dcr} зависимость κ_{PPNR} совпадает с идеальным случаем до некоторого критического уровня потерь, после чего порог резко возрастает, поскольку темновые отсчеты существенно влияют на статистику. Уменьшение квантовой эффективности детекторов Евы η_E приводит к пропорциональному росту порога.

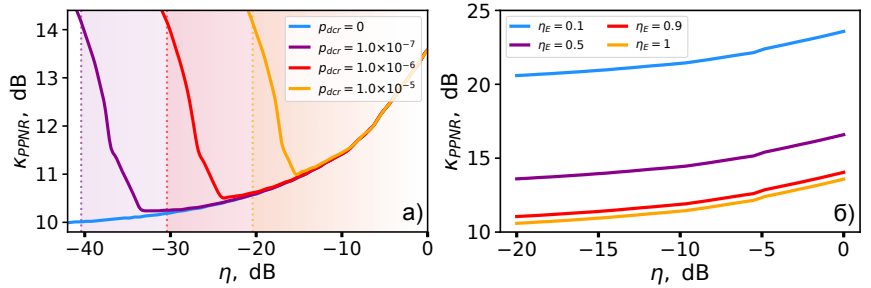

Рисунок 12 — а) Зависимость κ_{PPNR} от пропускания канала η для различных значений p_{dcr}; б) зависимость κ_{PPNR} от пропускания канала η для различных квантовых эффективностей детекторов Евы η_E

Полученные результаты показывают, что PPNR USD-атака может позволить нарушителю получить весь секретный ключ и одновременно имитировать основные наблюдаемые параметры у Боба. Несовершенства оборудования увеличивают требуемый порог κ_{PPNR}, но не делают атаку принципиально невозможной. В ряде случаев требуемые значения сопоставимы с величинами просветления оптических аттенюаторов, наблюдавшимися в экспериментах по лазерному повреждению.

Таким образом, показано, что анализ безопасности систем КРК, использующих метод «decoy state» не может быть ограничен рассмотрением

нереализуемых на сегодняшних день PNS-атак, а также требует учета USD-атак. Было показано, что при учете различных USD-атак метод «decoy state» обеспечивает защищенность КРК лишь до превышения порога степени увеличения интенсивности.

В **заключении** приведены основные результаты работы, которые заключаются в следующем:

1. Был разработан способ вычисления верхней границы информации доступной нарушителю при комбинировании коллективной атаки с атаками по побочным каналам. Было показано, что данная величина может быть вычислена с использованием верхней границы для величины Холево, при этом допущения о конкретном виде квантовых состояний в побочных каналах не требуются. Каждый побочный канал может быть параметризован величиной фиделити между состояниями, отвечающими разным битам. Фиделити может быть выражено через единственный параметр — интенсивность излучения в побочном канале.
2. Был разработан способ экспериментального определения интенсивности в активном оптическом побочном канале, связанным с атакой «Trojan Horse», включающий в себя измерение спектров пропускания пассивных волоконно-оптических элементов системы КРК, а также измерение спектра отражения внутри системы КРК. Был разработан и собран экспериментальный стенд для измерения спектров пропускания в спектральном диапазоне 1100—1800 нм с рекордным динамическим диапазоном, достигавшим 120 дБ, а также широкополосный оптический рефлектометром со спектром перестройки 1100—1800 нм и сантиметровым разрешением.
3. Были проведены исследования передатчика реальной системы КРК на предмет защищенности от атаки активного оптического зондирования с использованием разработанных методов. Было показано, что данная атака в спектральном диапазоне 1100—1800 нм является неэффективной.
4. Был проведен анализ атак на многофотонную компоненту систем КРК, использующих протокол BB84 и метод «decoy state», при увеличении интенсивности легитимного излучения. Было показано, что нарушитель способен получить весь секретный ключ при преодолении некоторого порогового значения степени увеличения интенсивности излучения, лежащего в области 10— 20 дБ, путем проведения безошибочных измерений (USD-атаки). Было показано, что для таких измерений достаточно лишь копии приемника КРК. Также была построена модифицированная версия USD-атаки, позволившая уменьшить требуемый порог увеличения интенсивности.

5. Была рассмотрена стратегия USD-атаки, позволяющая нарушителю провести имитирование всех наблюдаемых темпов отсчетов на приемной стороне, таким образом лишив легитимных пользователей возможности детектирования атаки. Было рассмотрено влияние реальных параметров на проведение данной атаки, таких как квантовая эффективность детекторов нарушителя, потери в канале, а также вероятность темновых отсчетов на приемной стороне.

Список публикаций по теме диссертации

1. Sushchev I. S., Bulavkin D. S., Bugai K. E., Sidelnikova A. S., Dvoretskiy D. A. Trojan-horse attack on a real-world quantum key distribution system: Theoretical and experimental security analysis // Physical Review Applied. — 2024. — Vol. 22, No. 3. — P. 034032. — Импакт-фактор 4,4 (JIF) / 0,81 п.л. / вклад соискателя: сборка экспериментальной установки, участие в реализации программного обеспечения для работы установки, проведение измерений, обработка результатов измерений, вывод аналитических формул, EDN: HBUUFK.
2. Молотков С. Н., Сущев И. С. О эквивалентности фазовых и поляризационных преобразований в квантовой оптике // Письма в Журнал экспериментальной и теоретической физики. — 2024. — Т. 120, № 7. — С. 505–510. — Импакт-фактор 0,353 (РИНЦ) / 0,38 п.л. / вклад соискателя: помощь в интерпретации теоретических результатов и проверка вывода формул, EDN: ELAYLF.
3. Bondar K. D., Sushchev I. S., Bulavkin D. S., Bugai K. E., Sidelnikova A. S., Melkonian D. M., Vakhrusheva V. M., Dvoretskiy D. A. Broadband optical time-domain reflectometry for security analysis of quantum key distribution // Physical Review Applied. — 2025. — Vol. 24, No. 1. — P. 014010. — Импакт-фактор 4,4 (JIF) / 0,56 п.л. / вклад соискателя: сборка экспериментальной установки, участие в реализации программного обеспечения для работы установки, помощь в проведении измерений, помощь в обработке результатов измерений, помощь в выводе аналитических формул, EDN: TCNMLQ.
4. Sushchev I. S., Bugai K. E., Molotkov S. N., Bulavkin D. S., Sidelnikova A. S., Melkonian D. M., Vakhrusheva V. M., Lokhmatov R. Yu., Dvoretskiy D. A. Realistic vulnerabilities of decoy-state quantum key distribution // Scientific Reports. — 2025. — Vol. 15, No. 1. — P. 44820. — Импакт-фактор 3,9 (JIF) / 0,81 п.л. / вклад соискателя: вывод аналитических формул и проведение численных симуляций, EDN: TQCBLN.

Список литературы

1. *Арбеков, И. М.* Одноразовый блокнот Вернама, Котельникова, Шеннона и квантовая криптография / И. М. Арбеков, С. Н. Молотков // Успехи Физических Наук. — 2025. — Т. 195, № 10. — С. 1021—1046.
2. *Renner, R.* Quantum advantage in cryptography / R. Renner, R. Wolf // AIAA Journal. — 2023. — Т. 61, № 5. — С. 1895—1910.
3. *Shannon, C. E.* Communication theory of secrecy systems / C. E. Shannon // The Bell System Technical Journal. — 1949. — Т. 28, № 4. — С. 656—715.
4. *Bell, J. S.* On the Einstein Podolsky Rosen paradox / J. S. Bell // Physics Physique Fizika. — 1964. — Т. 1, № 3. — С. 195.
5. *Aspect, A.* Experimental test of Bell's inequalities using time-varying analyzers / A. Aspect, J. Dalibard, G. Roger // Physical review letters. — 1982. — Т. 49, № 25. — С. 1804.
6. *Aspect, A.* Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: a new violation of Bell's inequalities / A. Aspect, P. Grangier, G. Roger // Physical review letters. — 1982. — Т. 49, № 2. — С. 91.
7. *Wootters, W. K.* A single quantum cannot be cloned / W. K. Wootters, W. H. Zurek // Nature. — 1982. — Т. 299, № 5886. — С. 802—803.
8. *Bennett, C. H.* Quantum cryptography: Public key distribution and coin tossing / C. H. Bennett, G. Brassard // Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing. — Bangalore, 1984. — С. 175.
9. Quantum cryptography / N. Gisin [и др.] // Reviews of Modern Physics. — 2002. — Т. 74, № 1. — С. 145.
10. The security of practical quantum key distribution / V. Scarani [и др.] // Reviews of Modern Physics. — 2009. — Т. 81, № 3. — С. 1301—1350.
11. Secure quantum key distribution with realistic devices / F. Xu [и др.] // Reviews of Modern Physics. — 2020. — Т. 92, № 2. — С. 025002.
12. Experimental quantum cryptography / C. H. Bennett [и др.] // Journal of Cryptology. — 1992. — Т. 5. — С. 3—28.
13. *Renner, R.* Security of quantum key distribution / R. Renner // International Journal of Quantum Information. — 2008. — Т. 6, № 01. — С. 1—127.