МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ

На правах рукописи

Сущев Иван Сергеевич

Исследование комбинированных атак на волоконные системы квантового распределения ключей

Специальность 1.3.19. Лазерная физика

Диссертация на соискание учёной степени
кандидата физико-математических наук

Научный руководитель:
доктор физико-математических наук
Молотков Сергей Николаевич

Москва — 2026

Оглавление

Стр.

Введение

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 ана-

лиза 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 состоя-

ний 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 журналах Scopus, WoS, RSCI, а также в Перечне изданий МГУ.

1. Trojan-horse attack on a real-world quantum key distribution system: Theoretical and experimental security analysis / I. S. Sushchev, D. S. Bulavkin, K. E. Bugai, A. S. Sidelnikova, D. A. Dvoretskiy//Physical Review Applied. — 2024. — Т. 22, № 3. — С. 034032. EDN: HBUUFK. WoS JIF 4,4; 0,81 п.л. Авторский вклад: сборка экспериментальной установки, участие в реализации программного обеспечения для работы установки, проведение измерений, обработка результатов измерений, вывод аналитических формул.
2. О эквивалентности фазовых и поляризационных преобразований в квантовой оптике / С. Н. Молотков, И. С. Сущев// Письма в Журнал

экспериментальной и теоретической физики. — 2024. — Т. 120, № 7. — С. 505—510. EDN: ELAYLF. WoS JIF 1,3; 0,38 п.л. Авторский вклад: помощь в интерпретации теоретических результатов и проверка вывода формул.

3. Broadband optical time-domain reflectometry for security analysis of quantum key distribution / K. D. Bondar, I. S. Sushchev, D. S. Bulavkin, K. E. Bugai, A. S. Sidelnikova, D. M. Melkonian, V. M. Vakhrusheva, D. A. Dvoretskiy//Physical Review Applied. — 2025. — Т. 24, № 1. — С. 014010. EDN: TCNMLQ. WoS JIF 4,4; 0,56 п.л. Авторский вклад: 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.
4. Realistic vulnerabilities of decoy-state quantum key distribution / I. S. Sushchev, K. E. Bugai, S. N. Molotkov, D. S. Bulavkin, A. S. Sidelnikova, D. M. Melkonian, V. M. Vakhrusheva, R. Yu. Lokhmatov, D. A. Dvoretskiy// Scientific Reports. — 2025.— Т. 15, № 1. — С. 44820. EDN: TQCBLN. WoS JIF 3,9; 0,81 п.л. Авторский вклад: вывод аналитических формул и проведение численных симуляций.

Объем и структура работы. Диссертация состоит из введения, 3 глав, заключения. Полный объём диссертации составляет 138 страниц, включая 22 рисунка и 1 таблицу. Список литературы содержит 156 наименований.

Глава 1. Литературный обзор

1.1 Критерий секретности в квантовой криптографии

Квантовая криптография, или квантовое распределение ключей (КРК), позволяет обеспечить двух легитимных пользователей, Алису и Боба, общей случайной битовой последовательностью, недоступной третьей стороне — Еве. Данная битовая последовательность называется секретным ключом. Выработанный секретный ключ может использоваться для шифрования при использовании симметричных криптографических алгоритмов.

Совокупность действий, выполняемых в заданной последовательности легитимными субъектами с целью осуществления КРК, называется протоколом КРК. Протокол КРК, а также действия нарушителя формализуются в виде преобразований квантовой системы Алиса—Боб—Ева. В основе оценки безопасности, или криптографической стойкости, протоколов КРК лежит сравнение реального квантового состояния системы с идеальным случаем, в котором полностью отсутствуют корреляции между подсистемой Евы и выработанным ключом [13].

На сегодняшний день известно множество протоколов КРК. Большинство из них содержит следующие этапы [11]:

- генерация случайной последовательности бит на стороне Алисы и Боба;
- приготовление, отправка по квантовому каналу и измерение квантовых состояний;
- обмен информацией по классическому аутентифицированному каналу между Алисой и Бобом;
- постобработка выработанной последовательности, выработка секретного ключа (просеивание ключа, оценка параметров, исправление ошибок, усиление секретности).

Рассмотрим данные этапы подробнее на примере протоколов типа точка–точка, в которых Алиса отвечает за приготовление и отправку квантовых состояний, а Боб за их измерение[1]. Сначала Алиса генерирует случайный

[1]Также существуют протоколы КРК других топологий, где оба пользователя отвечают за приготовление и отправку или измерение квантовых состояний.

бит x с использованием физического генератора случайных чисел (ГСЧ). Далее, используя ГСЧ, Алиса выбирает базис из множества, предусмотренного протоколом. В зависимости от сгенерированного бита Алиса приготавливает квантовую систему в одном из двух базисных состояний. В качестве квантовой системы, как правило, используется свет, а кодирование осуществляется с использованием таких степеней свободы как поляризация, фаза, временной промежуток, частота, пространственное распределение поля и др. Закодированное квантовое состояние отправляется Бобу, где он проводит над ним проекционные измерения в случайно выбранном базисе из заданного множества. В зависимости от результата измерений Боб сохраняет себе бит y. Полученные на данном этапе битовые последовательности называются сырым ключом.

На этом завершается «квантовая часть» протокола. Далее, между Алисой и Бобом осуществляется сеанс связи по каналу, обладающим свойством аутентичности — невозможностью подмены информации, передаваемой по нему. В рамках данного сеанса Боб оглашает номера успешно задетектированных посылок, а также разглашается информация о выбранных базисах. После этого начинается процедура постобработки. Сначала проводится просеивание сырого ключа, или согласование базисов. В результате данной процедуры из сырого ключа исключаются биты, отвечающие неинформативным исходам измерений (например, при несовпадающих базисах в протоколе BB84 [8]). Полученная последовательность называется просеянным ключом. Далее проводится оценка наблюдаемых параметров для количественного учета влияния Евы путем разглашения части просеянного ключа (например, оценка средней вероятности квантовой битовой ошибки QBER — quantum bit error rate, в протоколе BB84 [8]). Следующий шаг — исправление ошибок с использованием кодов коррекции ошибок. В рамках данной процедуры Алиса и Боб общаются по открытому каналу для согласования своих просеянных ключей, при этом часть информации о ключе разглашается. После проведения данной процедуры образуется исправленный ключ, одинаковый у Алисы и Боба. Наконец, для избавления от информации, попавшей к нарушителю, проводится процедура усиления секретности с использованием универсальных хэш-функций второго порядка [14], сокращая ключ до длины, обеспечивающей секретность. Полученную последовательность называют секретным ключом.

Сформулируем критерий секретности ключей в квантовой криптографии, предложенный Р. Реннером в 2005 году [13; 15]. Пусть после выполнения про-

токола Алиса и Боб имеют ключ $x = (x_1, x_2, ..., x_l)$, $x \in X = \{0,1\}^l$, где l — размер ключа. Пусть Ева имеет квантовую систему, заданную матрицей плотности ρ_E^x, скоррелированную с секретным ключом x. Пусть для каждого ключа x задана вероятность $P(x)$. Поставим в соответствие каждому биту x_k квантовое состояние некоторой двухуровневой системы (квантовый бит — кубит), заданное вектором $|x_k\rangle$ в гильбертовом пространстве $\mathcal{H}^{x_k}$ размерности 2. Далее, поставим в соответствие ключу x квантовое состояние, заданное вектором $|x\rangle \equiv |x_1\rangle \otimes |x_2\rangle \otimes ... \otimes |x_l\rangle$ в гильбертовом пространстве $\mathcal{H}^X \equiv \mathcal{H}^{x_1} \otimes \mathcal{H}^{x_2} \otimes ... \otimes \mathcal{H}^{x_l}$ размерности $N \equiv 2^l$. Будем называть соответствующую квантовую систему квантовой системой Алисы. Квантовое состояние составной системы Алиса—Ева описывается следующей матрицей плотности:

$$\rho_{XE}^{(l)} = \sum_{x \in X} P(x) |x\rangle\langle x| \otimes \rho_E^x. \tag{1.1}$$

Матрица плотности для квантовой подсистемы Евы может быть найдена путем вычисления частичного следа по подсистеме Алисы:

$$\rho_E^{(l)} = \mathrm{tr}_X (\rho_{XE}) = \sum_{x \in X} P(x) \rho_E^x. \tag{1.2}$$

Идеальному случаю отвечает ситуация, в которой отсутствуют корреляции между ключом и квантовой системой Евы, а сами ключи имеют равномерное распределение. В таком случае, квантовая система Алисы будет описываться матрицей плотности ρ_U, отвечающей полностью смешанному состоянию:

$$\rho_U^{(l)} = \frac{1}{N} \sum_{x \in X} |x\rangle\langle x|. \tag{1.3}$$

Тогда, ключ, полученный в результате сеанса КРК, называется ε-секретным, если для любой квантовой системы Евы, заданной матрицей плотности ρ_E, справедливо неравенство:

$$D\left(\rho_{XE}^{(l)}, \rho_U^{(l)} \otimes \rho_E^{(l)}\right) = \frac{1}{2} \left\| \rho_{XE}^{(l)} - \rho_U^{(l)} \otimes \rho_E \right\|_1 \leqslant \varepsilon, \tag{1.4}$$

где $D(\rho, \sigma)$ — следовое расстояние между матрицами плотности ρ и σ

$$D(\rho, \sigma) = \frac{1}{2} \|\rho - \sigma\|_1, \tag{1.5}$$

а $\|\rho\|_1$ — следовая норма оператора

$$\|\rho\|_1 = \mathrm{tr}\sqrt{\rho^\dagger \rho}. \tag{1.6}$$

Как показано в работах [15; 16], величина ε определяет превышение средней вероятности успешного определения ключа нарушителем $P_{key\ guess}$ над вероятностью простого угадывания $1/N$:

$$P_{key\ guess} < \frac{1}{N} + \varepsilon. \tag{1.7}$$

Величина ε также связана с трудоемкостью перебора $G(X)$ — средним числом шагов перебора до успешного определения ключа нарушителем [15]:

$$G(X) > \frac{N\,(1-2\varepsilon)+1}{2}. \tag{1.8}$$

В работе [15] показано, что при значении $\varepsilon \approx 10^{-10}$ и шифровании 256-битовых сообщений в режиме одноразового блокнота [17] в среднем может быть дешифровано одно из 10^{10} сообщений. При средней скорости отправки сообщений 1 раз в секунду нарушитель в среднем сможет дешифровать 1 сообщение примерно за 100 лет.

1.2 Энтропийный подход

Прямая проверка выполнения критерия ε-секретности представляет собой сложную задачу, поскольку явный вид матрицы плотности ρ_{XE} в общем случае неизвестен, а матрица ρ_E — произвольна. В связи с этим при доказательстве секретности протоколов КРК следовое расстояние мажорируется с использованием ε-гладкой min-энтропии.

Введем несколько определений (здесь и далее знаком log обозначается логарифм по основанию 2).

Пусть X — множество событий x, $p(x)$ — вероятность каждого события x. Тогда энтропией Шеннона называется величина

$$H(X) \equiv -\sum_{x\in X} p(x)\log p(x). \tag{1.9}$$

Пусть также определено множество Y событий y и задано совместное распределение вероятностей $p(x, y)$. Для множества $X \cup Y$ можно выразить энтропию Шеннона

$$H(X, Y) \equiv -\sum_{x \in X, y \in Y} p(x, y) \log p(x, y). \tag{1.10}$$

Условной энтропией Шеннона называется величина

$$H(X|Y) \equiv -\sum_{x \in X, y \in Y} p(x, y) \log p(x|y), \tag{1.11}$$

где $p(x|y)$ — условная вероятность события x при условии, что произошло событие y.

Известно соотношение:

$$H(X|Y) = H(X, Y) - H(Y). \tag{1.12}$$

Для описания квантовых систем вводится обобщение энтропии Шеннона — энтропия фон Неймана. Пусть ρ_X — матрица плотности квантовой системы X. Тогда энтропией фон Неймана называется величина

$$S(\rho_X) \equiv -\mathrm{tr}\left(\rho_X \log \rho_X\right). \tag{1.13}$$

Пусть определена составная квантовая система XY с матрицей плотности ρ_{XY}. Условная энтропия фон Неймана вводится как обобщение выражения (1.12) (зачастую сохраняется обозначение для энтропии Шеннона $H(X|Y)$):

$$H(\rho_{XY}|\rho_Y) = H(X|Y) \equiv S(\rho_{XY}) - S(\rho_Y), \tag{1.14}$$

где матрица плотности подсистемы Y выражается через частичный след $\rho_Y = \mathrm{tr}_X(\rho_{XY})$.

Квантовой условной min-энтропией называется величина

$$H_{\min}(\rho_{XY}|\rho_Y) \equiv -\log \lambda, \tag{1.15}$$

где λ — наименьшее вещественное число, при котором матрица $\lambda \cdot I \otimes \rho_Y - \rho_{XY}$ положительно определена, I — единичный оператор.

Гладкой (ε-гладкой) условной min-энтропией называется величина

$$H^{\varepsilon}_{\min}(\rho_{XY}|\rho_Y) \equiv \max_{\sigma_{XY} \in B_\varepsilon(\rho_{XY})} H_{\min}(\sigma_{XY}|\rho_Y), \tag{1.16}$$

где $B_\varepsilon(\rho_{XY})$ — ε-окрестность матрицы ρ_{XY} в смысле следового расстояния, такая что $\|\rho_{XY} - \sigma_{XY}\|_1 \leqslant \varepsilon$.

Согласно теореме, доказанной в работе [13], следовое расстояние между матрицей плотности ρ_{XE} и идеальной матрицей $\rho_U \otimes \rho_E$ мажорируется с использованием ε-гладкой min-энтропии:

$$D\left(\rho_{XE}^{(l)}, \rho_U^{(l)} \otimes \rho_E^{(l)}\right) \leqslant \varepsilon' + \frac{1}{2}\sqrt{2^{-H_{\min}^{\varepsilon'}(\rho_{XE}^{(n)}|\rho_E^{(n)}) + leak_n + l}}, \tag{1.17}$$

где $\rho_{XE}^{(n)}$ — матрица плотности квантовой системы Алиса—Ева после процедуры согласования базисов, $\rho_E^{(n)}$ — матрица плотности квантовой системы Евы после процедуры согласования базисов, $leak_n$ — количество бит, разглашенных при постобработке, l — длина секретного ключа.

Тогда из неравенства (1.17) следует, что достаточным условием для выполнения критерия ε-секретности (1.4) является выполнение неравенства

$$l \leqslant H_{\min}^{\varepsilon/2}(\rho_{XE}^{(n)}|\rho_E^{(n)}) - leak_n - 2\log\frac{1}{\varepsilon}, \tag{1.18}$$

где $\varepsilon = 2\varepsilon'$.

Таким образом, секретность ключа обеспечивается сжатием ключа до требуемой длины при процедуре усиления секретности. Вся информация о действиях Евы (атаках) заключена в гладкой min-энтропии. Заметим, что данная энтропия зависит от матрицы плотности системы Алиса—Ева, явный вид которой в общем случае неизвестен. Тем не менее, энтропийный подход позволяет произвести оценку снизу для длины ключа l с помощью методов, которые будут описаны далее.

Прямое вычисление гладкой min-энтропии может быть трудной задачей, поэтому удобно свести анализ к энтропиям фон Неймана. Для дальнейшего рассмотрения ограничимся протоколами КРК с независимыми посылками (например, BB84), т. е. такими, для которых квантовое состояние, отвечающее просеянному ключу, может быть представлено как тензорное произведение однокубитовых состояний ρ_{XE}:

$$\rho_{XE}^{(n)} = \rho_{XE}^{\otimes n}. \tag{1.19}$$

Это оказывается возможным благодаря квантовой теореме де Финетти [13], гласящей, что симметричное относительно перестановок квантовое состояние может быть сколь угодно близко приближено тензорным произведением

матриц плотности одночастичных квантовых состояний. Данная перестановочная симметрия может достигаться путем случайных (согласованных между Алисой и Бобом) перестановок измеренных бит [18].

Результаты работы [13] позволяют провести цепочку неравенств:

$$H_{\min}^{\varepsilon/2}(\rho_{XE}^{(n)}|\rho_E^{(n)}) \geqslant H_{\min}^{\varepsilon/2}(\rho_{XE}^{(n_1)}|\rho_E^{(n_1)}) \geqslant$$
$$\geqslant n_1 H(\rho_{XE}|\rho_E) - \sqrt{n_1}\log 5 \cdot \sqrt{2\log\frac{2}{\varepsilon}} \geqslant$$
$$\geqslant n_1 S(\rho_{XE}) - n_1 S(\rho_E) - \sqrt{n_1}\log 5 \cdot \sqrt{2\log\frac{2}{\varepsilon}}, \qquad (1.20)$$

где n_1 — количество посылок, отвечавших однофотонной компоненте, ρ_{XE} — матрица плотности квантовой системы Алиса—Ева для однофотонной компоненты, ρ_E — матрица плотности квантовой системы Евы для однофотонной компоненты. Здесь было использовано свойство аддитивности энтропии фон Неймана.

Таким образом, выполнение критерия секретности можно гарантировать в терминах энтропий фон Неймана от матриц плотности для отдельных посылок. В дальнейшем это позволит значительно упростить рассмотрение действий нарушителя.

Итоговое выражение для достаточного условия секретности (1.18) в случае независимых посылок удобно записать в виде неравенства для относительной длины секретного ключа:

$$\ell \equiv \frac{l}{n} \leqslant \Omega_1 S(\rho_{XE}) - \Omega_1 S(\rho_E) - leak - \delta, \qquad (1.21)$$

где Ω_1 — доля посылок, отвечавших однофотонной компоненте (метод оценки данной величины будет описан далее), $leak \equiv \frac{leak_n}{n}$ — доля бит, разглашенных при постобработке, а δ определяется выражением

$$\delta \equiv \sqrt{\frac{\Omega_1}{n}}\log 5 \cdot \sqrt{2\log\frac{2}{\varepsilon}} + \frac{2}{n}\log\frac{1}{\varepsilon}. \qquad (1.22)$$

Поскольку δ стремится к нулю в пределе бесконечных битовых последовательностей, данный член можно интерпретировать как поправку на конечную длину ключа.

1.3 Доказательство секретности протоколов КРК

Выражение (1.21) все еще содержит недоступные прямому наблюдению величины, а именно матрицы плотности ρ_{XE} и ρ_E. Явный вид данных матриц плотности зависит от действий нарушителя, который осуществляет атаку — попытку понизить уровень безопасности криптографической (в данном случае, квантовокриптографической) системы. Для обеспечения секретности в условиях атаки нарушителя протокол КРК должен предусматривать оценку параметров, через которые могут быть построены консервативные оценки (т. е. предполагающие оптимальность действий нарушителя) данных матриц плотности. В случае если атака не влияет на вид матриц плотности, то она должна быть пресечена техническими средствами, либо факт ее проведения должен детектироваться с надлежащей вероятностью.

Для начала рассмотрим случай идеальной технической реализации аппаратуры Алисы и Боба. Формально данное требование означает, что Алиса и Боб выполняют те и только те действия, которые предусмотрены протоколом КРК. На практике данное требование сводится к обеспечению доверия к используемому оборудованию (в частности, ГСЧ) и изоляции оборудования от внешних полей и механического воздействия[10]. В таком случае, единственной возможностью Евы является попытка извлечь информацию, воздействуя непосредственно на квантовые состояния, распространяемые по каналу между пользователями. Данный класс атак называют атаками на протокол, или атаками на квантовые состояния.

Первоначальное рассмотрение протоколов КРК ограничивалось описанием простейших атак, при этом вопрос оптимальности действий нарушителя выносился за скобки. Построение оптимальной атаки Евы может представляться чрезвычайно сложной задачей, поскольку в общем случае она располагает квантовой системой бесконечной размерности. Тем не менее, для ряда протоколов явный вид оптимальной атаки строится на основе симметрийных соображений, а оптимальность обосновывается фундаментальными принципами. Наиболее часто используемым фундаментальным принципом являются энтропийные соотношения неопределенности, о которых пойдет речь ниже.

Энтропийные соотношения неопределенности являются расширением знаменитых соотношений неопределенности Гейзенберга [19] и Робертсона [20]. В

работах [21; 22] энтропийные соотношения были сформулированы для результатов измерений над некоммутирующими физическими наблюдаемыми. В работе [23] были сформулированы энтропийные соотношения, применимые к случаю КРК. Пусть ρ_{ABE} — произвольная матрица плотности системы Алиса—Боб—Ева. Пусть Алиса проводит измерение над своей подсистемой в одном из двух ортонормированных базисах R: $\{|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_d\rangle\}$ или S: $\{|\varphi_1\rangle, |\varphi_2\rangle, ..., |\varphi_d\rangle\}$, где d — размерность гильбертова пространства Алисы. Обозначим $H(R|E)$ условную энтропию фон Неймана подсистемы Алиса—Ева после проведения измерений над подсистемой Алисы в базисе R и $H(S|B)$ условную энтропию подсистемы Алиса—Боб после проведения измерений над подсистемой Алисы в базисе S. Тогда выполняется неравенство:

$$H(R|E) + H(S|B) \geqslant \log \frac{1}{c}, \tag{1.23}$$

где

$$c \equiv \max_{j,k} |\langle \psi_j | \varphi_k \rangle|^2. \tag{1.24}$$

Правая часть энтропийных соотношений неопределенности (1.23) содержит параметр c, определяющий максимальное перекрытие между базисами R и S. В нашем случае размерность пространства системы Алисы $d = 2$, и максимум величины c достигается при использовании «сопряженных» базисов, для которых $c = 1/2$. Именно такой набор базисов используется в протоколе BB84 [8]. В этом случае неравенство (1.23) принимает вид

$$H(R|E) + H(S|B) \geqslant 1. \tag{1.25}$$

Для определенности далее будем рассматривать случай использования протокола BB84. В оригинальной работе Ч. Беннета и Ж. Брассара [8] в качестве «сопряженных» базисов предлагалось использовать поляризационные базисы, образованные парами горизонтальной— вертикальной поляризации (H/V) и диагональной— антидиагональной поляризации (D/A). Данные базисы образуются из собственных векторов матриц Паули σ_z и σ_x соответственно. При практической реализации протокола BB84 зачастую используются собственные состояния матрицы Паули σ_y вместо одной из пар, что отвечат правоциркулярной и левоциркулярной поляризации. В дальнейшем, для удобства, будем обозначать базисы H/V и D/A как базисы + (прямой базис) и × (сопряженный

базис) соответственно (данное обозначение также распространяется на случай кодирования, отличного от поляризационного).

Таким образом, энтропийные соотношения неопределенности устанавливают связь между энтропией фон Неймана системы Алиса—Ева и системой Алиса—Боб, что позволяет провести оценку информации, доступной Еве, без построения явного вида матрицы плотности ρ_{XE}. Однако использование данных соотношений для удовлетворения критерия ε-секретности (1.4) требует математической формализации рассматриваемого протокола КРК. Рассмотрим протокол BB84 и сформулируем так называемую ЭПР—версию данного протокола[2] [25].

Алиса приготавливает ЭПР—пару в состоянии

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0^+\rangle_A \otimes |0^+\rangle_B + |1^+\rangle_A \otimes |1^+\rangle_B\right), \tag{1.26}$$

где $|0^+\rangle$ и $|1^+\rangle$ — состояния прямого базиса. Алиса оставляет себе подсистему A, в то время как подсистему B она отправляет Бобу по квантовому каналу. Далее, Алиса и Боб выбирают измерительные базисы. Измерения описываются набором POVM-операторов, дающих ортогональное разложение единичного оператора I_A (для Алисы) и I_B (для Боба):

$$I_A = |0^+\rangle_A\langle 0^+| + |1^+\rangle_A\langle 1^+|, \quad I_B = |0^+\rangle_B\langle 0^+| + |1^+\rangle_B\langle 1^+| \tag{1.27}$$

для измерений в прямом базисе и

$$I_A = |0^\times\rangle_A\langle 0^\times| + |1^\times\rangle_A\langle 1^\times|, \quad I_B = |0^\times\rangle_B\langle 0^\times| + |1^\times\rangle_B\langle 1^\times| \tag{1.28}$$

для измерений в сопряженном базисе. Здесь $|0^\times\rangle_{A,B}$ и $|1^\times\rangle_{A,B}$ — состояния сопряженного базиса Алисы и Боба, соответственно, которые могут быть представлены в виде суперпозиции состояний прямого базиса:

$$|0^\times\rangle_{A,B} = \frac{1}{\sqrt{2}}\left(|0^+\rangle_{A,B} + |1^+\rangle_{A,B}\right), \quad |1^\times\rangle_{A,B} = \frac{1}{\sqrt{2}}\left(|0^+\rangle_{A,B} - |1^+\rangle_{A,B}\right). \tag{1.29}$$

В то же время, воздействие нарушителя общего вида описывается совместным унитарным преобразованием U_{BE} «половины» ЭПР—пары, направленной Бобу, и квантовой системы Евы:

$$|\Psi\rangle_{ABE} = U_{BE}\left(|\Psi\rangle_{AB} \otimes |E\rangle_E\right), \tag{1.30}$$

[2] название отсылает к знаменитому парадоксу Эйнштейна—Подольского—Розена [24], касавшегося проблемы измерений связанных частиц. В дальнейшем, термин ЭПР—пара распространился как обозначение двухкубитовой системы, находящейся в запутанном состоянии

где $|E\rangle_E$ — проинициализированное состояние системы Евы.

К полученной системе Алиса—Боб—Ева применимы энтропийные соотношения, описанные выше. В то же время, ЭПР—версия BB84 оказывается эквивалентной стандартной версии протокола со случайным и равновероятным выбором одного из четырех состояний. Итоговые энтропийные соотношения с учетом измерений Алисы и Боба можно записать в следующем виде:

$$H(X^+|E) + H(X^\times|Y^\times) \geqslant 1, \tag{1.31}$$

$$H(X^\times|E) + H(X^+|Y^+) \geqslant 1, \tag{1.32}$$

где X^+, $X^\times$ и Y^+, $Y^\times$ относятся к квантовым системам Алисы и Боба после проведения измерений в базисе $+$ и $\times$. Здесь мы воспользовались тем фактом, что энтропия системы не убывает после проведения измерений [23]. Заметим, что полученные условные энтропии фон Неймана системы Алиса—Боб могут быть заменены энтропиями Шеннона, поскольку после проведения измерений система вероятностным образом коллапсирует в одно из базисных состояний. Соответствующие вероятности могут быть оценены экспериментально.

Таким образом, для оценки относительной длины секретного ключа с учетом достаточного условия секретности (1.21) необходимо выделить биты, выработанные в базисах $+$ и $\times$. Относительные длины ключа для соответствующих битовых строк должны удовлетворять следующим неравенствам:

$$\ell^+ \leqslant \Omega_1^+ H(X^+|E) - leak^+ - \delta^+ = \Omega_1^+ \left[1 - H(X^\times|Y^\times)\right] - leak^+ - \delta^+, \tag{1.33}$$

$$\ell^\times \leqslant \Omega_1^\times H(X^\times|E) - leak^\times - \delta^\times = \Omega_1^\times \left[1 - H(X^+|Y^+)\right] - leak^\times - \delta^\times, \tag{1.34}$$

где символы $+$ и $\times$ указывают на принадлежность к битам, полученным в соответствующем базисе. Здесь было сделано допущение в пользу нарушителя о возможности достижения минимума энтропийных соотношений, поэтому перед правыми частями выражений (1.33) и (1.34) стоит знак равенства.

Для простоты формул будем считать, что ключ вырабатывается лишь в одном базисе (например, в прямом), а сопряженный базис используется лишь для оценки условной энтропии (на практике ключ вырабатывается во всех базисах). Опустим обозначения, указывающие на принадлежность к базису. Тогда достаточное условие секретности примет вид

$$\ell \leqslant \Omega_1 \left[1 - H(X|Y)\right] - leak - \delta. \tag{1.35}$$

Заметим, что правая часть выражения (1.35) не содержит величин, зависящих от системы Евы и может быть оценена экспериментально.

1.4 Оценка параметров

Выражение для длины секретного ключа (1.35) содержит величины, вычисление которых требует экспериментальных оценок. Условная энтропия системы Алиса—Боб после измерений, имеющая смысл «нехватки информации» Боба относительно битовой строки Алисы, может быть вычислена с помощью формул (1.9) — (1.12) при наличии оценки вероятности ошибочного измерения. В протоколе BB84 данная оценка дается путем измерения частоты битовой ошибки — величины QBER.

Удобно рассмотреть распределение ключа как передачу бит по каналу с ошибкой. В данном случае можно ограничиться рассмотрением двоичного симметричного канала, то есть канала с одинаковой вероятностью ошибки для нулевого и единичного бита (данное рассмотрение не ограничивает общности, поскольку свойство вогнутости энтропийных функций делает случай совпадающих вероятностей наиболее консервативным). Напомним, что достаточное условие секретности было получено для однофотонной компоненты отправляемых посылок. Пусть вероятность ошибочного измерения для однофотонной компоненты равна E_1 — в общем случае, данная величина неизвестна и не может быть прямо оценена через QBER (существующий способ оценки будет описан позже). Путем прямого вычисления [26], можно получить, что

$$H(X|Y) = h(E_1), \tag{1.36}$$

где $h(x) \equiv -x \log x - (1-x)\log(1-x)$ — бинарная энтропийная функция Шеннона.

Величина классической утечки $leak$ также тесно связана с условной энтропией системы Алиса—Боб, однако при ее вычислении следует учитывать не только однофотонную компоненту, поскольку исходы измерений с различным числом фотонов для Алисы и Боба неразличимы. При использовании оптимальных шенноновских кодов коррекции ошибок [27] величина $leak$ оказывается тождественно равна условной энтропии Шеннона для множества всех измерений Алисы и Боба в совпавших базисах. На практике используются менее эффективные коды коррекции, для которых имеет место эвристическая зависимость

$$leak = f_{EC}\, h(E_\mu), \tag{1.37}$$

где f_{EC} — параметр эффективности коррекции ошибок, как правило, лежащий в диапазоне $1.05 - 1.5$ [28], E_μ — общая вероятность ошибочного измерения в заданном базисе для импульсов Алисы со средним числом фотонов μ. Оценка величины E_μ дается через QBER.

Оценка доли однофотонной компоненты Ω_1 может быть дана путем прямой характеризации источника по заданному параметру — среднему числу фотонов в импульсах Алисы μ. Вероятность появления k фотонов в импульсе с параметром μ описывается распределением Пуассона $P_\mu(k)$. Отсюда имеет место консервативная оценка доли однофотонной компоненты [29]:

$$\Omega_1 \geqslant 1 - \frac{P(k>1)}{Q_\mu}, \tag{1.38}$$

где $P(k>1)$ — вероятность испускания источником компоненты, отвечающей более чем одному фотону, Q_μ — темп отсчетов на приемной стороне (частота детектирования при условии отправки импульса со средним числом фотонов μ). Обе величины могут быть определены легитимными участниками — среднее число фотонов может быть измерено предварительно (или во время сеанса КРК), а темп отсчетов определяется по завершении детектирования серии импульсов.

Консервативную оценку можно получить и для вероятности ошибки в однофотонной компоненте [29]:

$$E_1 \leqslant \frac{E_\mu}{\Omega_1}, \tag{1.39}$$

где E_μ оценивается через QBER, а Ω_1 берется из формулы (1.38).

Использование данных оценок обеспечивает выполнения критерия секретности. В то же время, данные оценки являются консервативными, т. е. дают сильно заниженный (завышенный) результат в пользу нарушителя, что негативно сказывается на скорости и максимальной дальности выработки ключа. Для построения более точных оценок необходимо использовать метод состояний-ловушек («decoy state») [30—32].

Метод состояний-ловушек заключается в том, что Алиса использует несколько различных когерентных состояний с различным средним числом фотонов. Состояния приготавливаются так, чтобы их начальная фаза была случайной и распределенной равномерно на интервале $[0, 2\pi]$. Помимо сигнальных состояний со средним числом фотонов μ используются так называемые

состояния-ловушки со средним числом фотонов $\nu_1, \nu_2, ..., \nu_m$, где m — число используемых состояний ловушек. Алиса случайным образом выбирает одно из них для отправки Бобу. В то же время, Боб (как и Ева) не знает, какое именно состояние было выбрано. На этапе обмена информацией по классическому каналу Алиса оглашает какому среднему числу фотонов отвечала каждая посылка, что позволяет Бобу вычислить темпы отсчетов для каждого типа посылок, а так же оценить для них уровень битовой ошибки. Используя результаты вычислений, Алиса и Боб могут оценить параметры протокола, в частности, можно оценить величины E_1, E_μ и Ω_1.

Точность оценок по методу «decoy state» зависит от числа состояний-ловушек и их параметров. Наиболее распространен вариант с двумя состояниями-ловушками. В работе [32] было показано, что наиболее точные оценки получаются при использовании состояний-ловушек с параметрами $\nu_1 \equiv \nu < \mu$ и $\nu_2 = 0$. Далее мы будем предполагать использование именно этого метода для упрощения формул, однако результаты можно распространить на случай произвольных состояний-ловушек.

Измерив темпы отсчетов Q_μ, Q_ν, Q_0 для сигнальных состояний, состояний-ловушек и вакуумных состояний, соответственно, а также оценив вероятности ошибок E_μ, E_ν для сигнальных состояний и состояний-ловушек, можно сделать следующие оценки:

$$Q_1 = Y_1 \mu e^{-\mu}, \tag{1.40}$$

$$Y_1 \geqslant Y_1^L \equiv \frac{\mu}{\nu(\mu-\nu)} \left[Q_\nu e^\nu - \frac{\nu^2}{\mu^2} Q_\mu e^\mu - \frac{\mu^2-\nu^2}{\mu^2} Q_0 \right], \tag{1.41}$$

$$E_1 \leqslant E_1^U \equiv \frac{E_\nu Q_\nu e^\nu - E_0 Q_0}{\nu Y_1^L}, \tag{1.42}$$

где Q_1 — темп отсчетов для однофотонной компоненты сигнальных состояний, Y_1 — выход (yield) однофотонной компоненты (условная вероятность детектирования сигнала при условии содержания в нем одного фотона), Y_1^L — нижняя оценка для Y_1 по методу «decoy state», E_1 — вероятность ошибки для однофотонной компоненты, E_1^U — верхняя оценка вероятности ошибки для однофотонной компоненты по методу «decoy state», E_0 — вероятность ошибки для вакуумной компоненты. Важно заметить, что μ и ν в данных выражениях обозначают полные интенсивности отправляемых состояний, которые в случае фазового кодирования часто представляют собой два отдельных импульса [33; 34].

Отсюда справедлива оценка

$$\Omega_1 = \frac{Q_1}{Q_\mu} \geqslant \Omega_1^L \equiv \frac{Y_1^L \mu e^{-\mu}}{Q_\mu}, \tag{1.43}$$

где Ω_1^L — нижняя оценка доли однофотонной компоненты по методу «decoy state».

Совместив выражения (1.35) — (1.37) и подставив в них оценки (1.42) и (1.43), можно получить выражение для длины секретного ключа в протоколе BB84 с учетом метода «decoy state»:

$$\ell \leqslant \Omega_1^L \left[1 - h(E_1^U)\right] - f_{EC}\, h(E_\mu) - \delta, \tag{1.44}$$

Подытоживая, заметим, что неточность оценки параметров в связи со статистическими эффектами также может быть учтена в выражении (1.44). Для этого экспериментально определяемые величины следует заменить на правые (левые) оценки внутри выбранного доверительного интервала. Конечность доверительного интервала может быть учтена в параметре δ (см. подробности в [25; 26; 35]). Далее мы будем использовать обозначения, принятые в выражении (1.44), подразумевая, что статистические эффекты в полученных оценках учтены.

1.5 Унитарная атака

Приведенные выше результаты были получены с учетом всевозможных действий нарушителя, направленных на состояния в квантовом канале, т. е. с учетом атак на протокол (или атак на квантовые состояния). Использование энтропийных соотношений неопределенности (1.23), (1.31) и (1.32) позволило обойтись без явного вида матрицы плотности системы Алиса—Боб—Ева, т. е. без явного построения атаки. Представленные в литературе явные построения атак на квантовые состояния для протокола BB84 носят иллюстративный характер (см., например, [18]). Картина радикально меняется при комбинировании атак на квантовые состояния с несовершенствами технической реализации (например, с атаками по побочным каналам), что приводит к необходимости явного построения атак на протокол [25]. Оказывается, что для множества протоколов КРК, включая BB84, можно построить явную атаку, информационный

выигрыш которой совпадает с границей, установленной энтропийными соотношениями неопределенности. Такая атака (или параметрическое семейство атак) является оптимальной, а значит, ее рассмотрение не ограничивает общности при доказательстве секретности протокола.

Опишем оптимальную атаку для протокола BB84. Преобразование общего вида, осуществляемое Евой, описывается унитарным оператором $U_{BE}^{(n)}$, действующим на все n посылок, отправляемых за сеанс, а также на квантовую систему Евы, над которой она проводит коллективное измерение после разглашения базисов. Данная атака называется когерентной, являясь частным случаем унитарных атак [18; 36]. Как было показано выше, благодаря квантовой теореме де Финетти состояния в канале факторизуется на n независимых состояний. Это позволяет ограничить рассмотрение случаем факторизующихся операторов $U_{BE}^{(n)} = U_{BE}^{\otimes n}$. Оператор U_{BE} действует на отдельную посылку в канале и на отдельный регистр в квантовой системе Евы, аналогично выражению (1.30). После разглашения базисов Ева проводит коллективное измерение над всеми регистрами своей системы. Данная атака называется коллективной[3] [18; 36]. Коллективная атака совпадает по эффективности с когерентной атакой при соблюдении условий квантовой теоремы де Финетти, что делает ее оптимальной для протокола BB84 и других протоколов с независимыми посылками.

В общем случае, можно построить бесконечное множество коллективных атак. Однако, как было показано в [37], для протокола BB84 достаточно рассмотреть однопараметрическое семейство симметричных атак, которые описываются следующим унитарным преобразованием:

$$U_{BE}|0\rangle_B \otimes |E\rangle_E = \cos\alpha\,|0\rangle_B \otimes |\Phi_0\rangle_E + \sin\alpha\,|1\rangle_B \otimes |\Theta_0\rangle_E, \tag{1.45}$$

$$U_{BE}|1\rangle_B \otimes |E\rangle_E = \cos\alpha\,|1\rangle_B \otimes |\Phi_1\rangle_E + \sin\alpha\,|0\rangle_B \otimes |\Theta_1\rangle_E, \tag{1.46}$$

где $|0\rangle_B$ и $|1\rangle_B$ задают состояния из выбранного базиса, α — параметр атаки, $|\Phi_{0,1}\rangle_E$ и $|\Theta_{0,1}\rangle_E$ — преобразованные состояния Евы, удовлетворяющие условиям

$$\langle\Phi_0|\Phi_1\rangle_E = \langle\Theta_0|\Theta_1\rangle_E = \cos 2\alpha, \quad \langle\Phi_{0,1}|\Theta_{0,1}\rangle_E = 0, \tag{1.47}$$

Таким образом, угол между состояниями Евы, отвечающим различным битам, равен 2α.

[3] в литературе также встречается наименование «индивидуальная атака с коллективными измерениями» более точно отражающее ее структуру [25]; мы, тем не менее, будем придерживаться названия «коллективная атака» во избежание путаницы со стандартной индивидуальной унитарной атакой.

В результате применения унитарного преобразования (1.45) и (1.46) к системе Алиса—Боб—Ева по формуле (1.30), а также после проведения измерений на стороне Алисы и Боба, можно получить явное выражение для результирующей матрицы плотности системы Алиса—Боб—Ева:

$$\begin{aligned}\rho_{XYE} = \\ = \frac{1}{2}|0\rangle_X\langle 0| \otimes \Big[\cos^2\alpha|0\rangle_Y\langle 0| \otimes |\Phi_0\rangle_E\langle\Phi_0| + \sin^2\alpha|1\rangle_Y\langle 1| \otimes |\Theta_0\rangle_E\langle\Theta_0|\Big] + \\ + \frac{1}{2}|1\rangle_X\langle 1| \otimes \Big[\cos^2\alpha|1\rangle_Y\langle 1| \otimes |\Phi_1\rangle_E\langle\Phi_1| + \sin^2\alpha|0\rangle_Y\langle 0| \otimes |\Theta_1\rangle_E\langle\Theta_1|\Big].\end{aligned} \tag{1.48}$$

Из нее выражаются матрицы плотности подсистем, необходимые для вычисления условной энтропии Алиса—Ева, путем взятия частичного следа:

$$\begin{aligned}\rho_{XE} = \mathrm{tr}_Y\rho_{XYE} = \frac{1}{2}|0\rangle_X\langle 0| \otimes \Big[\cos^2\alpha|\Phi_0\rangle_E\langle\Phi_0| + \sin^2\alpha|\Theta_0\rangle_E\langle\Theta_0|\Big] + \\ + \frac{1}{2}|1\rangle_X\langle 1| \otimes \Big[\cos^2\alpha|\Phi_1\rangle_E\langle\Phi_1| + \sin^2\alpha|\Theta_1\rangle_E\langle\Theta_1|\Big],\end{aligned} \tag{1.49}$$

$$\begin{aligned}\rho_E = \mathrm{tr}_X\rho_{XE} = \frac{1}{2}\Big[\cos^2\alpha|\Phi_0\rangle_E\langle\Phi_0| + \sin^2\alpha|\Theta_0\rangle_E\langle\Theta_0|\Big] + \\ + \frac{1}{2}\Big[\cos^2\alpha|\Phi_1\rangle_E\langle\Phi_1| + \sin^2\alpha|\Theta_1\rangle_E\langle\Theta_1|\Big].\end{aligned} \tag{1.50}$$

Для вычисления условной энтропии фон Неймана вычисляются собственные значения матриц плотности ρ_{XE} и ρ_E. Матрица плотности ρ_{XE} диагональна в записанном базисе, поэтому ее собственные значения равны

$$\lambda_1 = \lambda_2 = \frac{1}{2}\cos^2\alpha, \quad \lambda_3 = \lambda_4 = \frac{1}{2}\sin^2\alpha. \tag{1.51}$$

Далее вычисляется энтропия фон Неймана для матрицы плотности ρ_{XE}:

$$S(\rho_{XE}) = -\sum\lambda_i\log\lambda_i = 1 + h(\sin^2\alpha). \tag{1.52}$$

Матрица плотности ρ_E не является диагональной в записанном базисе, и для нахождения ее собственных значений решается секулярное уравнение

$$\det(\rho_E - \lambda\cdot I) = 0, \tag{1.53}$$

где I — единичная матрица. В базисе $\{|\Phi_0\rangle_E, |\Phi_1\rangle_E, |\Theta_0\rangle_E, |\Theta_1\rangle_E\}$ матрица плотности ρ_E имеет блочный вид:

$$\rho_E = \frac{1}{2}\begin{pmatrix}\cos^2\alpha\cdot B & O \\ O & \sin^2\alpha\cdot B\end{pmatrix}, \tag{1.54}$$

где O — нулевая матрица, а матрица B имеет вид

$$B = \begin{pmatrix} 1+\cos^2 2\alpha & 2\cos 2\alpha \\ 2\cos 2\alpha & 1+\cos^2 2\alpha \end{pmatrix}. \tag{1.55}$$

Выразив единичный оператор в базисе $\{|\Phi_0\rangle_E, |\Phi_1\rangle_E\}$ и $\{|\Theta_0\rangle_E, |\Theta_1\rangle_E\}$, можно записать секулярные уравнения для матрицы B для нахождения ее собственных значений Λ:

$$\det \begin{pmatrix} 1+\cos^2 2\alpha - \Lambda & \cos 2\alpha \cdot (2-\Lambda) \\ \cos 2\alpha \cdot (2-\Lambda) & 1+\cos^2 2\alpha - \Lambda \end{pmatrix} = 0. \tag{1.56}$$

В результате решения уравнения (1.56) получаются следующие собственные значения:

$$\Lambda = 1 \pm \cos 2\alpha = \begin{cases} 2\cos^2 \alpha, \\ 2\sin^2 \alpha. \end{cases} \tag{1.57}$$

Тогда, собственные значения матрицы плотности ρ_E выражаются следующим образом:

$$\lambda_1 = \cos^2\alpha\cos^2\alpha, \quad \lambda_2 = \lambda_3 = \sin^2\alpha\cos^2\alpha, \quad \lambda_4 = \sin^2\alpha\sin^2\alpha \tag{1.58}$$

Далее вычисляется энтропия фон Неймана для матрицы плотности ρ_E:

$$S(\rho_E) = -\sum \lambda_i \log \lambda_i = 2h(\sin^2\alpha). \tag{1.59}$$

Условная энтропия системы Алиса—Ева равна

$$H(X|E) = S(\rho_{XE}) - S(\rho_E) = 1 - h(\sin^2\alpha). \tag{1.60}$$

Тогда, достаточное условие секретности (1.21) приобретет следующий вид:

$$\ell \leqslant \Omega_1 \left[1 - h(\sin^2\alpha)\right] - leak - \delta. \tag{1.61}$$

Для того, чтобы понять физический смысл параметра α, обратимся к матрице плотности системы Алиса—Боб:

$$\begin{aligned} \rho_{XY} = \mathrm{tr}_E \rho_{XYE} = \frac{1}{2}|0\rangle_X\langle 0| \otimes \left[\cos^2\alpha|0\rangle_Y\langle 0| + \sin^2\alpha|1\rangle_Y\langle 1|\right] + \\ + \frac{1}{2}|1\rangle_X\langle 1| \otimes \left[\cos^2\alpha|1\rangle_Y\langle 1| + \sin^2\alpha|0\rangle_Y\langle 0|\right], \end{aligned} \tag{1.62}$$

Из структуры матрицы плотности (1.62) видно, что $\sin^2\alpha$ несет смысл вероятности ошибочного измерения бита ключа. Поскольку в рассматриваемом случае ключ вырабатывается только на однофотонной компоненте, доля

которой оценивается методом состояний-ловушек, то данная величина равна вероятности ошибки в однофотонной компоненте:

$$E_1 = \sin^2 \alpha. \tag{1.63}$$

С учетом выражения (1.63) достаточное условие секретности (1.61), полученное при явном построении коллективной атаки, оказывается эквивалентно выражению (1.35), полученному с помощью энтропийных соотношений неопределенности. Данный факт подчеркивает оптимальность коллективной атаки и позволяет использовать ее явный вид при рассмотрении комбинированных атак.

1.6 Атаки на многофотонную компоненту

Атаки, описанные в предыдущем разделе, были направлены на однофотонную компоненту излучения Алисы. Их детектирование легитимными сторонами обеспечивается связью вероятности ошибки в битах ключа (вырабатываемого на однофотонной компоненте) со степенью возмущения квантовых состояний Евой (1.63). В то же время, использование Алисой нестрого однофотонных посылок может быть использовано Евой в попытке считать информацию из квантового состояния без его возмущения. Более того, Ева может фильтровать квантовые состояния в канале, оставляя лишь те, для которых она получает благоприятный исход. Будем называть данный класс атак на квантовые состояния атаками на многофотонную компоненту.

Как и в случае любых атак на квантовые состояния, протокол BB84 с использованием метода «decoy state» обеспечивает защиту от атак на многофотонную компоненту по построению. В данном случае это обеспечивается оценкой доли однофотонной компоненты и вероятностью ошибки в ней по формулам (1.40) — (1.43), что делает данную версию протокола тождественной строго однофотонному случаю. Тем не менее, рассмотрение явных атак на многофотонную компоненту может быть важно с точки зрения оценки рисков в условиях неидеальной технической реализации. В частности, параметры системы, такие как среднее число фотонов в импульсах, могут быть изменены посредством внешнего воздействия, что, в принципе, может позволить Еве

осуществить атаку на многофотонную компоненту оставшись незамеченной. В связи с этим, рассмотрим основные стратегии атак данного типа.

Используемые в КРК когерентные состояния преобразуются самоподобно на элементах с потерями, например, на светоделителе с коэффициентом пропускания по интенсивности T и коэффициентом отражения $1-T$. Поместив такой светоделитель в канал между Алисой и Бобом, Ева может получить «копию» исходного состояния с меньшим средним числом фотонов, над которым Ева может проводить измерения. Данная атака впервые была описана в работе [12] (в этой же работе было экспериментально продемонстрирована устойчивость системы КРК к данной атаке). В литературе данная атака получила название «Beam Splitting» (BS), или атака со светоделителем [38]. В общем случае, нарушитель может выбрать произвольный коэффициент пропускания светоделителя T, а также заменить линию связи на идеальный канал без потерь. Последнее может позволить нарушителю сохранить скорость выработки ключа на уровне, близком к начальному, что убережет от детектирования атаки по наблюдению изменения скорости (отметим, однако, что скорость выработки ключа не входит как параметр в формулу для длины секретного ключа (1.44), и ее контроль в общем случае является опциональным). Отщепленное квантовое состояние нарушитель может сохранить до момента разглашения базисов, после чего провести коллективное измерение над всем ансамблем.

Атака со светоделителем оказывается неэффективной против протоколов, использующих метод «decoy state». Это связано с тем, что полезные для Евы события предполагают одновременного срабатывания детектора Боба и детектора Евы, что возможно лишь в случае реализации n-фотонной компоненты при $n \geqslant 2$. Однофотонная компонента, на которой вырабатывается ключ, приводит к срабатываниям только на стороне Боба, либо Евы, но не на обеих сторонах одновременно. Стоит также заметить, что даже при отсутствии состояний-ловушек (и любого другого метода оценки доли однофотонной компоненты) атака со светоделителем не обеспечивает Еве возможности выявления всего секретного ключа без дополнительной фильтрации состояний из-за ненулевой вероятности однофотонной компоненты.

Другим вариантом атаки на многофотонную компоненту является атака «Photon Number Splitting» (PNS), или атака с расщеплением по числу фотонов [39]. Ключевым отличием данной атаки от BS-атаки является полная или частичная блокировка неинфоматичной для Евы однофотонной компоненты

(для некоторых протоколов Еве также требуется блокировка компонент высших порядков [40]). Для этого Ева проводит неразрушающее измерение числа фотонов в квантовом состоянии и принимает решение о блокировке в зависимости от исхода. При обнаружении двух фотонов и более, Ева сохраняет квантовое состояние и проводит измерение над ним после разглашения базисов. Как и в случае атаки со светоделителем, Ева может заменить линию связи на идеальный канал для компенсации просадки скорости из-за блокировки однофотонной компоненты. Действуя таким образом, Ева может получить весь ключ. Метод «decoy state» исключает данную возможность (исторически, данный метод был предложен именно для защиты от PNS-атак [30; 31]).

Несмотря на потенциальную возможность раскрытия всего ключа, PNS-атака не представляется предпочтительной с точки зрения Евы. Это связано со значительными экспериментальными сложностями в ее реализации, в частности, с осуществлением неразрушающих измерений числа фотонов (скепсис по поводу возможности реализации атаки представлен в работах [9; 41], хотя в этой области есть и некоторые продвижения [42; 43]).

С этой точки зрения более перспективным представляется класс атак, использующих измерения с определенным исходом (Unambiguous Measurements — UM), или однозначное различение состояний (Unambiguous State Discrimination — USD) [44; 45]. Измерения такого рода позволяют однозначно различить N линейно независимых состояний с некоторой вероятностью, в общем случае отличной от единицы (такие измерения также иногда называют безошибочными). В случае успешного различения Ева сохраняет исход, в ином случае Ева блокирует посылку. Известно, что такие измерения над когерентными состояниями можно провести с использованием лишь линейных оптических элементов [46], что значительно упрощает практическую реализацию. Тем не менее, предложенные ранее стратегии USD-атак [44—46] представляются чрезмерно ресурсозатратными и тяжело выполнимыми в реальных условиях. Реалистичная USD-атака, предложенная в рамках настоящей работы, будет описана в главе 3.

Осуществимость USD-атак зависит от набора состояний, используемых в протоколе КРК. Согласно теореме о возможности осуществления UM, необходимым условием возможности однозначного различения N состояний является их линейная независимость [45]. При выработке ключа на однофотонной компоненте (например, при использовании метода «decoy state»), а также при отсутствии

дополнительных паразитных мод, ассоциированных с битовыми состояниями, UM возможны, если число состояний, используемых в протоколе не превышает размерность пространства состояний. Размерность состояний протокола BB84 равна 2, в то время как используется 4 состояния, следовательно, UM невозможны при идеальной технической реализации. В то же время, протоколы использующие 2 состояния (например, B92 [47]) могут быть подвержены USD-атакам.

1.7 Несовершенства технической реализации

Полученные выше результаты были получены в предположении идеальной технической реализации протокола КРК, или, иначе говоря, в предположении, что Алиса и Боб осуществляют те и только те действия, которые предусмотрены протоколом. По существу, к практической реализации системы КРК предъявляются следующие требования[4][10]:

1. Установки Алисы и Боба изолированы от внешнего воздействия (т. е. от внешних полей и вещества);
2. Алиса и Боб используют доверенное оборудование;
3. Классический канал между Алисой и Бобом аутентифицирован.

На практике, удовлетворение каждого из этих требований в полной мере является непростой задачей. Из общих соображений понятно, что при разработке системы данные требования должны быть удовлетворены в максимально полной мере, а недостаток «полноты удовлетворения» должен быть численно оценен и устранен в рамках криптографического протокола. Например, использование неидеальных протоколов аутентификации с известной стойкостью может быть учтено при оценке трудоемкости перебора ключа, наряду с параметром секретности протокола КРК ε [48]. В то же время, достижение максимального выполнения требований 1—2 и оценка степени их достижения являются предметом обширных научных исследований [10; 11; 29; 49]. Неполнота выполнения данных требований может приводить к возможностям

[4]Также очевидно, что обязательным требованием обеспечения секретности рассматриваемых протоколов КРК является верность и полнота квантовой теории. Обсуждение правомерности данного положения выходит за рамки настоящей работы.

осуществления атак на квантовые состояния, а также атак иного рода — атак на техническую реализацию, направленных на конкретные технические несовершенства систем КРК.

В то же время, важно понимать, что учет несовершенств технической реализации не переводит квантово-криптографические системы из разряда систем, секретность которых обеспечивается фундаментальными законами квантовой физики, в разряд систем, секретность которых обеспечивается техническими средствами. Как будет показано далее, несовершенства технической реализации приводят к необходимости дополнительной параметризации и добавления дополнительных допущений для выполнения достаточного условия секретности, в то время как само достаточное условие секретности сохранит чисто квантовую природу.

1.7.1 Несовершенства приготовления и измерения состояний

Как было отмечено, Алиса и Боб должны использовать доверенное оборудование. Это означает, что вся аппаратура должна штатно функционировать в течение всего срока службы системы. Это, с одной стороны, приводит к необходимости экспериментального определения параметров системы, задаваемых используемым оборудованием, а с другой стороны, к необходимости оценки срока службы системы, в течение которого данные параметры не выйдут за пределы допустимых значений с заданной вероятностью. Последнее решается, например, с использованием общей теории надежности [50]. Для решения первой проблемы необходимо выделить конкретные несовершенства технической реализации систем КРК, влияющих на приготовление и измерение квантовых состояний, а также выделить связанные с ними параметры, подлежащие экспериментальной оценке.

Первое несовершенство приготовления квантовых состояний состоит в использовании ослабленных когерентных состояний вместо строго однофотонных. Как обсуждалась выше, данное несовершенство приводит к необходимости оценки доли однофотонной компоненты и ошибки в ней с помощью, например, метода «decoy state». В свою очередь, приготовление когерентных состояний в заданной моде поля с заданной интенсивностью и рандомизированной об-

щей фазой тоже относится к идеальному случаю. На практике данные условия могут выполнятся не полностью. Например, интенсивность когерентных состояний может флуктуировать, а также могут наблюдаться корреляции между последовательно идущими посылками [51]. Для предотвращения корреляций интенсивности и ослабления флуктуаций интенсивности было предложено использовать модулятор интенсивности на базе асимметричного интерферометра Саньяка [52]. Данное решение отличается тем, что конкретное значение интенсивности состояния-ловушки задается лишь коэффициентом пропускания светоделителя, образующего интерферометр, в то время как фазовый модулятор внутри интерферометра выставляется лишь в два состояния — нулевым или полуволновым напряжением, что обеспечивает повышенную стабильность устройства. Далее будем считать, что для модуляции интенсивности используется именно такая реализация.

Другим возможным отклонением от модельного случая может являться возникновение паразитной различимости между состояниями с различными интенсивностями, нарушающее допущение о невозможности Евы различать состояния-ловушки от информационных состояний. В частности, могут возникать дополнительные степени свободы (паразитные моды поля), скоррелированные с интенсивностью состояния, например спектральные, временны́е и пространственные моды [53; 54]. В работах [54; 55] было показано, данные несовершенства можно учесть путем модификации метода «decoy state». Рассмотрим данную модификацию.

Степень различимости состояний ρ_ω и $\rho_{\omega'}$ с разным средним числом фотонов ω и ω' может быть выражена при помощи следового расстояния

$$D_{\omega\omega'} \equiv D(\rho_\omega, \rho_{\omega'}) = \frac{1}{2} \left\| \rho_\omega - \rho_{\omega'} \right\|_1 . \tag{1.64}$$

Тогда, охарактеризовав следовое расстояние $D_{\mu\nu}$ между информационным состоянием и состоянием-ловушкой можно получить модифицированные оценки метода «decoy state» (1.41) и (1.42):

$$Y_1^L \equiv \frac{\mu}{\nu(\mu-\nu)} \left[Q_\nu e^\nu - \frac{\nu^2}{\mu^2} Q_\mu e^\mu - \frac{\mu^2-\nu^2}{\mu^2} Q_0 - 2D_{\mu\nu}(e^\nu - 1) \right], \tag{1.65}$$

$$K^{\mu} \equiv \frac{E_{\mu}Q_{\mu}e^{\mu} - E_0Q_0e^{\mu}}{\mu Y_1^L}, \tag{1.66}$$

$$K^{\nu} \equiv \frac{E_{\nu}Q_{\nu}e^{\nu} - E_0Q_0e^{\nu} + 2\nu D_{\mu\nu}}{\nu Y_1^L}, \tag{1.67}$$

$$K^{\mu\nu} \equiv \frac{E_{\mu}Q_{\mu}e^{\mu} - E_{\nu}Q_{\nu}e^{\nu} + 2D_{\mu\nu}(e^{\nu} - 1)}{(\mu - \nu)Y_1^L}, \tag{1.68}$$

$$E_1^U \equiv \min\{K^{\mu}, K^{\nu}, K^{\mu\nu}\}, \tag{1.69}$$

Выражение для следового расстояния (1.64) содержит явный вид матриц плотности состояний Алисы. В общем случае определение матриц плотности требует полной томографии квантовых состояний Алисы, что может быть сопряжено с рядом сложностей, в т. ч. связанных с бесконечной размерностью Фоковского пространства. Тем не менее, для ряда практических реализаций можно ввести модельные соображения с учетом известных особенностей источников излучения. Так, например, в работе [54] было показано, что прямая модуляция тока накачки диодного лазера для генерации информационных состояний и состояний-ловушек приводит к дополнительной различимости состояний из-за различных спектральных и временны́х профилей импульса при различных интенсивностях излучения (при использовании нескольких лазерных источников для приготовления состояний с разной интенсивностью данная проблема проявляется еще сильнее [53]). Было показано, что в таком случае для оценки следового расстояния $D_{\mu\nu}$ достаточно измерить плотности распределения состояний по времени и по спектру.

Наконец, заметим, что выражения (1.65) — (1.69) получены в предположении пуассоновской статистики состояний по числу фотонов (отсутствии флуктуаций интенсивности) и равномерной рандомизации их общей фазы, что, в общем случае, может не отвечать действительности [56]. Рассмотренные несовершенства могут быть учтены в модифицированной версии метода «decoy state» при характеризации источника, а именно определении реального распределения фазы импульсов, а также их статистики по числу фотонов [57—59]. Показано, что при использовании стандартных лазерных источников с частотами повторений импульсов до 1 ГГц разница в длине ключа по сравнению с установленной выражениями (1.65) — (1.69) невелика. С учетом этого, далее будем пользоваться выражениями (1.65) — (1.69) для сохранения наглядности формул.

Неточность приготовления состояний может также приводить к смещению базисов относительно друг друга (например, вследствие неточной калибровки передатчика). Как видно из выражений (1.23) и (1.24), это приведет к уменьшению нижней границы энтропийных соотношений неопределенности. В последующих выражениях единица заменяется на $\log \frac{1}{c}$ с учетом фактического значения параметра c. На практике можно добиться высокой точности приготовления состояний, поэтому для сохранения наглядности формул будем считать $c = 1/2$.

Более сложной проблемой является неточность приготовления состояний, приводящая к повороту состояний внутри базиса, что может приводить к их неортогональности. В частности, это может приводить к проблеме базисной зависимости состояний (basis dependence), когда матрицы плотности Боба после измерения Алисы в прямом и сопряженном базисах не совпадают (иными словами, используются различные ЭПР-пары при приготовлении состояний в прямом и сопряженном базисах). Подходы, учитывающие данное несовершенство, основываются на оценке степени различимости состояний в разных базисах друг относительно друга [29], либо относительно идеального случая [60].

Измерения, проводимые Бобом, также в реальности могут отличаться от модельных однокубитовых измерений в заданных базисах. В реальных системах в качестве приемника используются детекторы одиночных фотонов (ДОФ), фактически различающие вакуумное состояние от состояний с ненулевым числом фотонов. Квантовая эффективность (вероятность успешного детектирования) ДОФ отлична от 100%, и, как правило, составляет 5—30% для InGaAs фотодиодов, 50—70% для кремниевых фотодиодов и 50—96% для сверхпроводниковых детекторов [61—63]. Эта особенность приводит к двум нежелательным эффектам: во-первых, часть посылок Бобом не детектируется, а во-вторых, при использовании двух и более ДОФ их различие в квантовой эффективности приводит к неравновероятности исходов измерений. Первая проблема не оказывает прямого влияния на безопасность КРК, поскольку «потеря фотонов» при детектировании эквивалентна их потере в линии связи, которая полностью подконтрольна нарушителю. В то же время, вторая проблема приводит к необходимости учитывать квантовую эффективность при явном построении операторов измерений на стороне Боба [25].

1.7.2 Классификация атак на техническую реализацию

Описанные особенности аппаратуры приводят к необходимости модификации протокола КРК с учетом реальных характеристик используемого оборудования, для того чтобы избежать возможности осуществления Евой атак на квантовые состояния. Однако несовершенства аппаратуры 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. Действия такого рода называются атаками на техническую реализацию систем КРК. Проведем классификацию таких атак.

Удобно провести классификацию по методологическому принципу. Атаки можно объединить используя общие принципы их проведения, при этом конкретные способы реализации будут отличаться. Как будет показано ниже, способы обеспечения безопасности КРК в условиях осуществления данных атак также имеют общую методологическую основу для каждого из классов. К этим классам относятся:

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

Рассмотрим каждый из классов подробно.

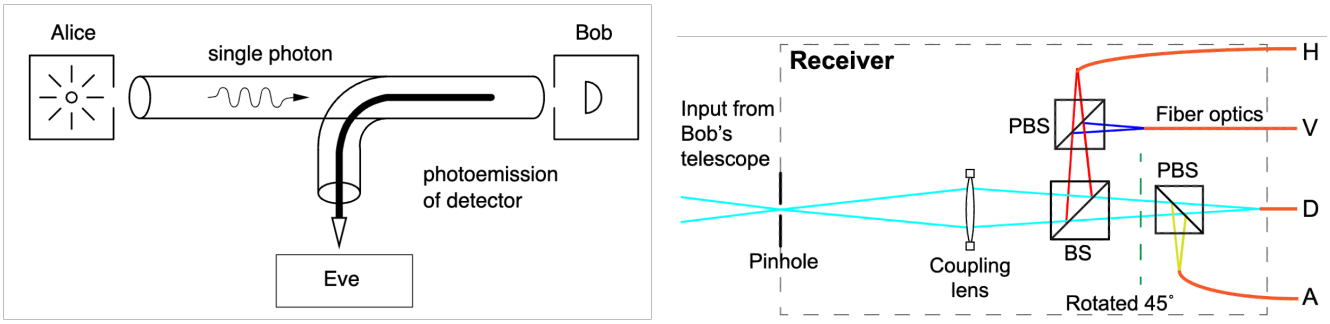
1.7.3 Побочные каналы утечки информации

Побочные каналы утечки информации — термин, унаследованный из классических систем защиты информации. В общем случае, в качестве побочных каналов могут выступать любые сигналы, несущие прямую или косвенную информацию о состоянии системы, которые могут быть использованы нарушителем для получения информации о секретном ключе. Известны электромагнитные радиочастотные [64], оптические [65], акустические [66], временны́е побочные каналы [67], а также побочные каналы по энергопотреблению [68]. Борьба с побочными каналами сводится, в первую очередь, к изоляции системы:

так, например, обеспечение автономного электропитания системы избавляет от побочного канала по энергопотреблению, а запрет на разглашение информации о времени отправки и получения данных избавляет от побочного канала по времени. Для подавления радиочастотных сигналов используется экранирование системы, однако ослабить энергию электромагнитного поля до нуля невозможно. Еще хуже обстоят дела с оптическими сигналами, поскольку они могут быть введены в систему и выведены из нее через оптический канал связи между легитимными пользователями. Это приводит к необходимости учета побочных каналов на уровне протокола КРК.

Внимание побочным каналам утечки в системах КРК стало уделяться с начала нулевых годов. Был выделен пассивный оптический побочный канал, связанный с переизлучением ДОФ из-за явления электролюминисценции (соответствующая атака получала название «Backflash» — BFA) [69], а также активный оптический канал, связанный с отражением излучения, введенного нарушителем внутрь оптической установки легитимного пользователя (атака «Trojan Horse» — THA) [9; 70].

Пассивный побочный канал «Backflash» возникает в связи с излучательной рекомбинацией носителей в полупроводниковых ДОФ при возникновении электронной лавины. Акт срабатывания ДОФ с некоторой вероятностью сопровождается переизлучением фотонов из детектора в сторону канала связи. Говоря точнее, возникает некогерентное излучение низкой интенсивности. Часть излучения, проходя через схему Боба в обратном направлении, выходит в квантовый канал, где может быть зарегистрировано нарушителем (рисунок 1.1а). Известны два варианта проведения атаки: первый нацелен на системы, использующие поляризационное кодирование и пассивный выбор базиса (то есть, без использования модуляторов света — рисунок 1.1б). Проходя через поляризационный светоделитель, изначально неполяризованный переизлученный свет поляризуется, обретая поляризацию, соответствующую сработавшему детектору, и выходит в канал связи. Ева может провести измерение поляризации излучения backflash, что с некоторой вероятностью позволит ей определить значение бита ключа [71]. Второй вариант атаки нацелен на системы, имеющие различную длину оптического пути до различных детекторов (в реальных системах данная особенность возникает практически всегда при использовании двух и более детекторов). В этом случае Ева может определить, какой из детекторов сработал, по времени прихода сигнала [72].



а) б)

Рисунок 1.1 — а) общая схема проведения BFA из работы [69]; б) схема установки Боба с пассивным выбором базиса, уязвимая к BFA из работы [71]. PBS — поляризационный светоделитель, BS — полупрозрачное зеркало, H, V, D, A — ДОФ, принимающие горизонтальную, вертикальную, диагональную и антидиагональную поляризацию соответственно

Активный побочный канал THA возникает в связи с возможностью введения в оптическую установку легитимного пользователя света извне [70; 73; 74]. Часть введенного света, проходя через установку, может отразиться от различных оптических элементов, пройти через устройство приготовления состояния (на стороне Алисы) или выбора базиса (на стороне Боба) и выйти обратно в канал связи, где может быть зарегистрирована нарушителем (рисунок 1.2). При этом на нелегитимное излучение будет наложено то же преобразование, что и на легитимный свет. Это может дать возможность нарушителю определить закодированный бит или выбранный базис.

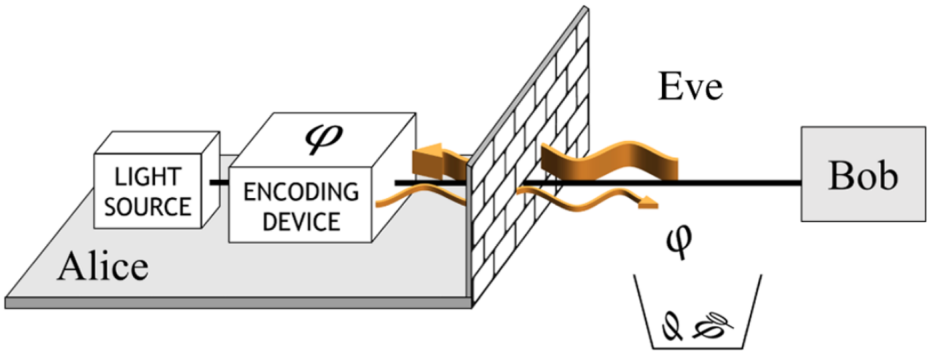


Рисунок 1.2 — Общая схема проведения THA на передатчик системы КРК из работы [74]

Наконец, выделяется оптический побочный канал, возникающий в связи с наличием паразитных мод поля, ассоциированных с битовыми состояниями

в результате неточного приготовления состояний [53; 65]. В частности, это может приводить к различимости состояний, используемых в протоколе КРК, по времени, спектру и пространственному распределению интенсивности. Как правило, данная уязвимость имеет место в системах, использующих несколько лазерных источников для приготовления состояний с различной поляризацией, из-за сложности изготовления полностью идентичных лазерных источников.

Успех атаки Евы по побочным каналам зависит от ее возможностей по различению приходящих к ней сигналов. Вероятность успешного различения тем выше, чем больше энергия различаемых сигналов. В связи с этим, основной мерой защиты от атак по побочным каналам является использование средств, понижающих интенсивность данных сигналов. Могут использоваться такие оптические элементы, как оптические изоляторы и циркуляторы, пропускающие свет лишь в заданном направлении, аттенюаторы, ослабляющие интенсивность излучения, распространяющегося в любом направлении, спектральные фильтры, ослабляющие излучение в заданном спектральном диапазоне и т.д. Понижение интенсивности излучения до нуля такими методами невозможно. Для обеспечения секретности легитимным пользователям необходимо знать конкретные параметры излучения, доходящего до Евы, и учесть их в протоколе КРК. Экспериментальные подходы для анализа побочных каналов были представлены в ряде работ [73—77], однако общая методология, примененная к реальной системе КРК, впервые сформирована в рамках настоящей работы и изложена в главе 2.

Считывание информации по побочным каналам не влияет на наблюдаемые параметры протокола КРК. В частности, оно не приводит к росту QBER. В связи с этим, для учета утечки по побочным каналам требуются модельные соображения. Распространенным в литературе вариантом является бинарная модель пассивного канала BFA [25; 72], а также допущение об использовании Евой когерентных состояний света при активном зондировании THA [25; 73; 74]. Отметим, что такие допущения ограничивают общность рассмотрения описанных атак. Решение данной проблемы будет представлено в главе 2.

Использование модельных допущений позволяет вычислить степень различимость состояний, приходящих к Еве по побочным каналам. Вводится величина фиделити как мера близости двух квантовых состояний, описывае-

мых матрицами плотности ρ и σ [78]:

$$\mathcal{F}(\rho,\sigma)=\left(\mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2. \tag{1.70}$$

Для чистых состояний $\rho=|\psi\rangle\langle\psi|$ и $\sigma=|\varphi\rangle\langle\varphi|$ формула (1.70) выражается через скалярное произведение векторов состояний:

$$\mathcal{F}(\rho,\sigma)=|\langle\psi|\varphi\rangle|^2. \tag{1.71}$$

Попытки учесть степень различимости состояний в побочных каналах при оценке относительной длины секретного ключа предпринимались в ряде работ [29; 74; 79; 80], однако использовавшийся формализм давал консервативно заниженную оценку длины ключа. Достижимая граница утечки информации при совместных коллективных измерениях Евы над ее вспомогательной квантовой подсистемой, введенной в разделе 1.1 и над квантовой подсистемой, ассоциированной с побочным каналом, была впервые представлена в работах С. Н. Молоткова [25; 81]. В рамках предложенного подхода рассматривается комбинированное проведение Евой унитарной коллективной атаки (в разделе 1.5 показана оптимальность данной атаки для протоколов с независимыми посылками) и считывания информации по побочному каналу.

Рассмотрим проведение нарушителем атаки «Trojan Horse» на передатчик Алисы. В общем случае, нарушитель может дождаться этапа оглашения базисов и проводить измерения после этого, что сводит задачу Евы к различению двух состояний в известном базисе. Для определенности, будем считать, что выбран прямой базис; для сопряженного базиса формулы эквивалентны. Пусть $|\xi_0\rangle_{\mathrm{THA}}$ и $|\xi_1\rangle_{\mathrm{THA}}$ — состояния, приходящие к Еве по побочному каналу, когда Алиса посылает Бобу состояния $|0\rangle_B$ и $|1\rangle_B$ соответственно. Эффективно, это приводит к возникновению дополнительной моды в распоряжении Евы и модификацией состояний (1.45) и (1.46):

$$U_{BE}|0\rangle_B\otimes|E\rangle_E\longrightarrow U_{BE}\Big[|0\rangle_B\otimes|E\rangle_E\Big]\otimes|\xi_0\rangle_{\mathrm{THA}} \tag{1.72}$$

$$U_{BE}|1\rangle_B\otimes|E\rangle_E\longrightarrow U_{BE}\Big[|1\rangle_B\otimes|E\rangle_E\Big]\otimes|\xi_1\rangle_{\mathrm{THA}}. \tag{1.73}$$

Тогда, матрица плотности системы Алиса—Боб—Ева с учетом побочного канала ТНА будет выглядеть следующим образом:

$$\begin{aligned}
&\rho_{XYE} = \\
&= \frac{1}{2}|0\rangle_X\langle 0| \otimes \Big[\cos^2\alpha|0\rangle_Y\langle 0| \otimes |\Phi_0\rangle_E\langle\Phi_0| + \sin^2\alpha|1\rangle_Y\langle 1| \otimes |\Theta_0\rangle_E\langle\Theta_0|\Big]\otimes \\
&\quad\otimes|\xi_0\rangle_{\text{ТНА}}\langle\xi_0| + \\
&+\frac{1}{2}|1\rangle_X\langle 1| \otimes \Big[\cos^2\alpha|1\rangle_Y\langle 1| \otimes |\Phi_1\rangle_E\langle\Phi_1| + \sin^2\alpha|0\rangle_Y\langle 0| \otimes |\Theta_1\rangle_E\langle\Theta_1|\Big]\otimes \\
&\quad\otimes|\xi_1\rangle_{\text{ТНА}}\langle\xi_1|.
\end{aligned} \tag{1.74}$$

Для обновленной матрицы плотности повторяются вычисления из раздела 1.5. Из нее выражаются матрицы плотности подсистем, необходимые для вычисления условной энтропии Алиса—Ева, путем взятия частичного следа:

$$\begin{aligned}
\rho_{XE} =& \text{tr}_Y\rho_{XYE} = \\
=&\frac{1}{2}|0\rangle_X\langle 0| \otimes \Big[\cos^2\alpha|\Phi_0\rangle_E\langle\Phi_0| + \sin^2\alpha|\Theta_0\rangle_E\langle\Theta_0|\Big] \otimes |\xi_0\rangle_{\text{ТНА}}\langle\xi_0| + \\
+&\frac{1}{2}|1\rangle_X\langle 1| \otimes \Big[\cos^2\alpha|\Phi_1\rangle_E\langle\Phi_1| + \sin^2\alpha|\Theta_1\rangle_E\langle\Theta_1|\Big] \otimes |\xi_1\rangle_{\text{ТНА}}\langle\xi_1|,
\end{aligned} \tag{1.75}$$

$$\begin{aligned}
\rho_E = \text{tr}_X\rho_{XE} = &\frac{1}{2}\Big[\cos^2\alpha|\Phi_0\rangle_E\langle\Phi_0| + \sin^2\alpha|\Theta_0\rangle_E\langle\Theta_0|\Big] \otimes |\xi_0\rangle_{\text{ТНА}}\langle\xi_0| + \\
+&\frac{1}{2}\Big[\cos^2\alpha|\Phi_1\rangle_E\langle\Phi_1| + \sin^2\alpha|\Theta_1\rangle_E\langle\Theta_1|\Big] \otimes |\xi_1\rangle_{\text{ТНА}}\langle\xi_1|.
\end{aligned} \tag{1.76}$$

Матрица плотности ρ_{XE} диагональна в записанном базисе, поэтому ее собственные значения равны

$$\lambda_1 = \lambda_2 = \frac{1}{2}\cos^2\alpha, \quad \lambda_3 = \lambda_4 = \frac{1}{2}\sin^2\alpha. \tag{1.77}$$

Далее вычисляется энтропия фон Неймана для матрицы плотности ρ_{XE}:

$$S(\rho_{XE}) = -\sum\lambda_i\log\lambda_i = 1 + h(\sin^2\alpha). \tag{1.78}$$

Полученное выражение совпадает с результатом без побочных каналов (1.52).

Матрица плотности ρ_E не является диагональной в записанном базисе, и для нахождения ее собственных значений решается секулярное уравнение

$$\det(\rho_E - \lambda\cdot I) = 0, \tag{1.79}$$

где I — единичная матрица.

В базисе $\{|\Phi_0\rangle_E \otimes |\xi_0\rangle_{\text{ТНА}}, |\Phi_1\rangle_E \otimes |\xi_1\rangle_{\text{ТНА}}, |\Theta_0\rangle_E \otimes |\xi_0\rangle_{\text{ТНА}}, |\Theta_1\rangle_E \otimes |\xi_1\rangle_{\text{ТНА}}\}$ матрица плотности ρ_E имеет блочный вид:

$$\rho_E = \frac{1}{2}\begin{pmatrix} \cos^2\alpha \cdot B & O \\ O & \sin^2\alpha \cdot B \end{pmatrix}, \tag{1.80}$$

где O — нулевая матрица, а матрица B имеет вид

$$B = \begin{pmatrix} 1+\eta^2\cos^2 2\alpha & 2\eta\cos 2\alpha \\ 2\eta\cos 2\alpha & 1+\eta^2\cos^2 2\alpha \end{pmatrix}, \tag{1.81}$$

где $\eta \equiv \sqrt{\mathcal{F}(|\xi_0\rangle\langle\xi_0|, |\xi_1\rangle\langle\xi_1|)} = \langle\xi_0|\xi_1\rangle$ Выразив едичный оператор в базисе $\{|\Phi_0\rangle_E, |\Phi_1\rangle_E\}$ и $\{|\Theta_0\rangle_E, |\Theta_1\rangle_E\}$, можно записать секулярные уравнения для матрицы B для нахождения ее собственных значений Λ:

$$\det\begin{pmatrix} 1+\eta^2\cos^2 2\alpha - \Lambda & \eta\cos 2\alpha\cdot(2-\Lambda) \\ \eta\cos 2\alpha\cdot(2-\Lambda) & 1+\eta^2\cos^2 2\alpha - \Lambda \end{pmatrix} = 0. \tag{1.82}$$

В результате решения уравнения (1.82) получаются следующие собственные значения:

$$\Lambda = 1 \pm \eta\cos 2\alpha = \begin{cases} 1-\eta\left(1-2\cos^2\alpha\right), \\ 1-\eta\left(1-2\sin^2\alpha\right). \end{cases} \tag{1.83}$$

Тогда, собственные значения матрицы плотности ρ_E выражаются следующим образом:

$$\begin{aligned} \lambda_1 &= \cos^2\alpha\cdot\frac{1-\eta\left(1-2\cos^2\alpha\right)}{2}, \quad \lambda_2 = \cos^2\alpha\cdot\frac{1-\eta\left(1-2\sin^2\alpha\right)}{2}, \\ \lambda_3 &= \sin^2\alpha\cdot\frac{1-\eta\left(1-2\cos^2\alpha\right)}{2}, \quad \lambda_4 = \sin^2\alpha\cdot\frac{1-\eta\left(1-2\sin^2\alpha\right)}{2}. \end{aligned} \tag{1.84}$$

Далее вычисляется энтропия фон Неймана для матрицы плотности ρ_E:

$$S(\rho_E) = -\sum\lambda_i\log\lambda_i = h\left(\frac{1-\eta\left(1-2\sin^2\alpha\right)}{2}\right) + h(\sin^2\alpha). \tag{1.85}$$

Условная энтропия системы Алиса—Ева равна

$$H(X|E) = S(\rho_{XE}) - S(\rho_E) = 1 - h\left(\frac{1-\eta\left(1-2\sin^2\alpha\right)}{2}\right). \tag{1.86}$$

Поскольку вид матрицы плотности ρ_{XY} (1.62) остается без изменений, то сохраняется и физический смысл величины $\sin^2\alpha$ (1.63) — вероятность ошибки в однофотонной компоненте E_1. Достаточное условие секретности (1.21) приобретает следующий вид:

$$\ell \leqslant \Omega_1 \left[1 - h\left(\frac{1-\eta\,(1-2E_1)}{2}\right)\right] - leak - \delta. \tag{1.87}$$

В работах [25; 81] предполагалось использование Евой когерентных состояний при проведении ТНА. Пусть среднее число фотонов в состояниях, приходящих к Еве равно μ_{THA}. Общий вид когерентного состояния со средним числом фотонов μ_{THA} в Фоковском базисе записывается следующим образом:

$$|\sqrt{\mu_{\text{THA}}}e^{i\varphi}\rangle = e^{-\frac{\mu_{\text{THA}}}{2}} \sum_{n=0}^{\infty} \frac{(\sqrt{\mu_{\text{THA}}})^n e^{in\varphi}}{\sqrt{n!}} |n\rangle, \tag{1.88}$$

где φ — фаза когерентного состояния, $|n\rangle$ — Фоковское состояние с числом фотонов n.

Тогда, рассмотрев для определенности протокол BB84 и случай фазового кодирования, будем считать, что Ева пытается различить состояния с разностью фаз π: $|\xi_0\rangle = |\sqrt{\mu_{\text{THA}}}\rangle$ и $|\xi_1\rangle = |-\sqrt{\mu_{\text{THA}}}\rangle$. Скалярное произведение таких состояний зависит только от среднего числа фотонов:

$$\eta = \langle\sqrt{\mu_{\text{THA}}}| - \sqrt{\mu_{\text{THA}}}\rangle = e^{-2\mu_{\text{THA}}}. \tag{1.89}$$

Аналогичные вычисления можно провести и для остальных побочных каналов при использовании модельных соображений для вида состояний нарушителя [25; 81]. Методы экспериментального определения величин, входящих в итоговую формулу относительной длины ключа будут обсуждаться в главе 2. Там же будет представлено расширение результатов на случай использования нарушителем состояний произвольного вида.

1.7.4 Атаки навязывания

Атаки навязывания (известные в англоязычной литературе как атаки «fake-state» или «faked-state») основаны на несовершенствах приемника Боба, позволяющих нарушителю путем внешнего воздействия на этот приемник

вызвать его срабатывание в соответствии с желаемым для него результатом измерения [82]. Общая схема атак навязывания состоит в следующем: Ева проводит измерение квантового состояния, посланного Алисой, в некотором базисе, и, в зависимости от результата измерения, посылает на приемник Боба специально подготовленный оптический сигнал. Исторически, первой атакой навязывания можно назвать атаку «Trojan Pony» [29]. Для ее проведения Еве требовалось послать на приемник Боба оптический сигнал с увеличенным в несколько раз средним числом фотонов. Если состояние сигнала Евы соответствовало базису Боба, то происходило срабатывание одного из детекторов Боба, согласно выбору Евы. Если же базисы Евы и Боба не совпадали, то срабатывали оба детектора. Системы КРК интерпретировали двойные срабатывания как несодержательные, удаляя такие события из дальнейшего рассмотрения. В результате, ключ формировался из тех состояний, которые были достоверно известны Еве. Решением проблемы стала модификация алгоритмов обработки результатов измерений Боба, при которой двойные срабатывания интерпретировались как случайный выбор одного из битов ключа, либо, более консервативно, как ошибочные, давая вклад в QBER.

Позже, были представлены более сложные подходы к атакам навязывания. Глобально, можно выделить две стратегии навязывания:

– навязывание срабатывания выбранного детектора;
– навязывание выбранного состояния.

Первый случай возможен для нарушителя, когда один из детекторов Боба оказывается чувствителен к излучению с некоторыми параметрами, в то время как остальные нет. В качестве данного параметра, в общем случае, могут выступать временны́е, спектральные или пространственные характеристики излучения. Экспериментально демонстрировалась возможность нарушителя осуществить навязывание срабатывание детектора, работающего в стробируемом режиме, в момент времени, когда его квантовая эффективность заметно превышает квантовую эффективность остальных детекторов, путем отправки оптического импульса таким образом, чтобы он пришел на приемную сторону именно в этот момент времени [83; 84].

Для исключения такой возможности навязывания применяется следующее решение: легитимный пользователь выбирает соответствие между детекторами и значениями бит ключа случайным образом, используя для этого генератор случайных чисел и выставляя модулятор на приемной стороне в од-

но из четырех состояний вместо двух для протокола BB84 [85]. В этом случае, даже если нарушитель сможет вызвать срабатывание одного из детекторов, значение бита останется случайным. Отметим, что данная мера фактически делает первую стратегию навязывания несостоятельной, однако требует использования дополнительного ГСЧ, либо повышения скорости работы уже используемого ГСЧ на стороне Боба. Наконец, данные атаки неприменимы к системам КРК, использующим один детектор на приемной стороне.

Вторая стратегия навязывания представляет более значительную опасность для систем КРК. Атаки, использующие эту стратегию, также называются атаками контроля детектора. Они основаны на «сверхлинейной» зависимости вероятности срабатывания ДОФ от энергии подаваемого излучения [86]. Как правило, данная зависимость имеет сигмоидальный вид [87; 88], из-за чего повышение энергии излучения на несколько децибел приводит к росту вероятности срабатывания ДОФ от нуля до единицы. Выделяются 2 атаки, использующие данную особенность: атака с ослеплением ДОФ («Detector Blinding Attack» — DBA) [89], основанная на выведении ДОФ из режима счета фотонов путем подачи на него интенсивного излучения, и атака на спаде строба («After-Gate Attack» — AGA) [90], при которой детектор, работающий в стробируемом режиме, выводится из режима счета фотонов самостоятельно из-за ненулевого времени спада задних фронтов стробов, подаваемых на детектор. Данное поведение детекторов создает условия для нарушителя, при которых событие детектирования состояния на стороне Боба становится зависимым от его выбора базиса. Так, посылая навязывающие импульсы заданной энергии, Ева может добиться срабатывания детектора Боба только в том случае, если выбранный ей базис совпадает с базисом Боба. В протоколе BB84 при реализации с двумя детекторами несовпадение базисов между Евой и Бобом приведет к тому, что на каждый из детекторов Боба придет энергия вдвое меньше изначальной. При правильном подборе параметров, этой энергии окажется недостаточно для регистрации срабатывания при данном режиме работы детекторов. В результате, ключ формируется только из состояний, достоверно известных Еве, при этом наблюдаемые параметры протокола КРК (в частности, QBER) остаются на уровне, характерном для работы без нарушителя.

Как и в случае с первой стратегией навязывания, существуют способы, исключающие саму возможность проведения таких атак. К ним можно отнести протоколы с недоверенными промежуточными узлами Measurement Device

Independent — MDI [91] и Twin Field [92]. Результаты измерений на приемной стороне в данных протоколах оглашаются открыто, и навязывание со стороны Евы не влияет на стойкость вырабатываемых ключей. Однако, техническая реализация данных протоколов на практике оказывается более сложной и дорогостоящей по сравнению с системами на базе протокола BB84 и подобных ему. Для них оказывается возможным обеспечить практическую недостижимость атак на спаде строба путем исключения событий детектирования в моменты спада стробов при постобработке путем использования точных таймеров внутри системы [90]. Такая мера, однако, не обеспечивает защиту от атак с ослеплением. В связи с этим, широко используются технические меры, детектирующие сам факт перевода ДОФ в ослепленный режим (например, мониторинг тока на нагрузочном резисторе в электрической схеме детектора [93]), или сигнализирующие о вводе мощного излучения внутрь системы (например, при использовании сторожевых детекторов). В ряде работ отмечалось, что данные меры не всегда гарантируют детектирование перевода детектора в ослепленный режим, особенно при использовании импульсного ослепляющего излучения с низкой частотой повторения импульсов [94—96]. В связи с этим, были предложены другие методы защиты от атак контроля детектора, включающие в себя «отрицательное квитирование» [97], контроль двойных срабатываний [98], самотестирование [99], рандомизация квантовой эффективности [100] (или затухания [101]), фазово-временно́е кодирование [102] и изотропный протокол КРК [103]. Состоятельность данных методов зачастую является предметом научных дискуссий [104—106]. В связи с этим, особую важность играет проведение сертификационных исследований мер защиты от атак навязывания на реальных системах КРК [95; 96]. В рамках настоящей работы при анализе атак на системы КРК будем предполагать, что меры защиты от атак навязывания обеспечивают надлежащий уровень безопасности, а сеанс выработки ключа при детекторировании попытки атаки будет прерван. В таком случае, учет атак навязывания в выражении достаточного условия секретности (1.21) не требуется.

1.7.5 Изменение параметров внешним воздействием

Использование достаточного условия секретности (1.21) позволяет обеспечить безопасность КРК при соответствии параметров, используемых в формуле, их реальным значениям. В действительности, нарушитель способен воздействовать на аппаратуру системы КРК, изменяя значение данных параметров. Так, например, было показано, что компоненты внутри системы КРК, использующие магнито-оптический эффект Фарадея (например, оптические изоляторы и циркуляторы) могут изменять свои характеристики под воздействием внешнего магнитного поля [107; 108]. Впрочем, данные эффекты наблюдаются лишь при нахождении источника магнитного поля в непосредственной близости к атакуемому компоненту. Корпусирование и размещение системы КРК внутри контролируемой зоны фактически избавляет от данной уязвимости. Иначе обстоят дела с оптическим воздействием на компоненты системы. Было показано, что среднее число фотонов в импульсах, выходящих из передатчика системы КРК может быть увеличено путем введения внешнего излучения через вентиляционные отверстия корпуса передатчика [109]. В то время как данная проблема решается путем изменения геометрии вентиляционных отверстий и размещением передатчика в закрытом помещении, существует альтернативная возможность ввода внешнего излучения внутрь системы, а именно, непосредственно через оптический канал связи. Выделяются следующие атаки[5], использующие данную возможность: 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).

Впервые LDA была рассмотрена в рамках воздействия нарушителя на ДОФ приемника КРК [110]. Было показано, что мощное излучение может

[5]Следует заметить, что данные действия нарушителя не попадают под формальное определение понятия атак на техническую реализацию, принятом в настоящей работе, поскольку само по себе изменение параметров системы не понижает криптографическую стойкость ключей. Для получения информации о выработанной последовательности после изменения параметров Еве необходимо провести некоторую атаку на квантовые состояния или техническую реализацию из описанных выше. В то же время, в литературе устоялось отнесение LDA, LSA и IPA к атакам на техническую реализацию, в связи с чем в тексте настоящей работы данные действия нарушителя также называются атаками.

привести к необратимому изменению свойств ДОФ. В частности, при некоторой мощности излучения (1,5 — 2 Вт) эффективность детектора начинала снижаться. Поскольку эффективность приема (наряду с другими параметрами детекторов) могут использоваться при оценке длины ключа, данное изменение может привести к компрометации сеанса КРК. Это обстоятельство делает предпочтительным измерение характеристик детектора, подверженных изменению, непосредственно во время сеанса КРК, а не заранее.

Ряд последующих работ был сосредоточен на исследовании воздействия мощного лазерного излучения на передатчик КРК. В частности, было продемонстрировано, что под действием мощного лазерного излучения свои свойства меняют постоянные и переменные оптические аттенюаторы (см. рисунок 1.3) [111—113], а также оптические изоляторы [114—116].

Аттенюаторы используются в оптической схеме передатчика КРК для ослабления лазерных импульсов до квазиоднофотонного уровня. При уменьшении степени аттенюации среднее число фотонов в импульсах, выходящих из передатчика, увеличивается (как для информационных состояний, так и для состояний-ловушек в методе «decoy state»). Данное обстоятельство, в частности, приводит к неверным результатам оценки доли однофотонной компоненты Ω_1^L (1.43) при использовании метода «decoy state», что открывает Еве возможности по проведению атак на многофотонную компоненту, описанных в разделе 1.6. Однако, конкретные возможности нарушителя по получению информации при значительном увеличении среднего числа фотонов ранее не исследовались. Подробный анализ данного вопроса будет представлен в главе 3.

Другой функцией оптический аттенюаторов в системах КРК является понижение интенсивности оптических сигналов в побочных каналах утечки информации, а именно, среднего числа фотонов μ_{THA} в состояниях, возвращающихся к Еве при проведении атаки «Trojan Horse» (см. раздел 1.7.3). Такую же функцию выполняют и оптические изоляторы, понижающие интенсивность излучения, распространяющегося в нелегитимном направлении (изоляторы размещаются как на стороне Алисы, так и на стороне Боба, для защиты от THA на модулятор Боба и от атаки «Backflash»). Уменьшение степени аттенюации и степени изоляции в данном случае приведет к недооценке информации, получаемой нарушителем по побочным каналам, согласно формуле (1.87).

В качестве мер защиты от LDA могут использоваться сторожевые детекторы, контролирующие мощность излучения, входящего внутрь системы,

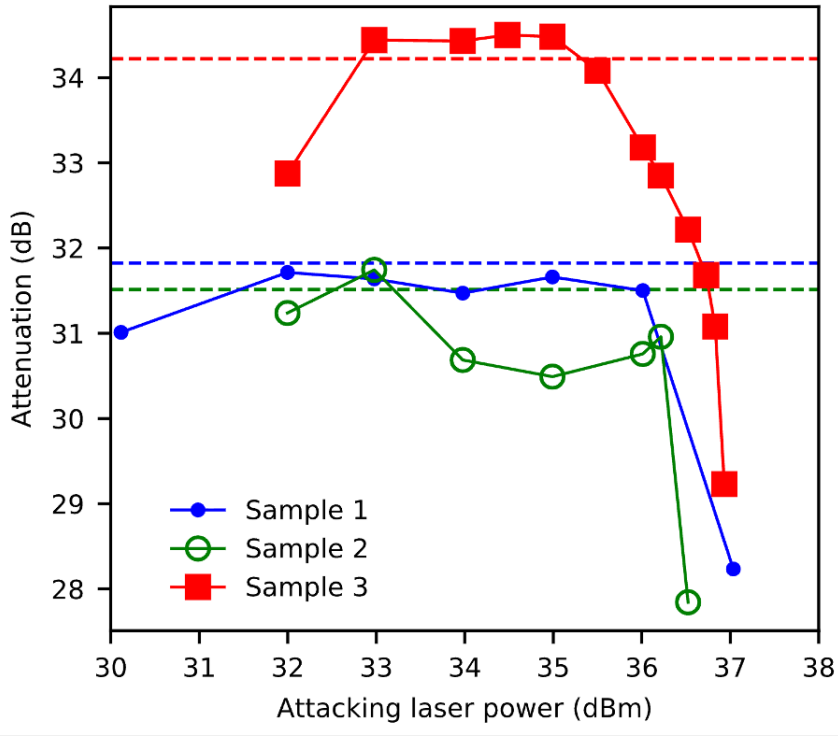


Рисунок 1.3 — Измеренная зависимость степени аттенюации от мощности воздействующего излучения для трех образцов переменных электромеханических аттенюаторов из работы [111]; пунктирными линиями обозначены значения степени аттенюации до приложения излучения

однако надежность такой меры представляется невысокой, в связи с деградацией свойств приемников под действием мощного света [110]. Более надежной мерой представляется включение в схему дополнительного светоделителя на выходе из системы с контрольным фотодетектором, подключенным к его порту. Данный детектор может осуществлять контроль мощности выходного излучения. Работоспособность данной меры, однако, существенно зависит от исправности контрольного фотодетектора и постоянстве коэффициента деления используемого светоделителя (в общем случае, также подверженному воздействию мощного излучения). Более перспективной мерой защиты являются пассивные устройства мониторинга — оптические заглушки, прерывающие оптическую связь при превышении некоторого порога по мощности. В качестве таких устройств были предложены некоторые модели оптических изоляторов [115], оптические волокна с нанесенной на их торец краской для возбуждения эффекта «fiber fuse» (инициации оптического разряда) [117], а также углеродные нанотрубки [118; 119]. Наконец, крайне важно использовать те виды аттенюаторов и изоляторов, которые сохраняют или увеличивают

степень аттенюации/изоляции при приложении мощного излучения. Согласно опубликованным данным, таковыми являются некоторые виды розеткообразных аттенюаторов [113] и нейтральные фильтры [112] при мощностях до 5 Вт на длине волны излучения 1550 нм.

Атаки LSA [120] и IPA [121; 122] также нацелены на увеличение среднего числа фотонов в импульсах, выходящих из передатчика. Их основное отличие от LDA состоит в том, что оптические компоненты, подверженные атаке — лазерный диод и модулятор интенсивности, соответственно, как правило располагаются вдали от выхода из системы передатчика. В связи с этим, мощность излучения, достигающего требуемых компонентов, ниже, чем при LDA, а наблюдаемые эффекты оказываются обратимыми.

Эффект, достигаемый атакой LSA состоит в увеличении мощности лазерных импульсов, генерируемых лазерным диодом при инжектировании внешнего затравочного излучения. При этом лазер, фактически, начинает работать как усилитель. Увеличение мощности лазерных импульсов при введении внешнего излучения внутрь лазерного диода экспериментально наблюдалось и при значительной отстройке от длины волны генерации в работах [123; 124] (увеличение мощности излучения на 1550 нм при введении внешнего излучения на 1310 нм). Как утверждается авторами, данное явление связано с оптической накачкой активной среды лазера.

Атака IPA, в свою, очередь направлена на фазовый модулятор, входящий в состав модулятора интенсивности или переменного аттенюатора. Под действием внешнего видимого или ультрафиолетового излучения, структура входящая в состав фазового модулятора меняет показатель преломления, что эффективно приводит к сдвигу полуволнового напряжения модулятора и, как следствие, неправильному значению интенсивностей импульсов, приготавливаемых с использованием модулятора интенсивности. Было показано, что переменный аттенюатор на базе интерферометра Маха—Цандера и фазового модулятора уменьшает степень аттенюации на величины до 25 дБ [121] при подсветке видимым излучением с мощностями в диапазоне от десятков нВт до десятков мкВт. В свою очередь, в работе [122], напротив, наблюдалось обратимое увеличение потерь на модуляторе интенсивности. Авторы рассмотрели возможность Евы использовать данную особенность на этапе калибровке модулятора, увеличивая потери на модуляторе, а по завершении калибровки переводя его в изначальное состояние, что приведет к росту среднего числа фотонов импульсов Алисы.

Относительно низкие мощности излучения, требуемые для проведения LSA и IPA усложняют их детектирование. В то же время, распространенное расположение оптических элементов, подверженных данным атакам, в оптической схеме передатчика — а именно, наличие дополнительных оптических элементов в схеме после них — позволяет использовать в качестве меры защиты мониторинг мощности излучения Алисы. Часто, лазерные диодные модули уже оснащены встроенным оптическим измерителем мощности, позволяющим точно определять мощность излучения, выходящего непосредственно из лазерного диода. При повышении мощности (спонтанной или обусловленной проведением LSA) необходимо прервать сеанс КРК и осуществить перекалибровку. Измеритель мощности также может быть размещен после модуляторов интенсивности и переменных аттенюаторов, выполняя ту же функцию, с учетом возможности проведения IPA. Наконец, пассивные элементы защиты, используемые для подавления побочных сигналов (оптические изоляторы, аттенюаторы, фильтры и др.), также подавляют мощность излучения Евы, заводимого ей внутрь передатчика для проведения LSA и IPA. Подавление мощности излучения Евы до величин ниже тех, при которых наблюдаются описанные эффекты, также может служить мерой защиты от описанных атак.

Другим вариантом проведения LSA является стратегия, в основе которой лежит явление оптического захвата частоты [125; 126]. При штатной работе в отсутствие внешнего излучения, лазерные диоды в системах КРК, как правило, работают в режиме переключения усиления, что приводит к началу лазерной генерации заново при каждой следующей подаче импульсов тока накачки, что обеспечивает случайность и равномерность начальной фазы генерируемых оптических импульсов. При введении Евой внешнего затравочного излучения внутрь лазера, выходящий из него свет оказывается когерентен затравочному. Управляя фазой затравочного излучения, Ева может выбирать общую фазу приготавливаемых Алисой импульсов. Это нарушает предположение о случайности и равномерности фазы, отмеченное в разделе 1.4, необходимое для корректной работы метода «decoy state». Известно [127], что в отсутствие данного допущения оказывается возможным проведение USD-атак, приводящих к различению информационных состояний от состояний-ловушек, что открывает возможность Еве подделать статистику детектирования для метода «decoy state» и незаметно провести атаки на многофотонную компоненту из раздела 1.6. Особенностью такой стратегии LSA является отсутствие наблюдаемых

признаков, по которым можно сделать вывод о проведении атаки, поскольку случайность фазы может быть сымитирована Евой, а роста мощности импульсов не происходит. Также, согласно опубликованным данным, эффекты, связанные с навязыванием фазы наблюдаются при мощностях затравочного излучения, меньших примерно на 2 порядка, по сравнению с эффектами роста мощности (1 нВт в работе [126] по сравнению со 100 нВт в работе [120]). Данное обстоятельство ужесточает требования к уровню аттенюации, которая должна быть наложена на свет, распространяющийся по схеме передатчика в нелегитимном направлении для исключения возможности проведения атаки.

Возможность исключения рисков, связанных с проведением атак, изменяющих свойства системы, позволяет обеспечить секретность КРК без изменения достаточного условия секретности (1.21). В то же время, проверка работоспособности мер защиты, обеспечивающих данную возможность, является важной задачей при разработке и сертификации систем КРК. Особую важность данных проверок подчеркивает тот факт, что при недетектируемом проведении атаки (например, просветлении аттенюатора посредством LDA) нарушителю будет доступен весь секретный ключ. Данное утверждение может показаться излишне консервативным, поскольку атаки на многофотонную компоненту, позволяющие нарушителю получить весь ключ, на сегодняшний день считаются неосуществимыми на практике [41]. Однако оказывается, что при определенных условиях возможно построить атаки на многофотонную компоненту, позволяющие Еве получить весь ключ при повышении среднего числа фотонов в импульсах Алисы до некоторого уровня, полностью осуществимые с использованием сегодняшних технологий. Данный вопрос будет подробно рассмотрен в главе 3.

1.8 Комбинированные атаки

В настоящий момент в литературе отсутствует общепринятое определение понятия комбинированных атак на системы КРК. Чаще всего под ними понимается одновременное проведение нескольких различных атак. В настоящей работе предлагается использовать более конкретное определение данного понятия — 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. Такая формулировка определения приводит к вопросу: если система КРК защищена от атаки А и атаки Б в отдельности, можно ли считать систему защищенной от комбинированного проведения атак А и Б? Как следует из приведенного выше обзора атак, ответ — нет. Например, как видно из формулы (1.87), достаточное условие секретности при наличии побочных каналов может быть сформулировано лишь при рассмотрении комбинирования коллективной атаки с атаками по побочным каналам, поскольку условная энтропия системы Алиса— Ева (1.86) не является аддитивной величиной. Из этих же соображений, следует рассматривать комбинированные атаки по всем побочным каналам одновременно.

Возникает вопрос: какие атаки имеет смысл комбинировать? Ответ можно получить при рассмотрении итоговой формулы для относительной длины секретного ключа (1.87). В состав выражения входят параметры, обеспечивающие учет коллективных атак, атак на многофотонную компоненту, а также атак по побочным каналам. Как видно из структуры формулы, соответствующие члены входят в выражение для длины ключа неаддитивно, т.е. достаточное условие секретности выполняется лишь при комбинированном рассмотрении данных атак. Атаки навязывания, рассмотренные в разделе 1.7.4, в отсутствие должных мер защиты позволяют нарушителю получить весь ключ без прибегания к комбинированию с другими атаками. Предложенные на сегодняшний день меры защиты от навязывания призваны сделать данные атаки неосуществимыми, благодаря использованию вспомогательных средств. С учетом этого, комбинирование атак навязывания с другими имеет смысл лишь в том случае, если эти другие атаки позволяют свести используемые меры защиты на нет, тем самым нарушив предположение о гарантированном детектировании навязывания. Так, например, в работе [128] рассмотрено комбинировании атак с несовпадением эффективностей детекторов и атаки «Trojan Horse» против системы, использующей 4 состояния фазового модулятора на приемной стороне. Зондирование фазового модулятора Боба позволяла Еве получить информация о выборе его состояния, что нарушало работоспособность меры защиты с рандомизацией соответствия бита детектору, и дало нарушителю возможность провести атаку на детекторы Боба.

Последний рассмотренный класс атак — атаки с изменением свойств системы. Как было отмечено, данный класс не попадает под формальное определение понятия атак, поэтому не подходит для построения комбинированных атак по нашему определению. Тем не менее, данные действия нарушителя увеличивают его шансы на успех при проведении атак на многофотонную компоненту (при увеличении среднего числа фотонов или дерандомизации фазы излучения), при проведении атак по побочным каналам (при увеличении интенсивности побочных сигналов), а также при проведении атак навязывания (при выводе из строя сторожевых детекторов или изменении свойств однофотонных детекторов).

Из сказанного выше следует, 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. Основная часть настоящей работы, изложенная в главах 2 и 3, посвящена экспериментальному и теоретическому проведению такого анализа.

Глава 2. Анализ побочных каналов утечки информации в системах КРК

2.1 Достаточное условие секретности при наличии побочных каналов утечки информации

В разделе 1.7.3 было приведено выражение (1.87) для достаточного условия секретности при наличии побочного канала утечки информации на примере атаки «Trojan Horse». Для вывода формулы (1.87) было сделано допущение об использовании Евой чистых состояний. Данное допущение согласуется с интуитивным представлением о чистых состояниях как о несущих большее количество информации, чем смешанные. В то же время, строго математически правомерность такого допущения не была доказана в литературе. С другой стороны, квантовые состояния в побочных каналах, связанных с переизлучением ДОФ и атакой «Backflash», вообще не зависят от действий Евы и определяются лишь физическими процессами, приводящими к образованию переизлученного света, т.е. явлением электролюминисценции. Как известно, полученный в результате люминисценции свет некогерентен и, в общем случае, находится в смешанном состоянии.

Следующим допущением в описанных выше работах являлось использование модельных соображений для выражения явной связи между параметром η — корнем из фиделити между двумя состояниями в побочном канале, отвечающим разным битам, и интенсивностью излучения в побочном канале — средним числом фотонов μ_{THA}. В рамках модели предполагалось, что Ева использует когерентные состояния (1.88). Опять же, данное утверждение является необоснованным при рассмотрении THA.

В связи с этим возникает вопрос: можно ли получить достаточное условие секретности, отказавшись от модельных соображений о виде состояний, доходящих до нарушителя? Как будет показано в настоящем разделе, ответ на этот вопрос положительный. Как оказалось, рассматривая квантовые состояния в побочных каналах самого общего вида, можно получить выражение для относительной длины ключа в условиях проведения нарушителем комбинации из коллективной атаки и атак по побочным каналам. При этом для парамет-

ризации побочных каналов достаточно лишь интенсивности их сигналов, что является экспериментально измеримой величиной.

Проведем рассмотрение данного вопроса на примере атаки «Trojan Horse».

2.1.1 Вычисление условной энтропии системы Алиса—Ева с учетом смешанных состояний в побочном канале

Откажемся от допущения об использовании Евой чистых состояний. Тогда, в выражениях (1.72) и (1.73) вектора состояний $|\xi_0\rangle_{\text{THA}}$ и $|\xi_1\rangle_{\text{THA}}$ нужно заменить на матрицы плотности ρ^0_{THA} и ρ^1_{THA}:

$$U_{BE}|0\rangle_B \otimes |E\rangle_E \otimes |\xi_0\rangle_{\text{THA}} \longrightarrow U_{BE}\Big[|0\rangle_B \otimes |E\rangle_E\Big] \otimes \rho^0_{\text{THA}} \tag{2.1}$$

$$U_{BE}|1\rangle_B \otimes |E\rangle_E \otimes |\xi_1\rangle_{\text{THA}} \longrightarrow U_{BE}\Big[|1\rangle_B \otimes |E\rangle_E\Big] \otimes \rho^1_{\text{THA}}. \tag{2.2}$$

Тогда, матрица плотности Алиса—Боб—Ева обретет вид

$$\begin{aligned}\rho_{XYE} = \frac{1}{2}|0\rangle_X\langle 0| \otimes \Big[&\cos^2\alpha|0\rangle_Y\langle 0| \otimes |\Phi_0\rangle_E\langle\Phi_0| + \\ &+ \sin^2\alpha|1\rangle_Y\langle 1| \otimes |\Theta_0\rangle_E\langle\Theta_0|\Big] \otimes \rho^0_{\text{THA}} + \\ +\frac{1}{2}|1\rangle_X\langle 1| \otimes \Big[&\cos^2\alpha|1\rangle_Y\langle 1| \otimes |\Phi_1\rangle_E\langle\Phi_1| + \\ &+ \sin^2\alpha|0\rangle_Y\langle 0| \otimes |\Theta_1\rangle_E\langle\Theta_1|\Big] \otimes \rho^1_{\text{THA}}.\end{aligned} \tag{2.3}$$

Матрицы плотности для подсистем примут следующий вид:

$$\begin{aligned}\rho_{XE} =& \text{tr}_Y\rho_{XYE} = \\ =&\frac{1}{2}|0\rangle_X\langle 0| \otimes \Big[\cos^2\alpha|\Phi_0\rangle_E\langle\Phi_0| + \sin^2\alpha|\Theta_0\rangle_E\langle\Theta_0|\Big] \otimes \rho^0_{\text{THA}} + \\ +&\frac{1}{2}|1\rangle_X\langle 1| \otimes \Big[\cos^2\alpha|\Phi_1\rangle_E\langle\Phi_1| + \sin^2\alpha|\Theta_1\rangle_E\langle\Theta_1|\Big] \otimes \rho^1_{\text{THA}} \equiv \\ \equiv&\frac{1}{2}|0\rangle_X\langle 0| \otimes \rho^0_Q \otimes \rho^0_{\text{THA}} + \frac{1}{2}|1\rangle_X\langle 1| \otimes \rho^1_Q \otimes \rho^1_{\text{THA}} \equiv \\ \equiv&\frac{1}{2}|0\rangle_X\langle 0| \otimes \rho^0_E + \frac{1}{2}|1\rangle_X\langle 1| \otimes \rho^1_E,\end{aligned} \tag{2.4}$$

$$\begin{aligned}\rho_E = \mathrm{tr}_X \rho_{XE} = \frac{1}{2}\Big[\cos^2\alpha|\Phi_0\rangle_E\langle\Phi_0| + \sin^2\alpha|\Theta_0\rangle_E\langle\Theta_0|\Big] \otimes \rho^0_{\text{ТНА}} + \\ + \frac{1}{2}\Big[\cos^2\alpha|\Phi_1\rangle_E\langle\Phi_1| + \sin^2\alpha|\Theta_1\rangle_E\langle\Theta_1|\Big] \otimes \rho^1_{\text{ТНА}} \equiv \\ \equiv \frac{1}{2}\rho^0_Q \otimes \rho^0_{\text{ТНА}} + \frac{1}{2}\rho^1_Q \otimes \rho^1_{\text{ТНА}} \equiv \frac{1}{2}\rho^0_E + \frac{1}{2}\rho^1_E,\end{aligned} \tag{2.5}$$

где мы ввели обозначение ρ^0_Q и ρ^1_Q для состояний вспомогательной квантовой системы Евы, ассоциированных с нулевым и единичным битом, а также ρ^0_E и ρ^1_E для состояний полной квантовой системы Евы для соответствующих бит.

Прямое вычисление энтропий для таких состояний представляется сложной задачей, особенно с учетом того, что система Евы может быть бесконечномерной. Тем не менее, вычисление можно упростить, воспользовавшись фундаментальным результатом, полученным в работах А. С. Холево [129—131]. Оказывается, что условная энтропия для квантовых состояний вида (2.4) (такие состояния называют квантово-классическими) может быть выражена следующим образом:

$$H(X|E) = 1 - \chi_E, \tag{2.6}$$

где χ_E — величина Холево для квантового ансамбля Евы

$$\chi_E \equiv S(\rho_E) - \frac{1}{2}S(\rho^0_E) - \frac{1}{2}S(\rho^1_E). \tag{2.7}$$

Прямое вычисление величины Холево все еще требует нахождения собственных значений матриц плотности ρ^0_E и ρ^1_E. Однако задачу можно значительно упростить, воспользовавшись теоремой из работы [132], гласящей, что для квантового ансамбля, равновероятно находящемся в одном из состояний ρ^0_E и ρ^1_E, величина Холево может быть ограничена сверху, причем верхняя граница задается величиной $\overline{\chi}_E$:

$$\chi_E \leqslant \overline{\chi}_E \equiv h\left(\frac{1-\sqrt{\mathcal{F}}}{2}\right) \equiv -\frac{1+\sqrt{\mathcal{F}}}{2}\log\frac{1+\sqrt{\mathcal{F}}}{2} - \frac{1-\sqrt{\mathcal{F}}}{2}\log\frac{1-\sqrt{\mathcal{F}}}{2}, \tag{2.8}$$

где $\mathcal{F} \equiv \mathcal{F}\left(\rho^0_E, \rho^1_E\right)$ — фиделити Ульмана, определяемое формулой (1.70).

Важным результатом является тот факт, что величина Холево и, как следствие, условная энтропия системы Алиса—Ева может быть ограничена величиной, зависящей лишь от фиделити — степени перекрытия состояний Евы. Найдем явный вид данной величины.

Фиделити обладает свойством мультипликативности [133], т.е.

$$\mathcal{F}\left(\rho_Q^0 \otimes \rho_{\text{THA}}^0,\, \rho_Q^1 \otimes \rho_{\text{THA}}^1\right) = \mathcal{F}\left(\rho_Q^0,\, \rho_Q^1\right) \cdot \mathcal{F}\left(\rho_{\text{THA}}^0,\, \rho_{\text{THA}}^1\right). \tag{2.9}$$

Следовательно, можно вычислять отдельно фиделити для каждой подсистемы Евы, а затем перемножить результаты.

Для вспомогательной подсистемы Евы, связанной с проведением коллективной атаки, воспользуемся эквивалентным определением фиделити Ульмана [134]:

$$\mathcal{F}\left(\rho_Q^0,\, \rho_Q^1\right) = \left(\operatorname{tr}\sqrt{\rho_Q^0 \rho_Q^1}\right)^2. \tag{2.10}$$

Вычислим произведение матриц плотности

$$\begin{aligned}\rho_Q^0 \rho_Q^1 =& \left[\cos^2\alpha|\Phi_0\rangle\langle\Phi_0| + \sin^2\alpha|\Theta_0\rangle\langle\Theta_0|\right] \cdot \left[\cos^2\alpha|\Phi_1\rangle\langle\Phi_1| + \sin^2\alpha|\Theta_1\rangle\langle\Theta_1|\right] = \\ =& \cos 2\alpha\, \cos^4\alpha|\Phi_0\rangle\langle\Phi_1| + \cos 2\alpha\, \sin^4\alpha|\Theta_0\rangle\langle\Theta_1|. \end{aligned} \tag{2.11}$$

Нетрудно видеть, что $|\Phi_0\rangle$ и $|\Theta_0\rangle$ являются собственными векторами полученной матрицы:

$$\rho_Q^0 \rho_Q^1 |\Phi_0\rangle = \cos 2\alpha\, \sin^4\alpha|\Phi_0\rangle\langle\Phi_1|\Phi_0\rangle = \cos^2 2\alpha\, \sin^4\alpha|\Phi_0\rangle, \tag{2.12}$$

$$\rho_Q^0 \rho_Q^1 |\Theta_0\rangle = \cos 2\alpha\, \cos^4\alpha|\Theta_0\rangle\langle\Theta_1|\Theta_0\rangle = \cos^2 2\alpha\, \sin^4\alpha|\Theta_0\rangle. \tag{2.13}$$

Полученные собственные значения равны $\cos^2 2\alpha \sin^4\alpha$ и $\cos^2 2\alpha \sin^4\alpha$. След квадратного корня из матрицы $\rho_Q^0 \rho_Q^1$ равен сумме корней собственных значений (берутся неотрицательные значения корней, поскольку в определении фиделити используется положительно-определенный квадратный корень):

$$\sqrt{\mathcal{F}\left(\rho_Q^0,\, \rho_Q^1\right)} = \operatorname{tr}\sqrt{\rho_Q^0 \rho_Q^1} = \cos 2\alpha\, \cos^2\alpha + \cos 2\alpha\, \sin^2\alpha = \cos 2\alpha. \tag{2.14}$$

Данный результат полностью согласуется с формулой (1.60) в отсутствие побочных каналов:

$$H(X|E) = 1 - \chi_E = 1 - h\left(\frac{1-\cos 2\alpha}{2}\right) = 1 - h(\sin^2\alpha) = 1 - h(E_1). \tag{2.15}$$

При наличии побочных каналов (в рассматриваемом случае, побочного канала THA) условная энтропия системы Алиса—Ева обретает вид

$$H(X|E) \geqslant 1 - \overline{\chi}_E = 1 - h\left(\frac{1-\eta\cdot\cos 2\alpha}{2}\right) = 1 - h\left(\frac{1-\eta\,(1-2E_1)}{2}\right), \tag{2.16}$$

где $\eta \equiv \sqrt{\mathcal{F}\left(\rho_{\text{THA}}^0, \rho_{\text{THA}}^1\right)}$. Видно, что формула (2.16) имеет точно такой же вид, как (1.86), с переопределением степени перекрытия квантовых состояний в побочном канале η (корнем из фиделити) для случая смешанных состояний. При использовании Евой чистых состояний ρ_{THA}^0 и ρ_{THA}^1 формулы (2.16) и (1.86) эквивалентны.

2.1.2 Оценка степени перекрытия состояний в побочном канале

Выражение (2.16) содержит величину η, зависящую от вида состояний, используемых нарушителем. Для точного определения данной величины необходимы модельные соображения, устанавливающие вид матриц плотности ρ_{THA}^0 и ρ_{THA}^1 (например, допущение об использовании когерентных состояний со средним числом фотонов μ_{Eve} в разделе 1.7.3). Однако, для выполнения достаточного условия секретности (1.21) точное значение условной энтропии системы Алиса—Ева не требуется. В качестве консервативной оценки данной величины можно использовать некоторую границу, зависящую от измеримых параметров побочных каналов. Найдем эту границу.

Нехватка информации Евы, а также определяющая ее степень различимости квантовых состояний, физически обусловлена принципиальным наличием вакуумной компоненты в любом достаточно слабом по интенсивности состоянии света. Вклад вакуумной компоненты определяется ее вероятностью p_0 для заданного состояния со средним числом μ, которые связаны соотношением

$$\mu = \sum_{n=0}^{\infty} p_n n = \sum_{n=1}^{\infty} p_n n \geqslant \sum_{n=1}^{\infty} p_n = 1 - p_0, \tag{2.17}$$

где p_n — вероятность n-фотонной компоненты в заданном квантовом состоянии. Отсюда получается выражение для нижней границы вероятности вакуумной компоненты (применимой для кодировки как по поляризации, так и по фазе):

$$p_0 \geqslant 1 - \mu. \tag{2.18}$$

Данное выражение имеет смысл только для $\mu < 1$, что и относится к нашему случаю при использовании пассивных мер защиты, подавляющих интенсивность излучения в побочных каналах.

Связь между вероятностью вакуумной компоненты p_0 и перекрытием состояний Евы η зависит от используемого способа кодирования. Рассмотрим наиболее распространенные случаи кодирования квантовых состояний в квантовой криптографии, а именно по поляризации и по фазе.

При использовании поляризационного кодирования в протоколе BB84, Еве требуется различить два ортогонально поляризованных состояния (для определенности выберем прямой базис, в котором используется горизонтальная и вертикальная поляризация света; для сопряженного базиса результат идентичен). Матрицы плотности этих состояний в общем случае имеют вид:

$$\rho^{\mathrm{H}} = \sum_{m,n=0}^{\infty} \rho^{\mathrm{H}}_{mn} |m\rangle_{\mathrm{H}}\langle n| \otimes |0\rangle_{\mathrm{V}}\langle 0|, \tag{2.19}$$

$$\rho^{\mathrm{V}} = \sum_{m,n=0}^{\infty} \rho^{\mathrm{V}}_{mn} |0\rangle_{\mathrm{H}}\langle 0| \otimes |m\rangle_{\mathrm{V}}\langle n|, \tag{2.20}$$

где ρ^{H} и ρ^{V} — состояния отвечающие горизонтальной и вертикальной поляризации, соответственно, $|k\rangle_{\mathrm{H(V)}}$ — Фоковские состояния с числом фотонов k в горизонтально (вертикально) поляризованной моде.

Удобно воспользоваться следующим неравенством для фиделити Ульмана [135]:

$$\mathcal{F}(\rho, \sigma) \equiv \left(\mathrm{tr}\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}} \right)^2 \geqslant \mathrm{tr}(\rho\sigma) \tag{2.21}$$

для любых матриц плотности ρ и σ.

Вычислим произведение $\rho^{\mathrm{H}}\rho^{\mathrm{V}}$:

$$\rho^{\mathrm{H}}\rho^{\mathrm{V}} = \sum_{m,n=0}^{\infty} \rho^{\mathrm{H}}_{m0}\, \rho^{\mathrm{V}}_{0n} |m\rangle_{\mathrm{H}}\langle 0| \otimes |0\rangle_{\mathrm{V}}\langle n|. \tag{2.22}$$

Тогда, вычисляя след, получаем:

$$tr\left(\rho^{\mathrm{H}}\rho^{\mathrm{V}}\right) = \sum_{i,j=0}^{\infty} \langle ij|\rho^{\mathrm{H}}\rho^{\mathrm{V}}|ij\rangle = \sum_{m,n,i,j=0}^{\infty} \rho^{\mathrm{H}}_{m0}\rho^{\mathrm{V}}_{0n}\langle i|m\rangle\langle 0|i\rangle\langle j|0\rangle\langle n|j\rangle = \rho^{\mathrm{H}}_{00}\rho^{\mathrm{V}}_{00} = p_0^2, \tag{2.23}$$

где $|ij\rangle \equiv |i\rangle_{\mathrm{H}} \otimes |j\rangle_{\mathrm{V}}$. Здесь мы положили вероятности вакуумной компоненты равными для двух состояний. И хотя в общем случае это может быть не так из-за поляризационно-зависимых потерь, выражение (2.23) может давать

консервативную оценку, если в качестве p_0 используется наименьшая из вероятностей вакуумной компоненты для двух состояний.

В итоге, мы получаем связь между фиделити и вероятностью вакуумной компоненты

$$\mathcal{F}\left(\rho^{\mathrm{H}}, \rho^{\mathrm{V}}\right) \geqslant p_0^2. \tag{2.24}$$

Окончательно, получаем неравенство для степени перекрытия состояний в побочном канале:

$$\eta \geqslant p_0 \geqslant 1 - \mu_{\mathrm{THA}}. \tag{2.25}$$

Достижима ли данная граница? При непосредственной проверке можно убедиться, что граница достигается при использовании чистых состояний следующего вида:

$$|\xi_{\mathrm{H}}\rangle = \sqrt{1-\mu_{\mathrm{THA}}}|\mathrm{vac}\rangle + \sqrt{\mu_{\mathrm{THA}}}|10\rangle, \tag{2.26}$$

$$|\xi_{\mathrm{V}}\rangle = \sqrt{1-\mu_{\mathrm{THA}}}|\mathrm{vac}\rangle + \sqrt{\mu_{\mathrm{THA}}}|01\rangle, \tag{2.27}$$

где $|\mathrm{vac}\rangle$ — вакуумное состояние.

Сравним полученный результат со случаем когерентных состояний, обычно рассматриваемом в литературе, т.е. состояний вида $|\alpha\rangle_{\mathrm{H}} \otimes |0\rangle_{\mathrm{V}}$ и $|0\rangle_{\mathrm{H}} \otimes |\alpha\rangle_{\mathrm{V}}$:

$$\eta = \langle\alpha|0\rangle\langle 0|\alpha\rangle = e^{-|\alpha|^2} = e^{-\mu_{\mathrm{THA}}} \tag{2.28}$$

Полученные зависимости удобно изобразить на графике (рисунок 2.1). При малых значениях μ_{Eve} границы асимптотически совпадают. Однако при приближении среднего числа фотонов к единице, границы начинают значительно отличаться. Данный факт подчеркивает важность использования консервативной границы (2.25) для чистых и смешанных состояний общего вида, в случае если в системе КРК не удается значительно подавить интенсивность излучения в побочном канале. Для атаки «Trojan Horse» такое может наблюдаться, например, в двухпроходных системах, содержащих в своем составе зеркала и не использующих оптические изоляторы [136].

Теперь рассмотрим случай фазового кодирования в протоколе BB84. Будем считать, что модуляция фазы состояний Евы приводит к тому, что каждая Фоковская компонента $|k\rangle$ получает набег фазы φ_k, в то время как модуль ее

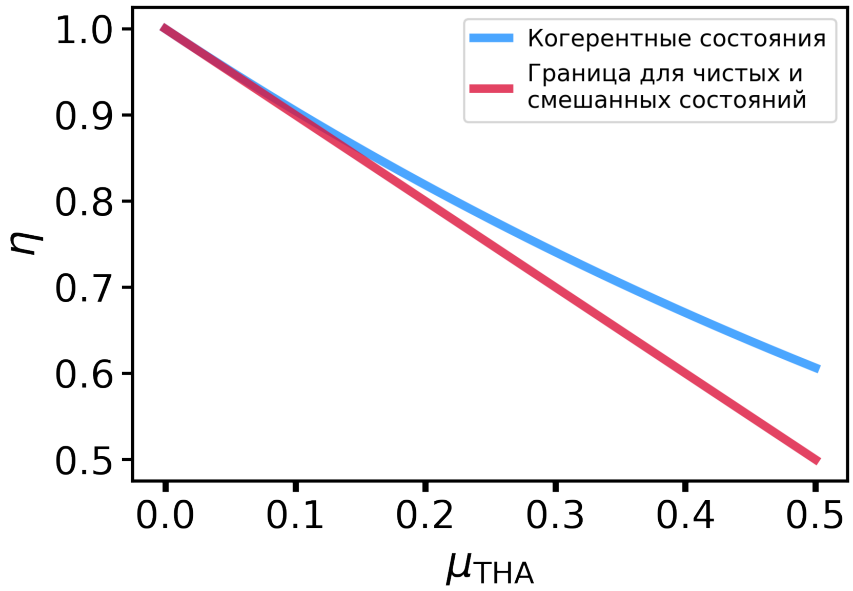


Рисунок 2.1 — Зависимость степени перекрытия квантовых состояний в побочном канале η от среднего числа фотонов μ_{THA} в этих состояниях

амплитуды вероятности сохраняется. Тогда, Еве необходимо провести различение между двумя состояниями в побочном канале, прошедших через фазовый модулятор:

$$\rho^0 = \sum_{m,n=0}^{\infty} \rho_{mn} |m\rangle\langle n|, \tag{2.29}$$

$$\rho^1 = \sum_{m,n=0}^{\infty} \rho_{mn} e^{i(\varphi_m - \varphi_n)} |m\rangle\langle n| = \sum_{m,n=0}^{\infty} \rho_{mn} e^{i\Delta\varphi_{mn}} |m\rangle\langle n|, \tag{2.30}$$

где $\Delta\varphi_{mn} \equiv \varphi_m - \varphi_n$.

Для вычисления степени перекрытия воспользуется определением фиделити Ульмана (1.70). Выразим матрицы плотности (2.29) и (2.30) как произведение их квадратных корней. Пусть σ^0 и σ^1 — квадратные корни ρ^0 и ρ^1, соответственно. Тогда:

$$\rho^0 = \sigma^0 \times \sigma^0 = \sum_{m,n=0}^{\infty} \sum_{k=0}^{\infty} \left(\sigma^0_{mk} \cdot \sigma^0_{kn}\right) |m\rangle\langle n|, \tag{2.31}$$

$$\rho^1 = \sigma^1 \times \sigma^1 = \sum_{m,n=0}^{\infty} \sum_{k=0}^{\infty} \left(\sigma^1_{mk} \cdot \sigma^1_{kn}\right) |m\rangle\langle n|, \tag{2.32}$$

С другой стороны,

$$\rho^1 = \sum_{m,n=0}^{\infty} \sum_{k=0}^{\infty} \left(\sigma^0_{mk} \cdot \sigma^0_{kn}\right) e^{i\Delta\varphi_{mn}} |m\rangle\langle n|. \tag{2.33}$$

Выразим $\Delta\varphi_{mn} = \varphi_m - \varphi_k + \varphi_k - \varphi_n = \Delta\varphi_{mk} + \Delta\varphi_{kn}$ и получим

$$\rho^1 = \sum_{m,n=0}^{\infty} \sum_{k=0}^{\infty} \left(\sigma^0_{mk} e^{i\Delta\varphi_{mk}} \cdot \sigma^0_{kn} e^{i\Delta\varphi_{kn}}\right) |m\rangle\langle n|. \tag{2.34}$$

Сравнивая выражения (2.33) и (2.34), можно получить связь между матрицами σ^0 и σ^1:

$$\sigma^1_{mn} = \sigma^0_{mn} \cdot e^{i\Delta\varphi_{mn}}. \tag{2.35}$$

Подставляя данные величины в определение фиделити, получим:

$$\begin{aligned}\eta =& \sqrt{\mathcal{F}(\rho^0, \rho^1)} = \mathrm{tr}\sqrt{\sqrt{\rho^1}\rho^0\sqrt{\rho^1}} = \mathrm{tr}\sqrt{\sigma^1\sigma^0\sigma^0\sigma^1} = \mathrm{tr}\sqrt{\left(\sigma^1\sigma^0\right)\left(\sigma^1\sigma^0\right)^\dagger} = \\ =& \mathrm{tr}\left(\sigma^1\sigma^0\right) = \mathrm{tr}\left(\sum_{m,n=0}^{\infty}\sum_{k=0}^{\infty}\left(\sigma^0_{mk}e^{i\Delta\varphi_{mk}}\cdot\sigma^0_{kn}\right)|m\rangle\langle n|\right) = \sum_{m,k=0}^{\infty}\sigma^0_{mk}\sigma^0_{mk}e^{i\Delta\varphi_{mk}}.\end{aligned} \tag{2.36}$$

Учитывая, что $(\sigma^0_{00})^2 = p_0$, получим финальное выражение для степени различимости квантовых состояний Евы, закодированных по фазе:

$$\begin{aligned}\eta =& p_0 + \sum_{(m,k)\neq(0,0)}^{\infty}\sigma^0_{mk}\sigma^0_{mk}e^{i\Delta\varphi_{mk}} \geqslant p_0 - \sum_{(m,k)\neq(0,0)}^{\infty}\sigma^0_{mk}\sigma^0_{mk} = \\ =& 1 - (1 - p_0) = 2p_0 - 1 \geqslant 1 - 2\mu_{\text{THA}}.\end{aligned} \tag{2.37}$$

Аналогично случаю поляризационного кодирования, данная граница достигается на чистых состояниях следующего вида:

$$|\xi_0\rangle = \sqrt{1-\mu_{\text{THA}}}|\text{vac}\rangle + \sqrt{\mu_{\text{THA}}}|1\rangle, \tag{2.38}$$

$$|\xi_1\rangle = \sqrt{1-\mu_{\text{THA}}}|\text{vac}\rangle - \sqrt{\mu_{\text{THA}}}|1\rangle. \tag{2.39}$$

Сравним полученный результат со случаем когерентных состояний, т.е. состояний вида $|\alpha\rangle$ и $|-\alpha\rangle$. Для них степень различимости дается выражением (1.89): $\eta = e^{-2\mu_{\text{THA}}}$. Сравнение данной зависимости с полученной границей для η изображено на рисунке 2.2. Как и в случае поляризационного кодирования, кривые асимптотически совпадают при малых μ_{THA}, однако значительно различаются при стремлении к $\mu_{\text{THA}} = 0{,}5$.

Примечательно, что структура выражений (2.25) и (2.37), определяющих границы степени различимости для состояний, закодированных по поляризации

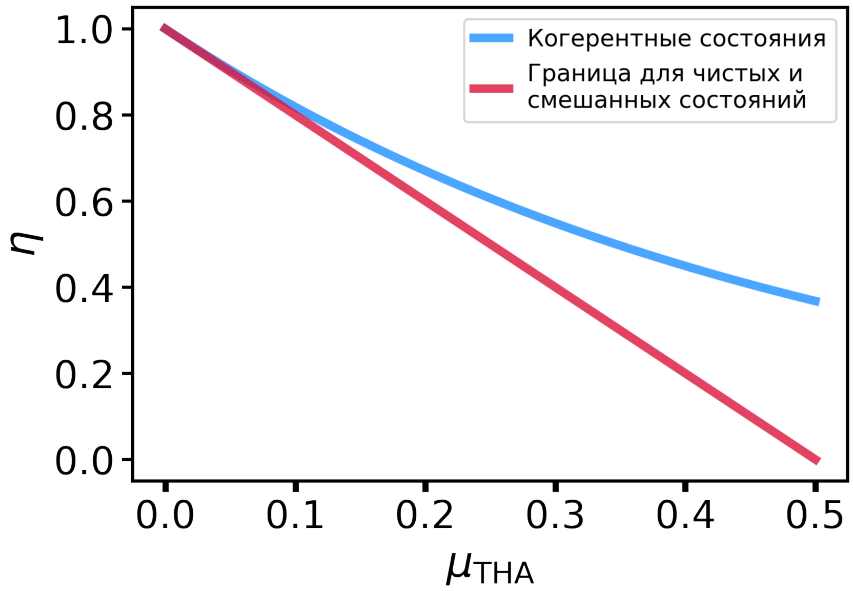


Рисунок 2.2 — Зависимость степени перекрытия квантовых состояний в побочном канале η от среднего числа фотонов μ_{THA} в этих состояниях

и по фазе, идентична. Однако, выражение (2.37) содержит удвоенное среднее число фотонов μ_{THA}. В работе [137] была продемонстрирована эквивалентность поляризационных и фазовых преобразований. С чем же связано различие формул (2.25) и (2.37)? Ответ состоит в следующем. Оба типа кодировки являются принципиально двухмодовыми. В случае поляризационного кодирования Ева посылает свет, распределенный по горизонтально и вертикально поляризованным модам. В случае фазового кодирования Ева распределяет свет по пространственным или временны́м модам, выбирая относительную фазу состояния в одной из мод, направляемой внутрь системы КРК, и сохраняя свет во второй моде в качестве репера для его сбивки на светоделителе с вернувшимся состоянием и наблюдением интерференции. Поскольку для максимальной видности интерференционной картины интенсивности в каждой из мод должны совпадать, то суммарное среднее число фотонов в двух модах при фазовом кодировании составит $2\mu_{\text{THA}}$, т.е. при заданной степени различимости квантовых состояний среднее число фотонов во всех модах в случае поляризационного и фазового кодирования совпадают, что согласуется с результатом работы [137].

Итак, мы получили явное выражение для границы степени перекрытия состояний в побочном канале на примере атаки «Trojan Horse» для случая поляризационного и фазового кодирования. Полученные границы являются однопараметрическими и зависят лишь от интенсивности состояний в побочном канале — среднего числа фотонов μ_{THA}. Данная величина является постоянной

при штатной работе системы и экспериментально измеримой. Способ экспериментального определения данной величины будет представлен в следующем разделе.

2.2 Определение интенсивности сигналов в активном побочном канале

Для использования достаточного условия секретности с учетом побочных каналов необходимо использовать выражение (2.16). Как было показано, данная величина зависит от интенсивности состояний в побочном канале. Таким образом, для полного анализа безопасности системы КРК при наличии побочных каналов необходимо экспериментально определить максимальное значение интенсивности состояний, доступных Еве. В настоящем разделе представлен способ экспериментального определения среднего числа фотонов μ_{THA} в состояниях активного побочного канала THA.

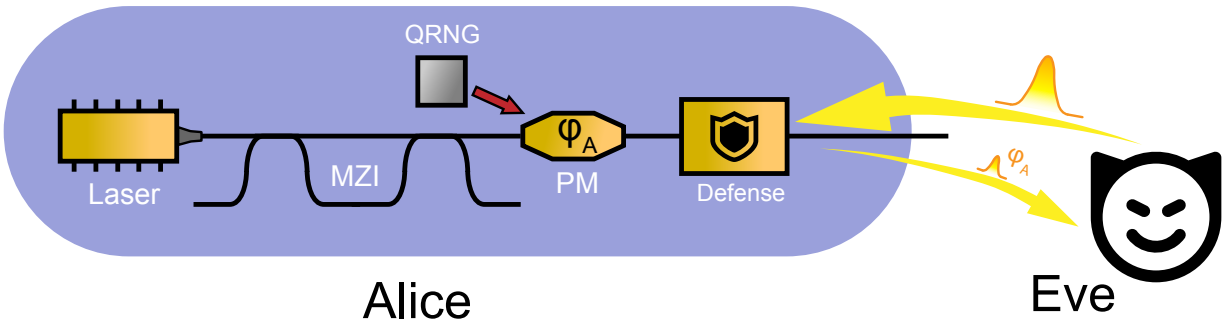


Рисунок 2.3 — Схематичное изображение атаки «Trojan Horse» на передатчик системы КРК с фазовым кодированием. Laser — источник лазерных импульсов, MZI — интерферометр Маха—Цандера, QRNG — квантовый генератор случайных чисел, PM — фазовый модулятор, Defense — пассивные элементы защиты для аттенюации излучения Евы (аттенюаторы, оптические изоляторы, циркуляторы, спектральные фильтры и др.)

Напомним последовательность событий при проведении нарушителем THA: сначала Ева готовит интенсивный световой импульс и заводит его внутрь системы КРК через квантовый канал; импульс распространяется внутри системы, проходя через пассивные элементы защиты, теряя энергию; импульс

претерпевает отражение на границе раздела сред при стыке или неоднородностях оптических элементов, при этом часть энергии теряется; наконец, импульс распространяется в обратном направлении, проходя через устройство приготовления состояния (или выбора базиса), испытывая модуляцию, и, вновь распространившись через элементы защиты, доходит до Евы (рисунок 2.3). Оптимальная стратегия Евы состоит в отправке оптических импульсов, временны́е характеристики которых обеспечивают совпадение с электрическими стробами, подаваемыми на фазовый модулятор, подвергающийся атаке [74]. Для этого она подбирает временну́ю задержку своих импульсов так, чтобы максимизировать мощность отраженных импульсов в момент работы фазового модулятора. Ева может установить частоту повторения своих импульсов f_{THA} равной частоте повторения легитимных импульсов f. Из-за вогнутости функции $\overline{\chi}_E$ (2.8), Ева получает максимальный информационный выигрыш при равномерном распределении интенсивности по всем импульсам [74]; следовательно, среднее число фотонов в каждом импульсе одинаково и равно μ_{THA}. Для увеличения информационного выигрыша Ева может снизить частоту повторения посылаемых ей импульсов, блокируя легитимные импульсы, не затронутые атакой. Наконец, Ева может подобрать длину волны атаки λ так, чтобы максимизировать μ_{Eve}.

Таким образом, среднее число фотонов в импульсах Евы можно вычислить как

$$\mu_{\text{THA}}(\lambda) = \frac{P_{\text{THA}}(\lambda)\,\lambda}{f_{\text{THA}}\,h\,c}, \tag{2.40}$$

где P_{THA} — мощность излучения, возвращающегося к Еве, λ — длина волны атаки, f_{THA} — частота повторения импульсов Евы, $h \approx 6{,}63 \times 10^{-34}$ Дж·с — постоянная Планка, $c \approx 3 \times 10^8$ м/с — скорость света в вакууме.

Рассмотрим некоторые реалистичные ограничения для выражения (2.40). Во-первых, для f_{THA} может существовать нижний предел, несмотря на то что протокол BB84 не предполагает явного мониторинга частоты регистрации событий. В реальных системах КРК низкая частота генерации ключа вызывает ошибку по времени выполнения, что приводит к прерыванию сеанса КРК. Конкретное значение максимально допустимой длительности сеанса КРК зависит от реализации системы, однако разумно полагать, что оно не превышает величину, в 10— 100 раз выше стандартной. При этом Ева может, в принципе, компенсировать потери в линии связи с помощью идеального канала, тем самым увеличив скорость генерации ключа. Для стандартного одномодового

оптоволокна SMF-28 с потерями порядка 0,2 дБ/км и длиной линии 100 км Ева может получить дополнительный запас до 20 дБ. Таким образом, эффективная частота повторения атакующих импульсов равна $f_{\text{THA}} = \alpha f$, где α обычно не менее 10^{-4}.

Наиболее очевидная реализация THA предполагает использование длины волны, совпадающей с легитимной, которая, обычно, лежит в телекоммуникационном диапазоне 1260—1625 нм для волоконных систем КРК, или в ближнем инфракрасном и видимом диапазоне для атмосферных систем КРК. Однако было показано, что атаки THA могут быть эффективны и при значительной отстройке от легитимной длины волны [76; 77; 138—141]. На практике для анализа безопасности экспериментально доступны лишь два спектральных диапазона: 200—1100 нм (область чувствительности кремниевых детекторов) и 1100—2600 нм (область чувствительности InGaAs-детекторов). Данные диапазоны могут быть расширены с использованием сверхпроводящих ДОФ, что было продемонстрировано в работе [141], однако такие приемники являются более дорогостоящим и сложным в обслуживании оборудованием.

Наконец, существование верхней границы мощности излучения Евы является основным ограничивающим фактором для μ_{THA}. Эта граница может определяться как чувствительностью сторожевого детектора, так и, в более общем случае, порогом лазерного повреждения (laser induced damage threshold — LIDT) оптических компонентов внутри атакуемого устройства [74]. Превышение LIDT во время сеанса КРК приведёт к разрыву связи между Алисой и Бобом и невозможности проведения атаки. Для типичной волоконной системы КРК значение LIDT можно оценить примерно как 10 Вт (40 дБм) с незначительными вариациями в пределах рассматриваемого спектрального диапазона. Важно отметить, что воздействие мощного излучения может существенно различаться для разных оптических элементов и приводить к изменению их свойств, в частности, степени пропускания. Следовательно, работоспособность мер защиты от атаки с лазерным повреждением LDA является важным допущением при проведении анализа безопасности системы при наличии оптических побочных каналов.

Итак, среднее число фотонов в импульсах Евы определяется мощностью возвращающегося к ней света, которая в свою очередь вычисляется следующим образом:

$$P_{\text{THA}} = P_{\max}[\text{дБм}] + T[\text{дБ}] + R[\text{дБ}], \tag{2.41}$$

где $P_{\max}$ — максимальная средняя мощность зондирования в дБм, T — суммарный коэффициент пропускания элементов защиты в прямом и обратном направлениях в дБ, R — максимальная величина отражения от внутренностей системы КРК без элементов защиты в дБ. Величина $P_{\max}$ для схем без сторожевого детектора может быть принята равной значению LIDT 10 Вт (40 дБм). Ниже мы рассмотрим способы экспериментального определения величин T и R на примере реальной системы КРК с фазовым кодированием.

2.2.1 Измерение спектров пропускания пассивных элементов системы КРК

Для подавления атаки «Trojan horse» в системах КРК используются следующие пассивные оптические элементы (будем называть их элементами защиты от ТНА):

- Оптические изоляторы, пропускающие излучение в направлении распространения легитимного сигнала и подавляющие излучение в обратном направлении;
- Оптические циркуляторы, работающие по схожему с изоляторами принципу, однако имеющие три порта вместо двух. Излучение хорошо проходит из 1-го во 2-й, из 2-го в 3-й порты и подавляется в остальных направлениях. Циркулятор может использоваться вместе с зеркалом, подключенным ко 2-му порту; в таком случае он будет работать как изолятор;
- Спектральные фильтры, пропускающие излучение в узком спектральном диапазоне в окрестности длины волны легитимного излучения. Вместо узкополосного фильтра спектральную селекцию в системе может осуществлять спектральный мультиплексор, или WDM-фильтр;
- Оптические аттенюаторы, одинаково ослабляющие оптическое излучение в любом направлении. Используются как постоянные, так и переменные аттенюаторы.

Как отмечалось в разделе 1.7.3, цель данных компонентов защиты состоит в максимальном ослаблении интенсивности оптического сигнала, возвращающегося злоумышленнику. Как видно из рисунка 2.2, степень перекрытия состояний

увеличивается при уменьшении среднего числа фотонов μ_{THA}, а значит, согласно формуле (2.16), увеличивается и нехватка информации Евы при заданном уровне ошибки E_1.

Поскольку злоумышленник волен в выборе длины волны зондирования, перечисленные элементы защиты должны обеспечивать безопасность не только на длине волны легитимного излучения, но и во всей остальной спектральной области (так, например, в работе [138] была продемонстрирована успешная атака «Trojan Horse» на длине волны 1924 нм).

Для измерения спектра пропускания оптических элементов используется источник излучения, свет от которого проходит через исследуемый элемент и идет на приемник. Оптические элементы защиты от атаки «Trojan horse» характеризуются сверхнизкими коэффициентами пропускания в окрестности рабочей длины волны, достигающими -100 дБ и ниже. При этом вне этой спектральной области их поведение может быть непредсказуемым: коэффициент пропускания может падать, а может расти до значений, близких к 0 дБ [76; 77; 139—141]. Такое поведение накладывает жесткие требования на динамический диапазон измерений.

С другой стороны, измерения в широком спектральном диапазоне требуют наличие широкополосного или широко перестраиваемого источника излучения и приемника (или нескольких приемников) с широкой спектральной чувствительностью. Таким образом, необходим мощный (для обеспечения широкого динамического диапазона) источник белого света (для измерений в широком спектральном диапазоне). К таким источникам относится суперконтинуумный лазер, спектр которого значительно превышает ширину спектров обычных лазеров и обладает значительно более высокой мощностью и качеством пучка по сравнению с некогерентными источниками белого света.

К суперконтинуумному лазеру необходимо добавить набор перестраиваемых фильтров (например, акустооптических) для осуществления спектральной селекции. В качестве приёмника можно использовать ДОФ на базе однофотонного лавинного фотодиода (ЛФД), поскольку классические измерители оптической мощности и спектроанализаторы обычно ограничены порогом чувствительности в районе от -80 дБм до -60 дБм из-за высокого уровня электрических шумов. ЛФД при работе в синхронном режиме с узкими электрическими стробами и достаточной величине мертвого времени демонстрируют низкую скорость темновых отсчётов (порядка 10 с^{-1} при частоте стробирова-

ния 10 МГц), что обеспечивает точные измерения в динамическом диапазоне до −120 дБ. Для ближнего инфракрасного диапазона подходит ЛФД на базе InGaAs, а для длин волн 400–1100 нм — кремниевый ЛФД.

Также в схему необходимо добавить переменный аттенюатор, поскольку для работы лавинного фотодиода в режиме счёта фотонов нужно, чтобы среднее число фотонов, приходящих на строб детектора, было много меньше 1. В противном случае нельзя пренебречь вероятностью одиночного срабатывания детектора от двух и более пришедших фотонов, из-за чего исчезает прямая пропорциональность между числом фотоотсчетов и числом пришедших фотонов. Это связано с пуассоновской статистикой когерентного излучения:

$$P_\mu(n=1) = \mu e^{-\mu} \approx \mu \tag{2.42}$$

$$P_\mu(n>1) = 1 - P_\mu(n=0) - P_\mu(n=1) \approx \frac{3\mu^2}{2} \ll P_\mu(n=1), \tag{2.43}$$

где мы пренебрегли высшие членами разложения в ряд при условии $\mu \ll 1$.

Предложенная в настоящей работе схема экспериментальной установки для измерения спектра пропускания пассивных волоконных элементов представлена на рисунке 2.4. Из системы КРК извлекаются элементы защиты от ТНА и измеряется спектр пропускания каждого из них в прямом и обратном направлении.

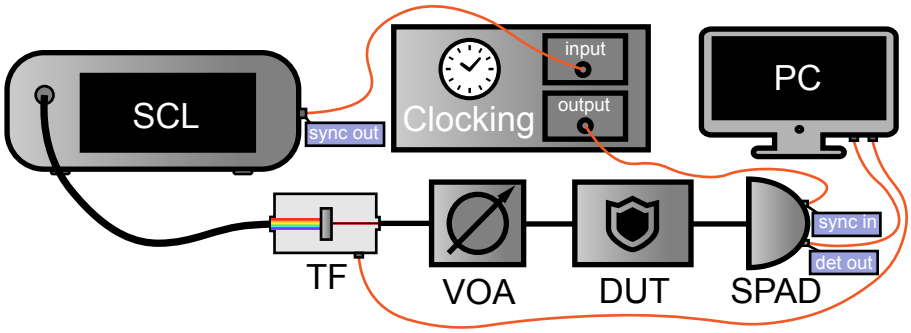


Рисунок 2.4 — Схема экспериментальной установки для измерения спектра пропускания: SCL — суперконтинуумный лазер, TF — перестраиваемый фильтр, VOA — переменный оптический аттенюатор, DUT — тестируемое устройство, SPAD — однофотонный ЛФД, Clocking — временной коррелятор электрических сигналов, PC — персональный компьютер. Черными линиями изображены оптические волокна, красными линиями изображены электрические провода

Для обеспечения минимального уровня темновых шумов необходим синхронный режим работы схемы. Для этого нужно соединить электрический выход синхронизации лазера со входом синхронизации ЛФД через электронику синхронизации, обеспечивающую нужный временной сдвиг, чтобы электрический стробы на ЛФД приходились на момент прихода на него лазерных импульсов. Описанная схема применялась для измерения спектров в диапазоне 1100—1800 нм с использованием ЛФД на базе InGaAs. Шаг по длине волны составлял 1 нм, а ширина полосы фильтра около 10 нм.

Для получения коэффициента пропускания необходимо также измерить опорный спектр (при извлеченном из схемы тестируемом элементе, DUT) и скорость темновых отсчётов при выключенном лазере. Тогда формула для коэффициента пропускания при заданной длине волны в дБ имеет вид:

$$T[\text{дБ}] = 10\log_{10}\left(\frac{N - N_{\text{dark}}}{N_{\text{ref}} - N_{\text{dark}}}\right) + (A_{\text{ref}}[\text{дБ}] - A[\text{дБ}]), \tag{2.44}$$

где N — число отсчетов на детекторе при подключённом DUT, N_{ref} — число отсчётов при измерении опорного спектра, N_{dark} — число темновых отсчётов за то же время (при выключенном лазере), A_{ref} — значение коэффициента аттенюации в дБ, выставленного на переменном аттенюаторе при измерении опорного спектра, A — значение коэффициента аттенюации в дБ при подключённом DUT.

Данная схема автоматически учитывает неоднородность спектра лазера, зависимость пропускания волокна и квантовой эффективности детектора от длины волны, благодаря измерению опорного спектра. Так как указанные факторы оказывают линейное влияние на число отсчётов, нормировка спектров пропускания на опорный позволяет их дополнительно не учитывать. Именно поэтому формула (2.44) содержит только значения числа отсчётов.

Динамический диапазон измерений связан с минимальным числом отсчётов, заметным на фоне темнового шума. Он может быть вычислен в дБ по формуле:

$$T_{\text{min}}[\text{дБ}] = 10\log_{10}\left(\frac{N_{\text{dark}}}{N_{\text{ref}} - N_{\text{dark}}}\right) + (A_{\text{ref}}[\text{дБ}] - A_{\text{min}}[\text{дБ}]), \tag{2.45}$$

где N_{ref} — число отсчётов при измерении опорного спектра, N_{dark} — число темновых отсчетов при выключенном лазере, A_{max} — коэффициент аттенюации (в дБ), выставленный при измерении опорного спектра, A_{min} — минимально возможное значение коэффициента аттенюации (обычно, 0 дБ).

Измерения опорного спектра и темновых шумов (на уровне 10—20 отсчётов в секунду) позволили вычислить динамический диапазон измерений по формуле (2.45), который достиг $|T_{\min}| = 120$ дБ. Это значение демонстрирует уникальные возможности разработанной экспериментальной установки, так как на несколько порядков превышает пределы, доступные при использовании классических приемников.

Перейдем к анализу компонентов защиты системы КРК. В рамках настоящей работы исследовался передатчик системы КРК, использующей фазовое кодирование и протокол BB84. Блок защиты от ТНА в составе данной системы представлен на рисунке 2.5. В состав данного блока входят циркулятор с зеркалом, изолятор, а также аттенюатор с WDM-фильтром. Дополнительно исследовался переменный аттенюатор, входящий в состав блока приготовления квантовых состояний.

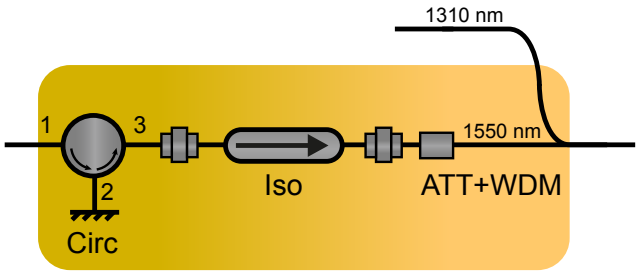


Рисунок 2.5 — Блок защиты от ТНА для установки Алисы. Circ — оптический циркулятор с зеркалом, подключенным к порту 2, Iso — оптический изолятор, ATT+WDM — сваренные аттенюатор и WDM-фильтр

Результаты измерений спектра пропускания пропускания приведены на рисунке 2.6.

Полученные результаты подтверждают непредсказуемость поведения волоконно-оптических элементов в широком спектральном диапазоне. Как видно из рисунка 2.6, масштаб изменения величины пропускания может достигать 60 дБ. Было выявлено, что спектры пропускания аттенюаторов и WDM не зависит от направления распространения излучения (поэтому здесь приведены лишь результаты измерений в прямом пропускании). Циркулятор и изолятор сильно изменяют уровень пропускания при отклонении от длины волны протокола 1550 нм, при этом характер изменения совпадает с опубликованными ранее результатами [76; 77]. Отметим, что области большого затухания в этих

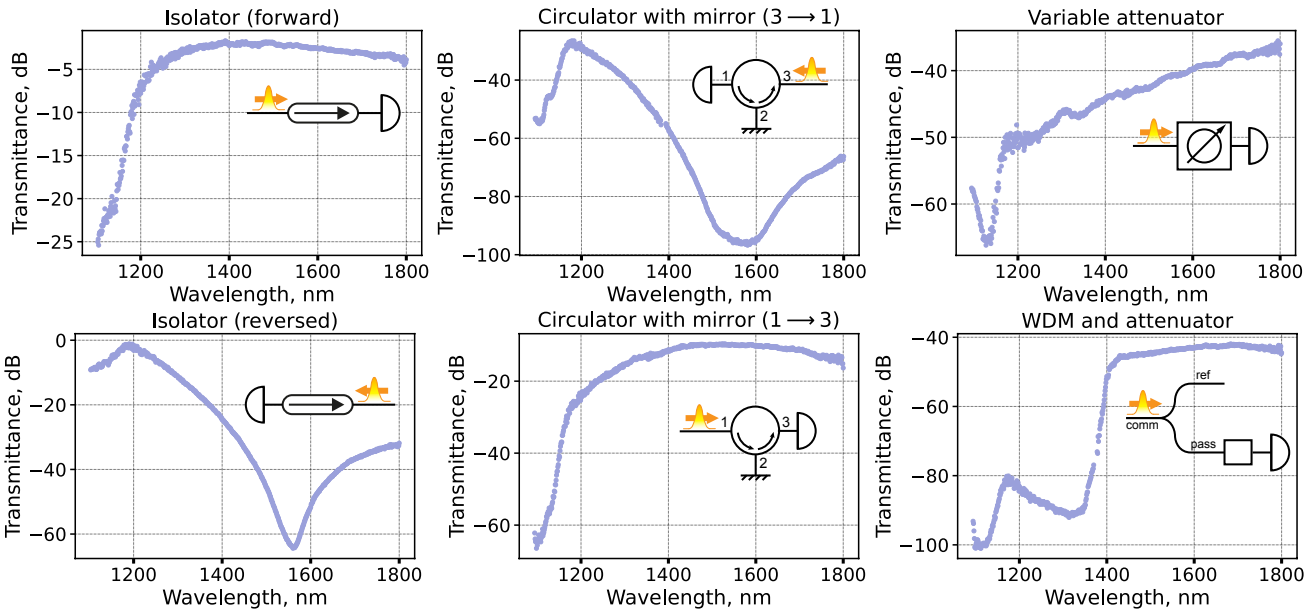


Рисунок 2.6 — Измеренные спектры пропускания элементов защиты из состава исследуемой системы КРК: оптический изолятор (в прямом и обратном подключении), оптический циркулятор с зеркалом (в прямом подключении $1 \to 3$ и обратном подключении $3 \to 1$), переменный аттенюатор (спектры пропускания в обе стороны совпали) и WDM-фильтр с постоянным аттенюатором (спектры пропускания в обе стороны совпали)

работах не были точно промерены из-за ограниченного динамического диапазона. В настоящей работе впервые представлены спектры пропускания элементов с потерями, достигающими 100 дБ.

Суммарный спектр пропускания блока защиты от ТНА состоит из суммы спектров пропускания изолятора, циркулятора и WDM-фильтра с аттенюатором в прямом и обратном проходе. Полученный результат приведен на рисунке 2.7.

2.2.2 Широкополосная рефлектометрия системы КРК

Основным физическим принципом, лежащим в основе атаки «Trojan Horse» является френелевское отражение света от границы раздела сред. Системы КРК являются составными системами, состоящими из набора волоконно-оптических элементов, соединенных между собой. Как правило, соединение осуществляется с помощью оптических разъемов, например, разъемов типа FC.

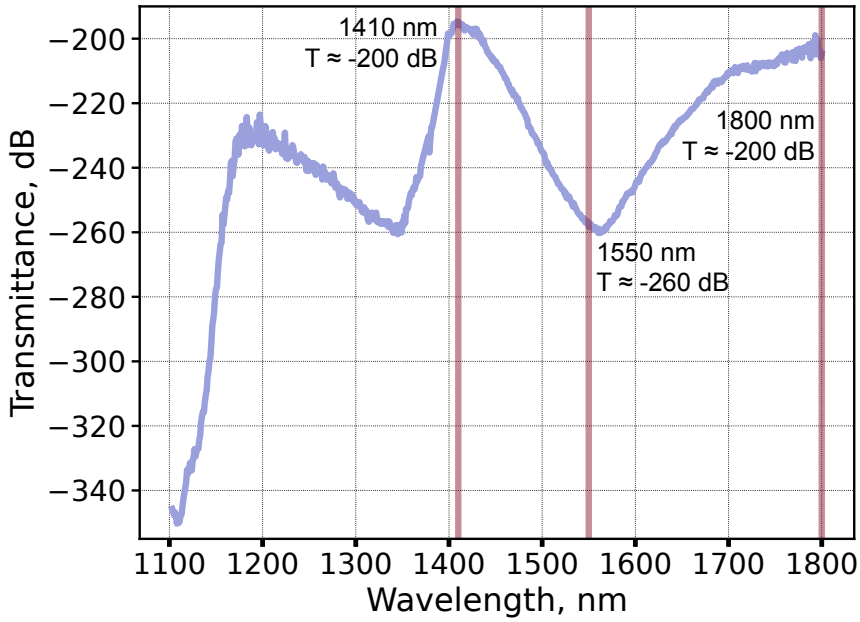


Рисунок 2.7 — Суммарный спектр пропускания блока защиты от ТНА в прямом и обратном проходе

Из-за неоднородности показателя преломления наконечников (ферул) оптических коннекторов возникает граница раздела сред, приводящая к отражению, величина которого варьируется от -60 дБ до -20 дБ в зависимости от типа разъема. Наилучшие показатели обеспечивают APC разъемы с угловой полировкой, поэтому их использование в системах КРК является простой, но достаточно эффективной мерой против атаки «Trojan Horse». Подавить отражение на соединениях до минимума можно с помощью оптической сварки различных оптических элементов, что, однако, затрудняет их сборку, отладку и обслуживание.

Соединения различных оптических элементов являются не единственным источником паразитных отражений. Как правило, системы КРК содержат ряд оптических элементов, имеющих сложную, оптически неоднородную внутреннюю структуру. Значительные отражения (-50 дБ и выше) зачастую наблюдаются от стенок фазовых модуляторов, поверхностей детекторов и лазеров. Более того, многие системы КРК содержат зеркала, что приводит к практически стопроцентному отражению.

Таким образом, для получения полного представления об отражениях от частей системы, необходимо измерить картину отражений по всему оптическому пути схемы после устройства приготовления состояния (далее будем считать, что таким устройством является фазовый модулятор). Данная про-

цедура хорошо известна в классической оптике и носит название оптическая рефлектометрия [142]. Так называемая оптическая рефлектометрия во временно́й области (optical time-domain reflectometry — OTDR) осуществляется с помощью прибора, называемого рефлектометром, представляющего собой синхронизированные лазер и фотодетектор. Лазерный импульс отправляется в оптический канал, отражается и возвращается назад, попадая на детектор внутри рефлектометра, после чего по времени его прихода вычисляется расстояние, на котором импульс претерпел отражение. Данный метод часто используется при поиске разрывов и повреждений в оптоволоконных сетях длиной в десятки километров. В случае исследования отражений системы КРК оптический рефлектометр должен удовлетворять следующим требованиям: во-первых, его пространственное разрешение должно быть не хуже чем несколько десятков сантиметров, что обеспечивается пикосекундной длительностью лазерных импульсов; во-вторых, измерения должны быть точны в достаточно большом динамическом диапазоне, что обеспечивается использованием чувствительных однофотонных детекторов (так называемый ν-OTDR метод). Такие однофотонные рефлектометры на длине волны 1550 нм со сверхвысоким разрешением на сегодняшний день являются коммерчески доступными приборами и выпускаются серийно.

Однако для применений в рамках анализа безопасности системы КРК, оптический рефлектометр должен удовлетворять еще одному требованию, а именно, иметь возможность перестройки в широком спектральном диапазоне. В рамках настоящей работы был впервые разработан и собран рефлектометр с разрешением по длинам волн от 1100 нм до 1800 нм. Схема рефлектометра изображена на рисунке 2.8.

Устройство работает следующим образом: суперконтинуумный лазер генерирует оптические импульсы длительностью 500—700 пс с некоторой частотой повторения и подает электрический сигнал на временной коррелятор для запуска таймера; спектральный фильтр, управляемый с персонального компьютера выделяет заданную длину волны (с полосой около 10 нм); импульс ослабляется на аттенюаторе до уровня, обеспечивающим режим счета фотонов (см. формулы (2.42) и (2.43)); импульс заводится внутрь тестируемой системы КРК, из которой предварительно извлекаются компоненты защиты от ТНА, обладающие высокими потерями; отраженный импульс проходит через циркулятор и попадает на ЛФД, который регистрирует срабатывание и посылает сигнал вы-

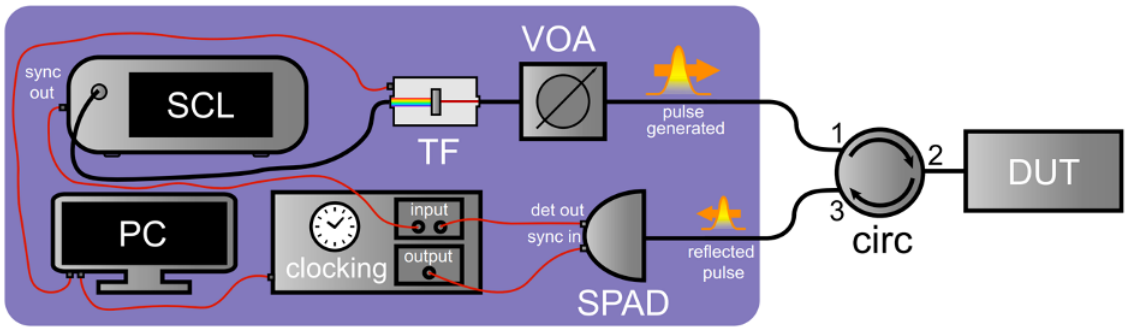


Рисунок 2.8 — Широкополосный ν-OTDR рефлектометр: SCL — суперконтинуумный лазер, TF — перестраиваемый фильтр, VOA — переменный оптический аттенюатор, circ — оптический циркулятор, DUT — тестируемое устройство, SPAD — однофотонный ЛФД, Clocking — временной коррелятор электрических сигналов, PC — персональный компьютер. Черными линиями изображены оптические волокна, красными линиями изображены электрические провода

ключения таймера на временной коррелятор. Измерение повторяется в течение установленного времени (1—10 с) для каждой длины волны. Временны́е отметки легко пересчитать в длину с учетом скорости света в кварцевом волокне. Для каждого разрешенного участка оптического пути записывается число фотоотсчетов за установленный промежуток времени. Для перевода в относительные единицы предварительно измеряется опорный спектр, как и в случае измерения спектров пропускания (раздел 2.2.1), путем подключения ЛФД ко 2-му порту циркулятора и увеличению уровня аттенюации на переменном аттенюаторе. Дополнительно измеряется спектр пропускания самого циркулятора из порта 1 в порт 2 и из порта 2 в порт 3 с использованием схемы, описанной в разделе 2.2.1.

Величина отражений для выбранной длины волны и для выбранного участка схемы вычисляется по формуле

$$R[\text{дБ}] = 10\log_{10}\left(\frac{N}{N_{\text{ref}}}\right) + A_{\text{ref}}[\text{дБ}] - A[\text{дБ}] - T_{1\to2}[\text{дБ}] - T_{2\to3}[\text{дБ}], \qquad (2.46)$$

где N — число отсчетов на детекторе при подключённом DUT, N_{ref} — число отсчётов при измерении опорного спектра, A_{ref} — значение коэффициента аттенюации в дБ, выставленного на переменном аттенюаторе при измерении опорного спектра, A — значение коэффициента аттенюации в дБ при подключённом DUT, $T_{1\to2}$ — пропускание циркулятора из порта 1 в порт 2, $T_{2\to3}$ — пропускание циркулятора из порта 2 в порт 3.

Результат рефлектометрии — рефлектограмма, изображается в виде зависимости величины отражения от расстояния. За нулевую отметку длины

берется вход в исследуемую оптическую схему. Рефлектограмма передатчика исследуемой системы КРК с извлеченными элементами защиты от ТНА на длине волны 1325 нм представлена на рисунке 2.9. На рефлектограмме видно, что каждому оптическому элементу и волоконному соединению отвечает пик отражения. Сильнее всего заметны отражения от волоконных коннекторов. В частности, наблюдаются три пика после интерферометра Маха—Цандера — характерная картина, отвечающая прохождению импульса согласно одному из четырех вариантов: короткое плечо—короткое плечо, короткое плечо—длинное плечо, длинное плечо—короткое плечо, длинное плечо—длинное плечо. Динамический диапазон измерений определяется, в основном, уровнем фонового рэлеевского рассеяния в оптоволокне, а также темновыми срабатываниями.

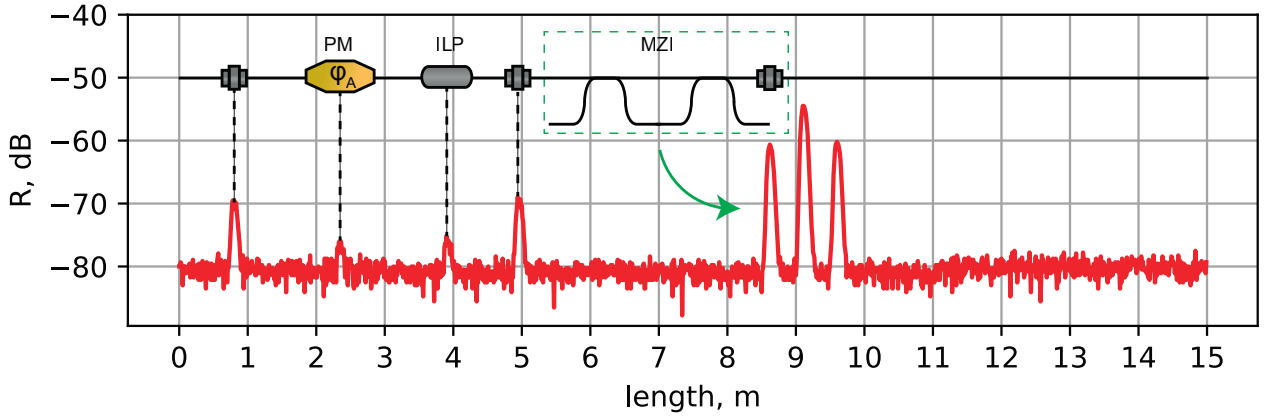


Рисунок 2.9 — Рефлектограмма передатчика исследуемой системы КРК на длине волны 1325 нм с расшифровкой пиков: PM — фазовый модулятор, ILP — поляризатор, MZI — интерферометр Маха—Цандера

Возможность выбора длины волны в данной схеме позволяет построить развертку рефлектограммы по длинам волн в виде «тепловой карты» (рисунок 2.10). Для этого была проведена рефлектометрия схемы в диапазоне 1100—1800 нм с шагом 25 нм. Видно, что максимальный пик отражения приходится на участок схемы в окрестности дистанции 8 м и соответствует отражению от конца интерферометра Маха—Цандера. Сама величина отражения изменяется в зависимости от длины волны. Также видно, что шумовой порог также зависит от длины волны и растет при движении в коротковолновую область. Это связано с тем, что интенсивность рэлеевского рассеяния обратно пропорциональна четвертой степени длины волны.

Отдельно изобразим зависимость величины отражения от длины волны для участка максимального отражения (рисунок 2.11). Видно, что отражение

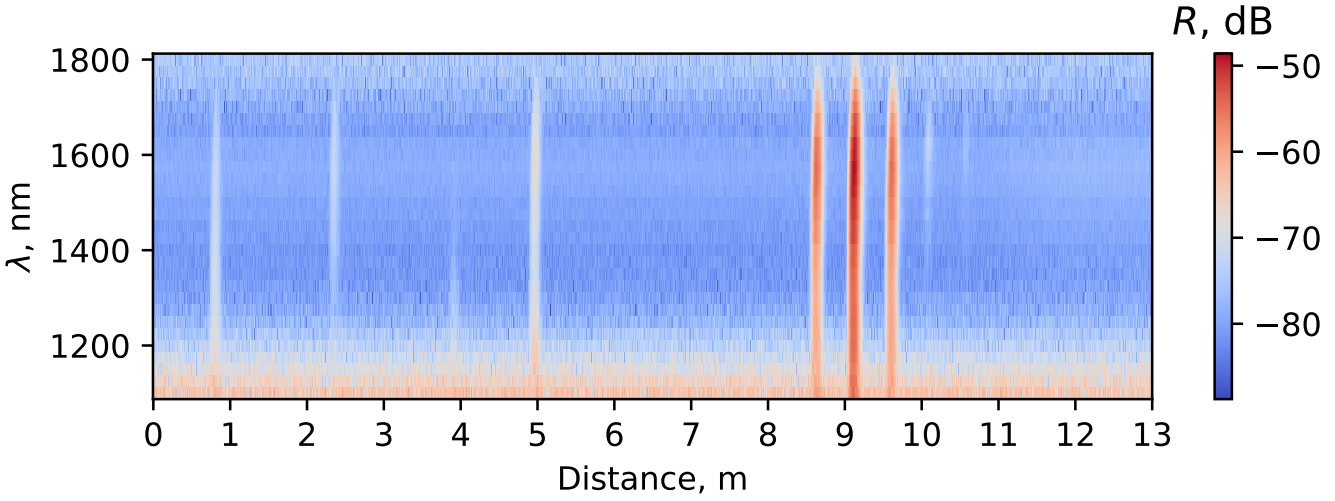


Рисунок 2.10 — «Тепловая карта» отражений, полученная при широкополосной рефлектометрии передатчика исследуемой системы КРК

на легитимной длине волны 1550 нм практически достигает максимального значения, которое соответствует длине волны 1575 нм и величине $R = -48$ дБ. Полученная зависимость будет использована нами для дальнейшего анализа безопасности системы КРК.

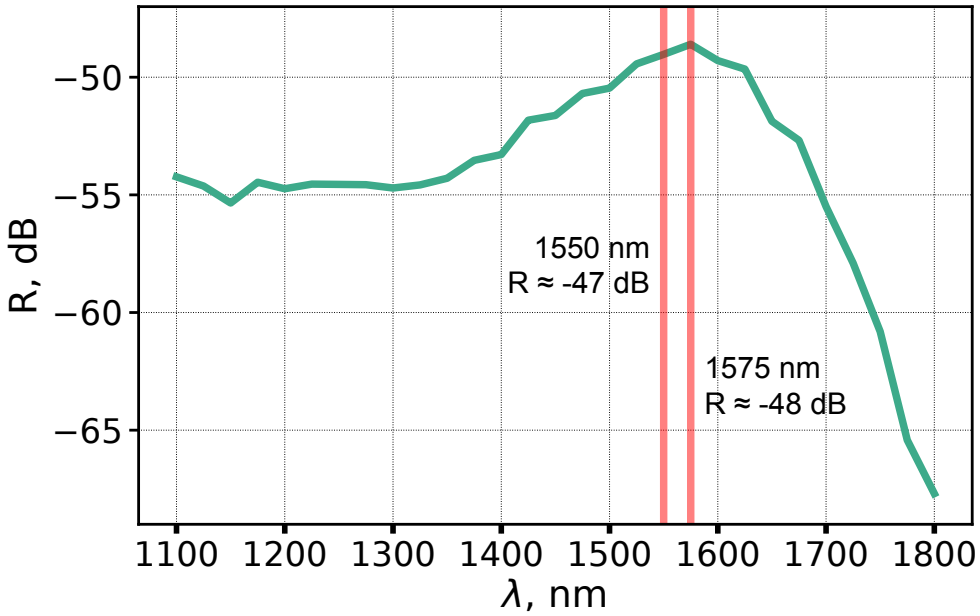


Рисунок 2.11 — Зависимость величины отражения от длины волны для максимального пика отражения в окрестности участка схемы на дистанции 9 м

2.2.3 Анализ результатов измерений

Итак, были определены все слагаемые, входящие в формулу (2.41): максимальная мощность излучения определяется LIDT (40 дБм), измеренные зависимости для T и R изображены на рисунках 2.7 и 2.11, соответственно. Теперь мы можем вычислить мощность излучения, доходящего до Евы, и подставить полученную величину в выражение (2.40), чтобы определить μ_{THA}. Будем использовать следующие параметры: $f = 10$ МГц, $\alpha = 10^{-4}$, следовательно, $f_{\text{THA}} = 1$ кГц. Полученная зависимость μ_{THA} от длины волны излучения Евы изображена на рисунке 2.12.

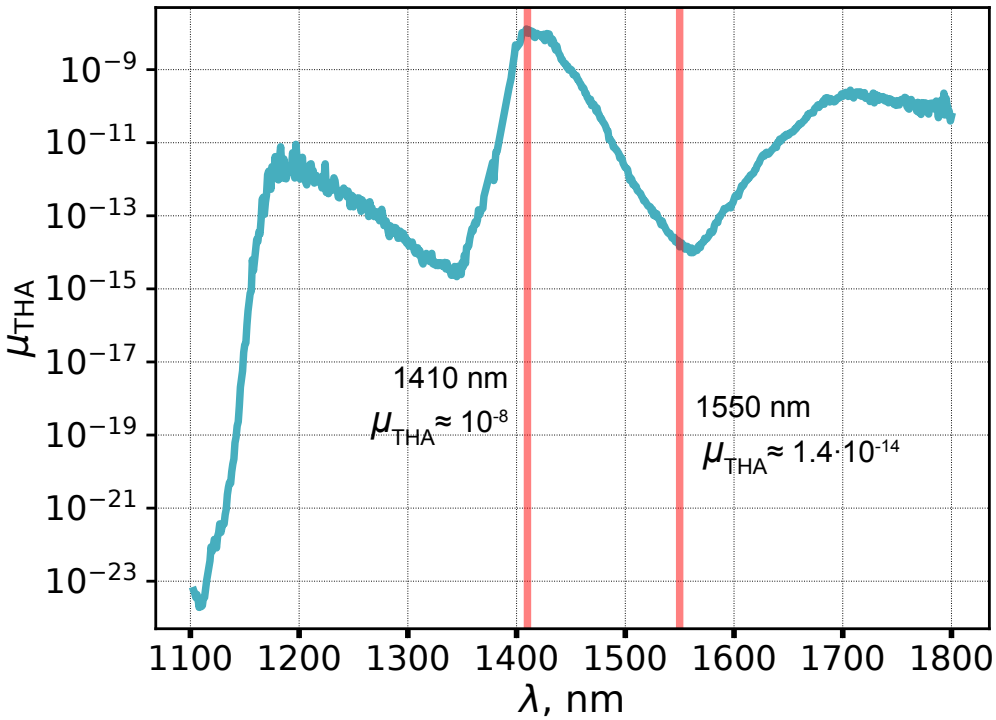


Рисунок 2.12 — Зависимость величины отражения от длины волны для максимального пика отражения в окрестности участка схемы на дистанции 9 м

Таким образом, среднее число фотонов в импульсах Евы существенно зависит от длины волны излучения, используемого Евой при THA. Так, максимальная величина $\mu_{\text{THA}} \approx 10^{-8}$ соответствует длине волны 1410 нм, что более чем на 5 порядков больше величины на легитимной длине волны 1550 нм, равной $\mu_{\text{THA}} \approx 10 \cdot 1{,}4^{-14}$. Это подчеркивает важность проведения анализа в широком спектральном диапазоне, поскольку оценки, ограничивающиеся легитимной длиной волны, дают заниженную величину интенсивности излучения, приходящего к Еве и, как следствие, заниженные значения утечки информации.

С другой стороны, подобный анализ избавляет от необходимости использования чрезмерно консервативных методов оценивания μ_{THA}, включающих в себя допущение о стопроцентной величине отражения во всем спектральном диапазоне, за незнанием реального значения R. Конечно, такая оценка нефизична для большинства систем. В работе, посвященной подготовке коммерческой системы КРК к проведению сертификации [143], предположение о стопроцентном отражении привело авторов к выводу о необходимости добавить в систему дополнительный элемент защиты, например, изолятор, для обеспечения требуемого уровня μ_{THA}. Вероятно, такого вывода можно было бы избежать при проведении широкополосной рефлектометрии системы и определении действительной величины μ_{THA} описанным выше способом.

Наконец, проведем вычисление минимальной степени перекрытия состояний Евы по формуле (2.37):

$$\eta_{\text{THA}} = 1 - 2\mu_{\text{THA}} = 0{,}99999998. \tag{2.47}$$

Данная величина отличается от единицы лишь в 8 знаке после запятой. Для иллюстрации, вычислим верхнюю границу величины Холево $\overline{\chi}_E$, входящую в условную энтропию системы Алиса—Ева, по формуле (2.8), положив $E_1 = 0$ (отсутствие коллективной атаки):

$$\overline{\chi}_E = h\left(\frac{1-\eta_{\text{THA}}}{2}\right) = h\left(\mu_{\text{THA}}\right) \approx 2{,}8 \cdot 10^{-7}. \tag{2.48}$$

Полученная величина заметно меньше единицы. Отсюда можно сделать вывод, что атака «Trojan Horse» неэффективна против передатчика исследуемой системы КРК. Действительно, использование элементов защиты в достаточной мере привело к крайне низким значениям μ_{THA}, что обеспечило малость информации, доступной Еве. В то же время, не следует интерпретировать данный результат как возможность исключения данного побочного канала из анализа безопасности и, например, формулы для длины секретного ключа (1.21). Во-первых, при значениях QBER, близких к предельно высокому, данная величина может отличаться от единицы значительно меньше. Во-вторых, как отмечалось выше, все атаки по побочным каналам комбинируются, что приводит к кумулятивному эффекту и возможности возникновения заметной утечки информации.

2.3 Секретность в условиях комбинированных атак по побочным каналам

Выше была описана последовательность действий для обеспечения безопасности КРК при наличии побочного канала утечки информации на примере активного оптического побочного канала — атаки «Trojan Horse». В общем случае, могут иметь место несколько побочных каналов, например, связанные с переизлучением ЛФД и излучением электронных компонентов в радиочастотном диапазоне. В таком случае, набор возможных квантовых состояний (2.1) и (2.2) должен быть преобразован с учетом дополнительных квантовых подсистем, связанных с соответствующими побочными каналами:

$$U_{BE}\Big[|0\rangle_B \otimes |E\rangle_E\Big] \otimes \rho^0_{\text{THA}} \longrightarrow U_{BE}\Big[|0\rangle_B \otimes |E\rangle_E\Big] \otimes \rho^0_{\text{SC}_1} \otimes \rho^0_{\text{SC}_2} \otimes ... \otimes \rho^0_{\text{SC}_N}, \tag{2.49}$$

$$U_{BE}\Big[|1\rangle_B \otimes |E\rangle_E\Big] \otimes \rho^1_{\text{THA}} \longrightarrow U_{BE}\Big[|1\rangle_B \otimes |E\rangle_E\Big] \otimes \rho^1_{\text{SC}_1} \otimes \rho^1_{\text{SC}_2} \otimes ... \otimes \rho^1_{\text{SC}_N}, \tag{2.50}$$

где $\rho^0_{\text{SC}_i}$ и $\rho^1_{\text{SC}_i}$ — матрицы плотности состояний некоторого i-го побочного канала, отвечающих битам 0 и 1, соответственно, N — число побочных каналов.

В силу вышеупомянутой мультипликативности фиделити Ульмана, величина η, требуемая для вычисления условной энтропии системы Алиса—Ева по формуле (2.16), может быть вычислена как произведение степеней перекрытия состояний соответствующих побочных каналов:

$$\eta = \eta_{\text{SC}_1} \cdot \eta_{\text{SC}_2} \cdot ... \cdot \eta_{\text{SC}_N}, \tag{2.51}$$

где η_{SC_i} — степень перекрытия состояний i-го побочного канала, отвечающих битам 0 и 1.

Поскольку каждый из рассматриваемых побочных каналов представляет собой электромагнитное излучение, для него будут выполнятся те же соотношения, что и для THA. Так, например, соотношение (2.25) дает общее выражение для связи степени перекрытия состояний, содержащих фотоны в ортогональных модах (не обязательно поляризационных), с вероятностью вакуумной компоненты и средним числом фотонов в данных состояниях.

Общепринятой в литературе величиной для характеризации пассивного оптического побочного канала «Backflash» является величина, называемая

вероятностью «Backflash» P_{BF}, определяемая как условная вероятность зарегистрировать переизлученный свет идеальным детектором при условии срабатывания переизлучающего детектора [71; 72; 144; 145]. Из определения следует, что данная величина представляет собой не что иное как разность единицы и вероятности наблюдения нуля фотонов в переизлученном состоянии, т.е. вероятности вакуумной компоненты. Тогда, для степени различимости состояний переизлученнного света справедлива оценка:

$$\eta_{\mathrm{BF}} \geqslant 1 - p_0 = P_{\mathrm{BF}}. \tag{2.52}$$

Величина P_{BF} может быть оценена экспериментально при накоплении статистики фотоотсчетов от переизлученных сигналов (экспериментальные схемы представлены в работах [71; 72; 144; 145]). Следует учесть, что пассивные компоненты защиты от THA на приемной стороне также оказывают влияние на интенсивность переизлученного света, доходящего до Евы, поэтому оценка вероятности «Backflash», полученная при непосредственном подключении к тестируемому детектору, должна быть домножена на коэффициент пропускания элементов защиты, измеренных, например, способом, описанным в разделе 2.2.1.

Аналогичные соображения применимы и для других типов побочных каналов. И хотя экспериментальный анализ неоптических побочных каналов выходит за рамки настоящей работы, можно с уверенностью сказать, что электромагнитная природа радиочастотного излучения позволяет применять все те же соотношения, справедливые для THA и BFA.

2.4 Выводы по главе

Описан способ вычисления длины секретного ключа для выполнения достаточного условия секретности в квантовой криптографии при комбинированном проведении унитарной коллективной атаки и атак по побочным каналам утечки информации. В рамках данного способа каждый побочный канал может быть описан лишь одним параметров — степенью перекрытия квантовых состояний (квадратному корню из фиделити Ульмана), отвечающих нулевому и единичному биту. Показано, что консервативная граница для данной величины

может быть выражена лишь с использованием одного параметра — максимальной вероятностью вакуумной компоненты в состояниях в побочном канале, которая, в свою очередь, может быть консервативно оценена через среднее число фотонов, т.е. экспериментально измеримый параметр. Были явно построены квантовые состояния, для которых данная консервативная оценка достигается. Полученные расчеты были проведены для поляризационного и фазового кодирования квантовых состояний. Показана эквивалентность оценок для поляризационного и фазового кодирования.

Описан экспериментальный способ определения среднего числа фотонов в активном оптическом побочном канале, связанным с атакой «Trojan Horse». Разработан и собран экспериментальный стенд на основе суперконтинуумного лазера, акустооптических фильтров и детектора одиночных фотонов, позволяющий проводить измерение спектров пропускания пассивных волоконно-оптических компонентов в спектральном диапазоне 1100—1800 нм с рекордно высоким динамическим диапазоном, составившим 120 дБ. Также был разработан и собран экспериментальный стенд, позволяющий проводить оптическую рефлектометрию волоконных систем в спектральном диапазоне 1100—1800 нм с сантиметровым разрешением. Устройство, позволяющее проводить рефлектометрию в широком спектральном диапазоне было представлено впервые.

Разработанные экспериментальные стенды были применены для исследования безопасности реальной системы КРК. Были измерены спектры пропускания оптических элементов защиты от атаки «Trojan Horse» в спектральном диапазоне 1100—1800 нм в прямом и обратном направлении, а именно, оптического изолятора, оптического циркулятора с подключенным зеркалом, WDM-фильтра с постоянным оптическим аттенюатором, а также переменного оптического аттенюатора. Впервые удалось экспериментально получить спектры пропускания волоконных оптических элементов в спектральной области, где их потери превышают 80 дБ. Впервые была проведена рефлектометрия системы КРК с извлеченным блоком защиты от атаки «Trojan Horse» в спектральном диапазоне 1100—1800 нм. Были выявлены максимальные пики отражения от внутренностей передатчика системы КРК в диапазоне 1100—1800 нм. Полученные экспериментальные данные позволили вычислить максимальное среднее число фотонов в импульсах, возвращающихся к нарушителю при проведении атаки, и провести анализ безопасности с учетом

теоретических методов, полученных в рамках настоящей работы. Полученные результаты были обобщены на другие побочные каналы утечки информации.

Результаты второй главы опубликованы в работах [137; 146; 147].

Глава 3. Анализ рисков при изменении параметров системы КРК

Достаточное условие секретности (1.21) при учете побочных каналов, согласно главе 2, позволяет обеспечить безопасность КРК. Это, однако, справедливо лишь при соответствии реальных значений параметров тем значениям, которые используются для вычисления длины секретного ключа (1.21). Как было описано в разделе 1.7.5, нарушитель может попытаться изменить некоторые параметры системы внешним воздействием. Способом защиты от таких действий нарушителя является мониторинг внешнего воздействия или его результатов, исключающее влияние нарушителя на длину секретного ключа. Такой подход существенно отличается от способов защиты от атак по побочным каналам, состоящих в минимизации интенсивности паразитных сигналов и учета их остаточного влияния в длине секретного ключа. В итоге, побочные каналы оказываются охарактеризованы численно, что позволяет судить о рисках, связанных с проведением соответствующих атак, имея конкретные численные метрики. Влияние побочных каналов может быть численно охарактеризовано даже при условии возможного выхода из строя некоторого элемента защиты — для этого лишь следует провести анализ, согласно главе 2, исключив соответствующий элемент защиты из рассмотрения. С другой стороны, имеется возможность определить условия, при которых нарушитель получит весь секретный ключ (например, определить, какие элементы защиты должны выйти из строя), и оценить вероятность такого события, исходя из надежности соответствующих компонентов. Все это позволяет провести комплексный анализ рисков, связанных с наличием побочных каналов, для системы КРК как криптографической системы.

Такой анализ, как кажется, неприменим к изменению параметров при внешнем воздействии нарушителя. Механизм защиты дается качественно: при исправной работе механизмов защиты достаточное условие секретности выполняется, при выходе же из строя — нет. С другой стороны, как было сказано выше, изменение параметров системы нарушителем не относится к атакам в принятой в настоящей работе терминологии; за ними должны следовать действия, направленные на извлечение секретного ключа при проведении комбинированной атаки по побочным каналам и атак на многофотонную компоненту. Последние, как известно, зачастую являются технически нереа-

лизуемыми на сегодняшний день. Для их осуществления может требоваться долгосрочная квантовая память, оптический канал без потерь, или неразрушающие измерения числа фотонов. Возможность проведения атаки PNS — атаки с расщеплением по числу фотонов, ставилась под сомнение в литературе [9; 41]. Отсутствие численной характеризации влияния внешнего воздействия нарушителя с одной стороны, и невозможность проведения ряда атак, использующих эффект от данного воздействия с другой, делает задачу оценки рисков, связанных с данным несовершенством технической реализации, весьма сложной. Могут ли быть созданы реалистичные условия, позволяющие нарушителю получить весь ключ? Существует ли некоторый «запас прочности», позволяющий обеспечить секретность при успешном изменении параметров системы нарушителем? В настоящей главе мы получим ответ на данные вопросы.

3.1 Метод «decoy state» в условиях увеличения интенсивности легитимного излучения

Рассмотрим атаки, приводящие к увеличению среднего числа фотонов в легитимных импульсах. К таковым относятся, LDA — атака с лазерным повреждением, и LSA — атака с затравочным излучением. Пусть в системе КРК применяется метод «decoy state» с двумя состояниями-ловушками, представленный в разделе 1.4. Тогда средние числа фотонов в импульсах изменятся следующим образом:

$$\mu \longrightarrow \tilde{\mu} = \kappa\mu, \tag{3.1}$$

$$\nu_1 \longrightarrow \tilde{\nu}_1 = \kappa\nu_1, \tag{3.2}$$

$$\nu_2 \longrightarrow \tilde{\nu}_2 = \kappa\nu_2, \tag{3.3}$$

где κ — степень увеличения интенсивности излучения. Далее, для определенности, мы будем иметь в виду атаку LDA и связывать увеличение интенсивности света с понижением аттенюации в схеме передатчика системы КРК. Полученные результаты, впрочем, справедливы для любых других способов увеличения среднего числа фотонов.

Как мы договорились ранее, рассмотрим оптимальный вариант метода «decoy state» с использованием вакуумного и ослабленного состояния-ловушки

$\nu_1 \equiv \nu < \mu$ и $\nu_2 = 0$. Оценки параметров, получаемые в результате использования метода, даются выражениями (1.40) — (1.42). Темпы отсчетов Q_μ, Q_ν и Q_0, входящие в состав данных выражений, определяются действиями нарушителя. Рассмотрим различные стратегии Евы для извлечения секретного ключа после увеличения интенсивности излучения.

3.1.1 Атака с расщеплением по числу фотонов при увеличении интенсивности легитимного излучения

Стандартно, при обсуждении рисков, связанных с ростом среднего числа фотонов, обсуждается атака с расщеплением по числу фотонов. Тем не менее, представленный на сегодняшний день в литературе анализ ограничивается построением длины секретного ключа по формуле для достаточного условия секретности, подобной (1.21), с учетом темпов отсчетов, возникающих в следствие увеличения среднего числа фотонов, и сравнением данной величины с действительной длиной секретного ключа, которая должна была бы получиться в расчетах, если бы формулы метода «decoy state» содержали бы реальное значение параметров. Положив, что в обоих случая темпы отсчетов определяются потерями в канале, в работе [120] авторы построили зависимость длины секретного ключа от длины волоконной линии для протокола BB84. Было показано, что метод «decoy state» с неверным значением интенсивностей посылок завышает длину секретного ключа при любой длине линии (при любых потерях), и, следовательно, выработанный ключ нельзя считать секретным.

В самом подходе, однако, содержится противоречие: с одной стороны, оценка длины секретного ключа дается в условиях, при которых темпы отсчетов определяются потерями в канале в отсутствие нарушителя, а с другой стороны, делается вывод о нарушении секретности. Конечно, Ева может заменить канал с потерями на идеальный канал и светоделитель, отщепляя себе часть излучения, при этом сохраняя темпы отсчетов без изменений (например, при проведении атаки «Beam Splitting» или ее вариаций [12]). Однако такое рассмотрение требует явного описания действий нарушителя и оценки его информационного выигрыша (так, например, атака BS позволяет нарушителю получить лишь часть ключа). Поэтому, для анализа рисков безопасности необ-

ходимо рассматривать атаки в том смысле, в котором они были определены в главе 1.

Вернемся к PNS-атаке. При проведении PNS-атаки общего вида, Ева осуществляет неразрушающие измерения числа фотонов n над поступающими к ней посылками. Для простоты оценок, будем считать, что Ева блокирует все посылки кроме тех, для которых результат измерений составил $n = 2$. В случае такого исхода Ева сохраняет состояние одного из фотонов пары в квантовую память, а второй посылает по каналу без потерь Бобу. После процедуры разглашения базисов, Ева безошибочно узнает бит ключа. При штатной работе метода «decoy state» такая атака бы детектировалась, поскольку оценка доли однофотонной компоненты Ω_1 оказалась бы отрицательной. Рассмотрим ситуацию в условиях увеличения среднего числа фотонов. Полагая вероятность темновых отсчетов на стороне Боба пренебрежимо малой, получим:

$$Q_\mu = \sum_{n=0}^{\infty} \frac{\tilde{\mu}^n}{n!} e^{-\tilde{\mu}} Y_n \approx \frac{\tilde{\mu}^2}{2} e^{-\tilde{\mu}} Y_2 \tag{3.4}$$

$$Q_\nu \approx \sum_{n=0}^{\infty} \frac{\tilde{\nu}^n}{n!} e^{-\tilde{\mu}} Y_n \approx \frac{\tilde{\nu}^2}{2} e^{-\tilde{\nu}} Y_2 \tag{3.5}$$

$$Q_0 = 0. \tag{3.6}$$

Здесь мы учли пуассоновскую вероятность для двухфотонной компоненты в лазерном импульсе. Подставим данные выражения в формулу (1.41):

$$Y_1^L = \frac{\mu}{\nu(\mu - \nu)} \left[\frac{(\kappa\nu)^2}{2} e^{-\kappa\nu} Y_2 \, e^{\nu} - \frac{\nu^2}{\mu^2} \frac{(\kappa\mu)^2}{2} e^{-\kappa\mu} Y_2 \, e^{\mu} \right]. \tag{3.7}$$

Найдем условия, при которых доля однофотонной компоненты будет ошибочно оцениваться как положительная величина: $Y_1^L > 0$. Сокращая общие множители, получим:

$$e^{-\nu(\kappa-1)} - e^{-\mu(\kappa-1)} > 0. \tag{3.8}$$

Поскольку $\mu > \nu$, то данное условие выполняется для любого значения $\kappa > 1$. Таким образом, PNS-атака позволяет нарушителю получить весь ключ при сколь угодно малом увеличении среднего числа фотонов в легитимных импульсах. Конечно, на практике, нарушителю, скорее всего, требовалось бы более значительное увеличение интенсивности, поскольку положительная оценка доли однофотонной компоненты сама по себе не гарантирует положительную

длину секретного ключа из-за наличия классической утечки $leak$. Более того, незначительные флуктуации среднего числа фотонов, обычно, включены в оценку величин с использованием доверительных интервалов. Однако не следует полагаться на это при оценке рисков, поскольку увеличение среднего числа фотонов в ряде экспериментальных работ достигало значений в несколько децибел и более [111—113; 120].

Таким образом, при допущении возможности проведения атаки с расщеплением по числу фотонов, риски безопасности оказываются максимальными. Само же это допущение требует существования, как минимум, долгосрочной квантовой памяти и возможности проведения неразрушающих измерений числа фотонов. В парадигме квантовой криптографии устанавливается, что нарушитель способен осуществлять любые действия с квантовыми состояниями, которые не противоречат законам физики. Для реальных криптографических систем такой подход зачастую оказывается избыточен. Так, например, стойкость большого числа криптографических алгоритмов основана на допущениях о вычислительных возможностях нарушителя [148]. Для многих случаев оказывается достаточным обеспечить секретность в допущении о том, что нарушитель обладает лишь существующими на сегодняшний день технологиями. Более того, КРК обладает свойством «вечной стойкости», исключающим возможность получения нарушителем информации об уже распределенных ключах в будущем, при появлении новых технологий [2] (в отличие от алгоритмов, основанных на вычислительной сложности). Поэтому целесообразно оценить риски, связанные с возможностью с осуществимыми на сегодняшний день атаками на многофотонную компоненту.

3.1.2 Атака с расщеплением по числу фотонов без квантовой памяти при увеличения интенсивности легитимного излучения

Исключим из «арсенала» нарушителя долгосрочную квантовую память, которая прежде использовалась им для сохранения состояния отщепленного фотона до момента оглашения базисов. Без квантовой памяти нарушитель вынужден проводить измерения сразу после отщепления. Поскольку базис ему неизвестен, часть измерений будет произведена ошибочно и будет извлечена

лишь доля секретного ключа. Однако Ева может модифицировать свою стратегию. Пусть после проведения измерения числа фотонов она блокирует все посылки кроме тех, для которых $n = 3$. Отщепляя себе 2 фотона, Ева может провести измерение в каждом из двух базисов протокола BB84 — по одному над каждым из отщепленных фотонов. Теперь ей достаточно хранить лишь результат измерений в классической памяти до момента оглашения базисов, после чего выбрать верный результат. Таким образом, трехфотонная PNS-атака позволяет нарушителю получить весь ключ без использования квантовой памяти. Рассмотрим ее влияние на метод «decoy state» при увеличении интенсивности сигналов Алисы. Для этого выразим темпы отсчетов на стороне Боба:

$$Q_\mu = \sum_{n=0}^{\infty} \frac{\tilde{\mu}^n}{n!} e^{-\tilde{\mu}} Y_n \approx \frac{\tilde{\mu}^3}{6} e^{-\tilde{\mu}} Y_3 \tag{3.9}$$

$$Q_\nu = \sum_{n=0}^{\infty} \frac{\tilde{\nu}^n}{n!} e^{-\tilde{\mu}} Y_n \approx \frac{\tilde{\nu}^3}{6} e^{-\tilde{\nu}} Y_3 \tag{3.10}$$

$$Q_0 = 0. \tag{3.11}$$

Формула (1.41) примет вид:

$$Y_1^L = \frac{\mu}{\nu(\mu - \nu)} \left[\frac{(\kappa\nu)^3}{6} e^{-\kappa\nu} Y_3 \, e^{\nu} - \frac{\nu^2}{\mu^2} \frac{(\kappa\mu)^3}{6} e^{-\kappa\mu} Y_3 \, e^{\mu} \right]. \tag{3.12}$$

Вновь найдем условия, при которых доля однофотонной компоненты будет ошибочно оцениваться как положительная величина: $Y_1^L > 0$. Сокращая общие множители, получим:

$$\nu e^{-\nu(\kappa-1)} - \mu e^{-\mu(\kappa-1)} > 0. \tag{3.13}$$

Решая данное неравенство, нетрудно получить условие для κ:

$$\kappa > \kappa_{3\text{ph}} \equiv 1 + \frac{1}{\mu - \nu} \ln \frac{\mu}{\nu}. \tag{3.14}$$

Таким образом, метод «decoy state» начинает ошибочно оценивать долю однофотонной компоненты при проведении трехфотонной PNS-атаки начиная с некоторого порогового значения увеличения интенсивности $\kappa_{3\text{ph}}$. Это качественно отличается от случая двухфотонной PNS-атаки, для которой в идеальном случае метод «decoy state» переставал корректно работать при сколь угодно малом увеличении интенсивности. Несмотря на то что даже трехфотонный вариант атаки с расщеплением по числу фотонов экспериментально недостижим

на сегодняшний день, пороговый характер, как будет показано ниже, сохранится и для других атак, имеющих трехфотонную природу. Данная особенность окажется удобной в контексте анализа реалистичных рисков.

Заметим, что возникновение порогового значения характерно для любой версии PNS-атаки с блокировкой двухфотонной компоненты. Вводя аналогичным образом n-фотонную PNS-атаку, легко получить, что условие $Y_1^L > 0$ выразится как

$$\nu^{n-2}e^{-\nu(\kappa-1)} - \mu^{n-2}e^{-\mu(\kappa-1)} > 0, \tag{3.15}$$

а решение данного неравенства обретет вид

$$\kappa > \kappa_{n\mathrm{ph}} \equiv 1 + \frac{1}{\mu-\nu}\ln\left(\frac{\mu}{\nu}\right)^{n-2} = 1 + \frac{n-2}{\mu-\nu}\ln\frac{\mu}{\nu}. \tag{3.16}$$

Пороговое значение степени увеличения интенсивности растет с увеличением n, а потому использование Евой компонент с $n > 3$ не принесет ей никакого выигрыша. Эта особенность далее будет учтена при модификации атак, реализуемых сегодняшними средствами.

3.1.3 Атака с однозначным различением состояний при увеличении интенсивности легитимного излучения

Атака с расщеплением по числу фотонов нереализуема даже при отказе от квантовой памяти, поскольку для ее выполнения требуются неразрушающие измерения числа фотонов. Однако существует класс атак, позволяющих нарушителю безошибочно определить закодированный бит с использованием лишь линейных оптических элементов и однофотонных детекторов — атаки с однозначным различением состояний, или USD-атаки (unambiguous state discrimination). Для реализации простейшей из них достаточно воспользоваться приемником КРК с пассивным выбором базиса (для определенности, будем считать, что используется поляризационное кодирование, однако все полученные результаты применимы и к другим кодировкам).

Установка для проведения однозначного различения состояний изображена на рисунке 3.1. В ее основе лежит идея, высказанная в работе [12]: пусть

Ева разделит импульс на две половины, и над каждой из них проведет измерение в различном базисе; в случае если сработало три детектора (т.е. один в одном базисе и два в другом), то она однозначно определяет закодированное состояние. Действительно, по наличию двух срабатываний в одном базисе нарушитель может сделать вывод о том, что этот базис неверный, а по результату измерения в другом базисе определить приготовленное состояние. Такой исход измерений называется определенным.

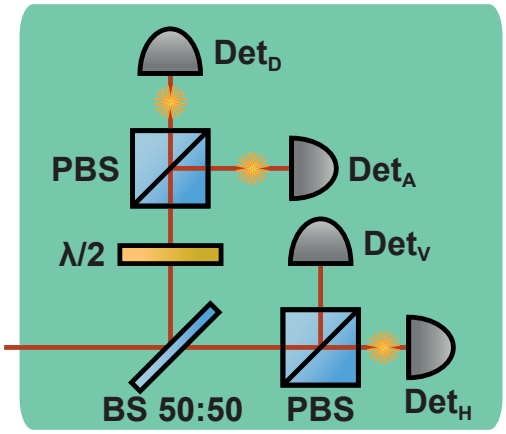


Рисунок 3.1 — Установка для проведения однозначного различения состояний для протокола BB84 с поляризационным кодированием: BS 50:50 — полупрозрачное зеркало, $\lambda/2$ — полуволновая пластинка для поворота поляризации на 45°, PBS — поляризационный светоделитель, $\mathrm{Det}_{\mathrm{H,V,D,A}}$ — ДОФ для горизонтально, вертикально, диагонально и антидиагонально поляризованных состояний, соответственно. Распределение фотонов на рисунке отвечает исходу с горизонтальной поляризацией

При получении определенного исхода измерений Ева готовит классический импульс с интенсивностью, достаточной для практически стопроцентной вероятности его детектирования Бобом. Поляризация данного импульса соответствует исходу измерений Евы и, следовательно, если Боб верно выбирает базис, то все участники получают одинаковый бит ключа. Таким образом, данная атака позволяет Еве получить весь секретный ключ.

Рассмотрим ее влияние на работу метода «decoy state». Темпы отсчетов в данном случае будут определяться вероятностями определенного исхода для

каждого типа состояний:

$$Q_\mu = \left(1 - e^{-\frac{\tilde{\mu}}{2}}\right)\left(1 - e^{-\frac{\tilde{\mu}}{4}}\right)^2, \tag{3.17}$$

$$Q_\nu = \left(1 - e^{-\frac{\tilde{\nu}}{2}}\right)\left(1 - e^{-\frac{\tilde{\nu}}{4}}\right)^2, \tag{3.18}$$

$$Q_0 = 0. \tag{3.19}$$

Здесь мы учли, что вероятность определенного исхода определяется произведением вероятностей прихода хотя бы одного фотона на каждый из трех детекторов, распознающих определенный исход. Эффективность детекторов мы положили равной единице, однако это условие будет позже ослаблено. Мы также пренебрегли вероятностью темновых отсчетов, что оправдано при достаточно больших значениях среднего числа фотонов.

Найдем пороговое значение κ_{USD}, при превышении которого начнется выполнение условия $Y_1^L > 0$, т.е.:

$$Y_1^L(\kappa_{\text{USD}}) = 0. \tag{3.20}$$

Подставляя темпы отсчетов (3.17) — (3.19) в формулу (1.41), получаем следующий вид уравнения (3.20) для определения порогового значения:

$$\frac{\left[1 - \exp\left(-\frac{\tilde{\nu}}{2}\right)\right]\left[1 - \exp\left(-\frac{\tilde{\nu}}{4}\right)\right]^2}{\left[1 - \exp\left(-\frac{\tilde{\mu}}{2}\right)\right]\left[1 - \exp\left(-\frac{\tilde{\mu}}{4}\right)\right]^2}\frac{\mu^2}{\nu^2}e^{-(\mu-\nu)} = 1. \tag{3.21}$$

Преобразуем левую часть уравнения (3.21) и получим трансцендентное уравнение относительно κ_{USD}:

$$\frac{\operatorname{sh}\left(\frac{\kappa_{\text{USD}}\nu}{4}\right)\operatorname{sh}^2\left(\frac{\kappa_{\text{USD}}\nu}{8}\right)}{\operatorname{sh}\left(\frac{\kappa_{\text{USD}}\mu}{4}\right)\operatorname{sh}^2\left(\frac{\kappa_{\text{USD}}\mu}{8}\right)}\frac{\mu^2}{\nu^2}\exp\left[\frac{\kappa_{\text{USD}} - 2}{2}(\mu - \nu)\right] = 1,. \tag{3.22}$$

где мы использовали обозначение $\operatorname{sh}(x) \equiv \frac{e^x - e^{-x}}{2}$ для гиперболического синуса.

Уравнение (3.22) можно решить численно. Однако прежде, имеет смысл рассмотреть его приближенное аналитическое решение. Для этого разложим числитель и знаменатель первой дроби в левый части уравнения (3.22) в ряд Тейлора при малых аргументах (в реальности малости аргумента не будет при

достаточно больших значениях κ_{USD}, однако, как мы увидим, итоговое приближение будет давать достаточно близкую к верной оценку):

$$\frac{\mathrm{sh}\left(\frac{\kappa_{\mathrm{USD}}\nu}{4}\right)\mathrm{sh}^2\left(\frac{\kappa_{\mathrm{USD}}\nu}{8}\right)}{\mathrm{sh}\left(\frac{\kappa_{\mathrm{USD}}\mu}{4}\right)\mathrm{sh}^2\left(\frac{\kappa_{\mathrm{USD}}\mu}{8}\right)} \lesssim \left(\frac{\nu}{\mu}\right)^3. \tag{3.23}$$

Учитывая приближение (3.23), преобразуем левую часть уравнения (3.22):

$$\frac{\nu}{\mu}\exp\left[\frac{\kappa_{\mathrm{USD}}-2}{2}(\mu-\nu)\right] = 1, \tag{3.24}$$

откуда легко выразить приближенное значение порога:

$$\kappa_{\mathrm{USD}} = 2 + \frac{2}{\mu-\nu}\ln\frac{\mu}{\nu} = 2\kappa_{3\mathrm{ph}}. \tag{3.25}$$

Любопытно, что приближенное значение порога для атаки с однозначным различением состояний оказывается вдвое больше порогового значения для трехфотонной PNS-атаки (3.14). Схожесть вида обеих границ подчеркивает общий трехфотонный характер данных атак. Действительно, для определенного исхода USD-измерений требуется наличие как минимум трех фотонов. С другой стороны, n-фотонные срабатывания с $n > 3$ также могут привести к определенному исходу. Как обсуждалось выше, использование таких компонент при PNS-атаке не принесет нарушителю никакого выигрыша, поскольку пороговое значение будет лишь расти с увеличением n. В случае рассмотренной атаки с однозначным различением состояний их наличие увеличивает порог вдвое. Позже мы рассмотрим способ уменьшения вклада многофотонных срабатываний и приближения порога USD-атаки к значению для трехфотонной PNS-атаки.

Для получения точного результата, уравнение (3.22) было также решено численно. Полученные результаты для различных параметров метода «decoy state» приведены в таблице 1. Как видно, приближенная формула (3.25) дает достаточно точную оценку порогового значения κ_{USD}, но ее значение всегда оказывается меньше реального на 1—2 дБ. Это связано с тем, что приближение (3.23) занижает значение левой части уравнения (3.22). Тем не менее, такая оценка оказывается консервативной, что может оправдывать ее использование в некоторых случаях. Сами пороговые значения лежат в пределах от 10 дБ до 20 дБ.

Проиллюстрируем результаты работы метода «decoy state» при проведении USD-атаки в зависимости от степени увеличения интенсивности излучения.

Таблица 1 — Пороговое значение κ_{USD} в децибелах, полученное в результате численного решения уравнения (3.22), и приближенная аналитическая оценка по формуле (3.25) для различных значений параметров метода «decoy state»

	Численное решение	Формула (3.25)
$\mu = 0{,}5$, $\nu = 0{,}1$	11,1 дБ	10,0 дБ
$\mu = 0{,}5$, $\nu = 0{,}01$	14,5 дБ	12,5 дБ
$\mu = 0{,}1$, $\nu = 0{,}01$	18,3 дБ	17,2 дБ

Для этого на рисунке 3.2 приведены зависимости оценок доли однофотонной компоненты Q_1 по формулам (1.40) и (1.41) с учетом темпов отсчетов (3.17) — (3.19) от степени увеличения интенсивности излучения κ для различных параметров метода «decoy state». Видно, что при превышении порогового значения κ_{USD} оценка доли однофотонной компоненты начинает быстро расти. Таким образом, подобрав подходящую степень увеличения интенсивности κ нарушитель может добиться любого значения оценки доли однофотонной компоненты на стороне Боба, включая то, которое бы имело место в отсутствие атаки.

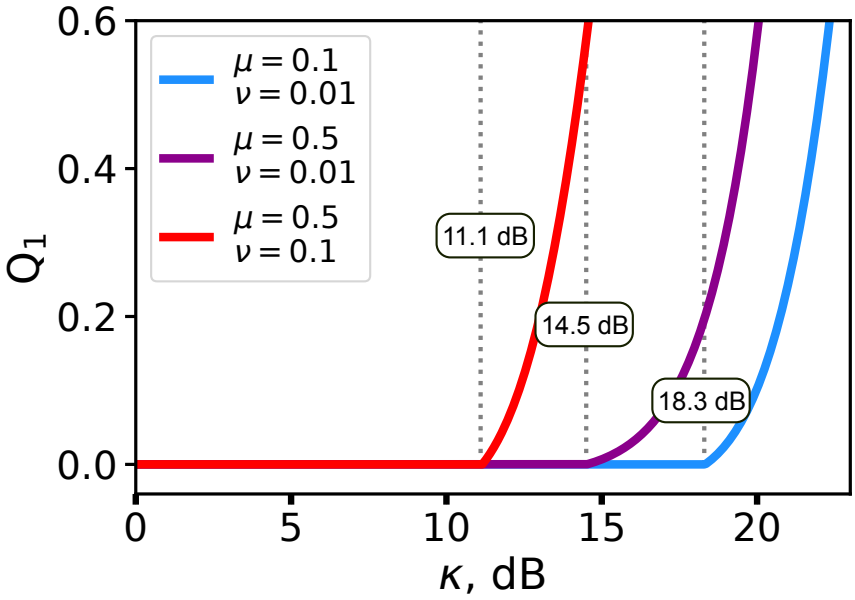


Рисунок 3.2 — Зависимость оценки доли однофотонной компоненты Q_1 по формулам (1.40) и (1.41) от степени увеличения интенсивности излучения κ при проведении USD-атаки для различных параметров метода «decoy state»: $\mu = 0.5$, $\nu = 0.1$ (красный); $\mu = 0.5$, $\nu = 0.01$ (фиолетовый); $\mu = 0.1$, $\nu = 0.01$ (синий). Пороговые значения (11,1 дБ, 14,5 дБ и 18,3 дБ, соответственно) отмечены серыми линиями

Итак, простейшая USD-атака позволяет нарушителю получить весь секретный ключ при превышении некоторого порогового значения степени увеличения интенсивности излучения κ_{USD} с использованием доступных на сегодняшний день технологий. Однако данные пороговые значения вдвое превышают предел трехфотонной PNS-атаки. В следующем разделе мы рассмотрим модификацию USD-атаки, позволяющую приблизить пороговое значение к пределу трехфотонной PNS-атаки.

3.1.4 Модифицированная атака с однозначным различением состояний

Добавим к установке для проведения USD-измерений дополнительный светоделитель с коэффициентом пропускания T (рисунок 3.3). Данный светоделитель отщепляет часть излучения, пропорциональную $1 - T$, которая направляется на ДОФ, регистрирующий «лишние» фотоны, т.е. те, которые могли бы дать вклад в определенный исход при $n > 3$. В случае срабатывания данного детектора нарушитель блокирует посылку, не посылая ее Бобу. В случае отсутствия срабатывания детектора нарушитель продолжает проведение USD-атаки по описанной в разделе 3.1.3 схеме.

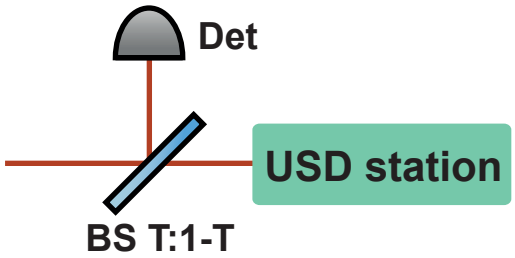


Рисунок 3.3 — Установка для модифицированной USD-атаки: Det — ДОФ для обнаружения «лишних» фотонов, BS T:1-T — асимметричный светоделитель с коэффициентом пропускания T, USD station — установка для USD-измерений из рисунка 3.1

Темпы отсчетов при проведении модифицированной USD-атаки примут вид:

$$Q_\mu = e^{-(1-T)\tilde{\mu}}\left(1-e^{-\frac{T\tilde{\mu}}{2}}\right)\left(1-e^{-\frac{T\tilde{\mu}}{4}}\right)^2, \tag{3.26}$$

$$Q_\nu = e^{-(1-T)\tilde{\nu}}\left(1-e^{-\frac{T\tilde{\nu}}{2}}\right)\left(1-e^{-\frac{T\tilde{\nu}}{4}}\right)^2, \tag{3.27}$$

$$Q_0 = 0. \tag{3.28}$$

Трансцендентное уравнение (3.22) для порогового значения κ_T преобразуется в

$$\frac{\mathrm{sh}\left(\frac{T\kappa_T\nu}{4}\right)\mathrm{sh}^2\left(\frac{T\kappa_T\nu}{4}\right)}{\mathrm{sh}\left(\frac{T\kappa_T\mu}{4}\right)\mathrm{sh}^2\left(\frac{T\kappa_T\mu}{4}\right)}\frac{\mu^2}{\nu^2}\exp\left[(\kappa_T - 1 - \frac{T\kappa_T}{2})(\mu-\nu)\right] = 1. \tag{3.29}$$

Используя приближение (3.23), нетрудно получить приближенное аналитическое выражение для порогового значения:

$$\kappa_T = \frac{2}{2-T}\left(1+\frac{1}{\mu-\nu}\ln\frac{\mu}{\nu}\right) = \frac{\kappa_{\mathrm{USD}}}{2-T} = \frac{2\kappa_{3\mathrm{ph}}}{2-T}. \tag{3.30}$$

Таким образом, порог κ_T при использовании светоделителя с коэффициентом пропускания T меньше единицы оказывается ниже порога κ_{USD} стандартной USD-атаки. При $T \to 0$ пороговое значение стремится к пределу трехфотонной PNS-атаки $\kappa_{3\mathrm{ph}}$. Однако важно заметить, что уменьшение T приведет значительному снижению темпов отсчетов на стороне Боба:

$$\lim_{T\to 0} Q_\mu = \frac{T^3}{32}e^{-\tilde{\mu}}\tilde{\mu}^3. \tag{3.31}$$

Слишком сильное понижение темпов отсчетов по сравнению с ожидаемым может привести к ошибке по времени выполнения на стороне Боба и прерыванию сеанса КРК. Однако при не столь значительном снижении T, Ева может добиться практически любого значения темпа отсчетов на стороне Боба, включая ожидаемое Бобом в отсутствие атаки (рисунок 3.4). Таким образом, подбор правильного значения коэффициента пропускания светоделителя T может позволить нарушителю не только понизить пороговое значение степени увеличения интенсивности, но также и сохранить темпы отсчета на стороне Боба без изменений.

Мы рассмотрели влияние атак на многофотонную компоненту при увеличении интенсивности легитимного излучения на работу метода «decoy state».

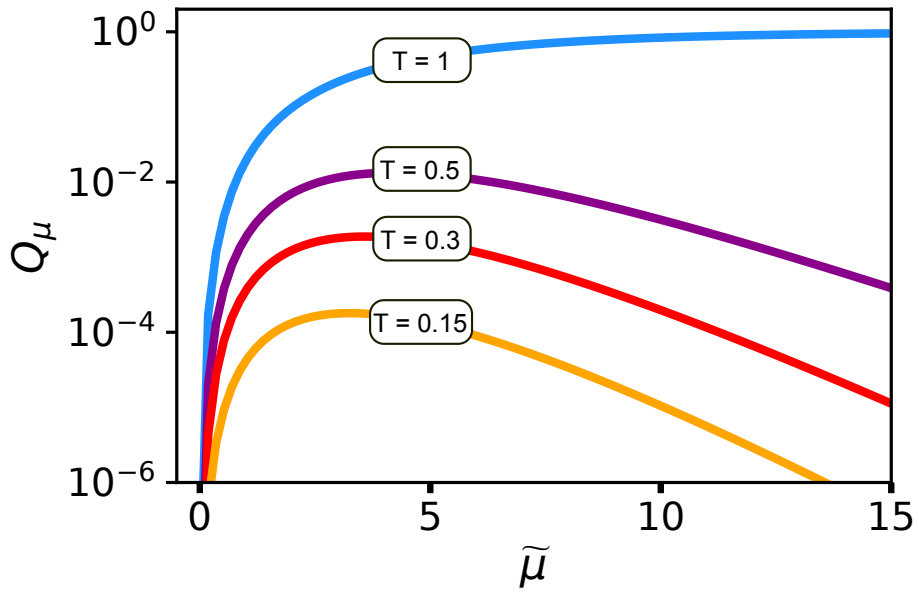


Рисунок 3.4 — Зависимость темпа отсчетов для информационных импульсов от среднего числа фотонов при проведении модифицированной USD-атаки для различных значений коэффициента пропускания светоделителя T: $T = 1$ (синий); $T = 0{,}5$ (фиолетовый); $T = 0{,}3$ (красный); $T = 0{,}15$ (желтый)

Мы получили результаты, показывающие, что метод «decoy state» завышает долю однофотонной компоненты при превышении некоторого порогового значения степени увеличения интенсивности излучения κ, тем самым полностью компрометируя весь вырабатываемый ключ. Тем не менее на практике, такие действия нарушителя, в принципе, могут быть обнаружены легитимными участниками по различным статистическим аномалиям в темпах отсчетов для информационных состояний и состояний-ловушек, а также по темпам двойных срабатываний. Также, мы считали оборудование Евы идеальным, а темновыми шумами на стороне Боба пренебрегли. Чтобы закрыть данные пробелы, в следующем разделе мы рассмотрим более сложную, но все еще достижимую с использованием современных технологий USD-атаку, позволяющую нарушителю полностью сымитировать нормальную работу системы КРК, даже с учетом несовершенств оборудования.

3.2 Имитация нормальной работы системы КРК в условиях увеличения интенсивности легитимного излучения

Метод «decoy state» позволяет легитимным пользователям оценить две величины: долю однофотонной компоненты Ω_1 и вероятность ошибки в однофотонной компоненте E_1. Рассмотренные выше атаки на многофотонную компоненту не вносят дополнительных ошибок, поэтому не влияют на оценку величины E_1. Величина Ω_1, как было показано, может быть воспроизведена Евой в точности, как если бы атака не производилась. Однако в реальных системах КРК может осуществляться более детальный статистический мониторинг наблюдаемых величин. Так, например, до изобретения метода «decoy state» в системах КРК предлагалось использование мониторинга темпов двойных срабатываний, т.е. одновременных отсчетах на двух детекторах при неправильном выборе базиса, наряду с мониторингом обычного темпа отсчетов. При некоторых значениях потерь в канале (как правило, небольших) такой способ позволял обнаружить атаки на многофотонную компоненту [149]. Использование состояний-ловушек открывает возможность мониторинга дополнительных параметров: темпов отсчетов состояний-ловушек и темпов двойных срабатываний состояний-ловушек. Существуют протоколы КРК, использующие эти данные (наряду с измеренными значениями QBER) для определения длины секретного ключа численными методами, рассматривая вычисление информации, доступной нарушителю, как задачу оптимизации [150; 151]. Наконец, при проведении атаки нарушитель может столкнуться с рядом ограничений реальной аппаратуры, усложняющими или даже делающими невозможным незаметное проведение атаки. Так, детекторы Евы и Боба обладают конечной эффективностью и вероятностью темновых отсчетов, в канале имеются потери, а приготовление и измерение состояний легитимными пользователями происходит с конечной точностью. В настоящем разделе мы построим новую стратегию атаки с однозначным различением состояний — USD-атаку с псевдоразличением числа фотонов и последовательно учтем все вышеперечисленные ограничения реального мира.

Рассмотренные выше USD-атаки предполагали отправку классического света для навязывания результата измерения Бобу. Такие импульсы с высоким средним числом фотонов практически неизбежно привели бы к росту

темпов двойных срабатываний в неправильном базисе. Понижение интенсивности импульсов, в свою очередь, приведет уменьшению темпов отсчетов для информационных состояний и состояний-ловушек. Поскольку вероятность определенного исхода при USD-измерениях для состояний-ловушек значительно ниже таковой для информационных состояний, то их темп отсчетов может оказаться ниже значения, ожидаемого легитимными пользователями. Одновременная имитация всех наблюдаемых величин, а именно темпов отсчетов для информационных состояний и состояний-ловушек и темпов двойных срабатываний для информационных состояний и состояний ловушек для описанных выше USD-атак, является, по-видимому, невыполнимой задачей. Это связано с тем, что при успешном измерении нарушитель может лишь определить, какой бит был закодирован, но не понять, является ли измеренное состояние информационным или состоянием-ловушкой. Следовательно, нарушитель не может знать, с какой вероятностью ему следует произвести одиночное или двойное срабатывание на стороне Боба.

Невозможность различить информационные состояния от состояний ловушек лежит в основе доказательства работы метода «decoy state». Физически, данная особенность связана с пуассоновской статистикой по числу фотонов используемых импульсов. Как известно, дисперсия распределения Пуассона равна его математическому ожиданию, т.е., в данном случае, среднему числу фотонов. Это делает распределения с малым средним числом фотонов сильно перекрывающимися. При увеличении среднего числа фотонов распределения начинают «разъезжаться», становясь полностью различимыми в пределе классического интенсивного света. Достижение данного классического предела, однако, потребовало бы увеличение интенсивности излучения на десятки децибел, что представляется нереалистичным с учетом опубликованных результатов по атакам LDA и LSA. Тем не менее, можно попытаться построить измерения, позволяющие различить данные распределения и, как следствие, дать нарушителю указание о дальнейших действиях, вероятностным образом.

Построим следующую схему измерений. Пусть перед установкой для однозначного различения состояний установлен светоделитель с коэффициентом пропускания T, как и в случае модифицированной USD-атаки. Пусть теперь отщепленная доля излучения, пропорциональная $1 - T$ идет на так называемый детектор с псевдоразличением числа фотонов (pseudo-photon-number resolution — PPNR). Так в литературе принято называть набор ДОФ, работаю-

щих в гейгеровском режиме (т.е. позволяющих лишь различать наличие хотя бы одного фотона и их отсутствие), подключенных к выходам из системы светоделителей, обеспечивающих равновероятный приход фотонов на каждый их них [152; 153]. По количеству сработавших детекторов можно сделать предположение о числе фотонов в изначальном состоянии, однако даже в случае использования бесшумных детекторов с единичной эффективностью данное предположение будет верным лишь с некоторой вероятностью, обусловленной биномиальным распределением фотонов по портам светоделителей. На рисунке 3.5а изображен пример реализации рассматриваемой схемы, где в качестве PPNR-детектора используется набор из трех ДОФ с двумя светоделителями, обеспечивающими равновероятное распределение фотонов по их выходам. В зависимости от одного из четырех исходов на PPNR-детекторе (0, 1, 2 или 3 срабатывания) Ева принимает решение о посылке того или иного сигнала с использованием своей передающей станции, изображенной на рисунке 3.5б. Она может с некоторой вероятностью послать одиночный фотон или ослабленный лазерный импульс, на который будет наложена поляризация в соответствии с результатом USD-измерения. Вероятности и интенсивности отправляемых состояний могут регулироваться модулятором интенсивности.

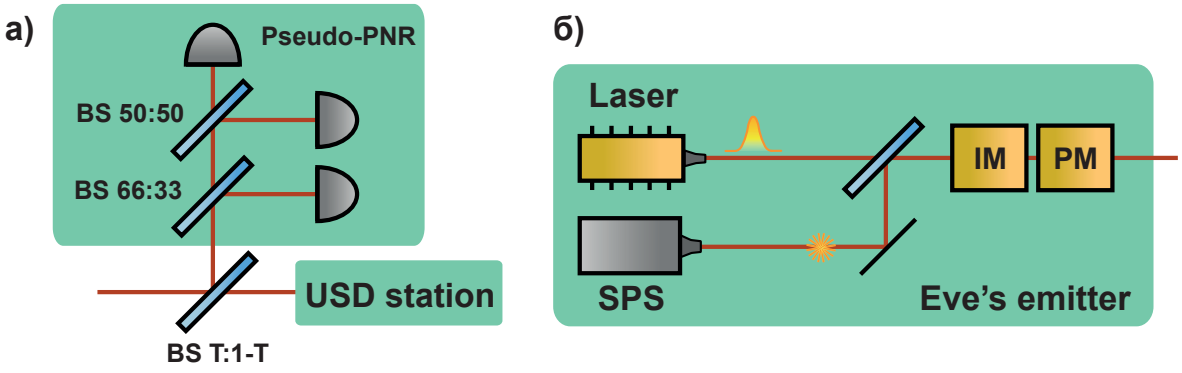


Рисунок 3.5 — а) Установка Евы для PPNR USD-измерений: BS — светоделитель (рядом указан коэффициент деления), USD station — установка для USD-изерений из рисунка 3.1; б) передатчик Евы: Laser — источник лазерных импульсов, SPS — источник одиночных фотонов, IM — модулятор интенсивности, PM — модулятор поляризации

Найдем условия, при которых Ева может «подделать» все наблюдаемые параметры на стороне Боба. Ожидаемые темпы отсчетов в отсутствие Евы опре-

деляются потерями в канале, и параметрами детекторов Боба:

$$Q_\mu \approx \mu\eta\eta_B + p_{\text{dcr}}, \tag{3.32}$$

$$Q_\nu \approx \nu\eta\eta_B + p_{\text{dcr}}, \tag{3.33}$$

$$Q_\mu^{(2)} \approx \left(\frac{\mu\eta\eta_B}{2}\right)^2 + \mu\eta\eta_B\, p_{\text{dcr}} + p_{\text{dcr}}^2, \tag{3.34}$$

$$Q_\nu^{(2)} \approx \left(\frac{\nu\eta\eta_B}{2}\right)^2 + \nu\eta\eta_B\, p_{\text{dcr}} + p_{\text{dcr}}^2, \tag{3.35}$$

где $Q_\mu^{(2)}$ и $Q_\nu^{(2)}$ — темпы двойных срабатываний для информационных состояний и состояний-ловушек, соответственно, η — коэффициент пропускания канала между Алисой и Бобом, η_B — квантовая эффективность ДОФ Боба, p_{dcr} — вероятность темновых отсчетов на ДОФ Боба.

Обратим внимание на то, что темпы отсчетов, как и темпы двойных срабатываний, для вакуумных посылок не изменятся при проведении любой USD-атаки, поскольку вероятность одновременного срабатывания трех детекторов на стороне Евы в отсутствие излучения примерно равна p_{dcr}^3 (для удобства, положим вероятность темновых отсчетов на детекторах Евы равной таковой на детекторах Боба). В силу выполнения условия $p_{\text{dcr}} \gg p_{\text{dcr}}^3$ отсчеты, навязанные Евой будут незаметны на фоне собственных темновых шумов Боба.

Имея в распоряжении четыре возможных исхода PPNR-измерения, Ева может приписать каждому из них одно из четырех событий, которые она будет пытаться навязать. Исход, отвечающий 0 или 2 фотонам, она может ассоциировать с одиночным срабатыванием, порожденным информационным состоянием и состоянием-ловушкой, соответственно. Получив такой исход, она дает команду на передатчик, чтобы отправить одиночный фотон с вероятностью $p_{\nu,1}/\eta_B$ и $p_{\mu,1}/\eta_B$, соответственно (что приведет к вероятностям детектирования фотона Бобом $p_{\nu,1}$ и $p_{\mu,1}$, соответственно). Исход, отвечающий 1 или 3 фотонам, она может ассоциировать с двойными срабатываниями, порожденными информационным состоянием и состоянием-ловушкой, соответственно. В таком случае, она дает команду на передатчик, чтобы отправить лазерный импульс со средним числом фотонов ν' и μ', соответственно. В результате, темпы отсчетов на стороне Боба примут следующий вид:

$$Q_\mu = Q_\mu^{\text{USD}}\Big(P_\mu(0)\, p_{\nu,1} + P_\mu(1)\, p_{\nu'} + P_\mu(2)\, p_{\mu,1} + P_\mu(3)\, p_{\mu'}\Big) + p_{dcr}, \tag{3.36}$$

$$Q_\nu = Q_\nu^{\text{USD}}\Big(P_\nu(0)\, p_{\nu,1} + P_\nu(1)\, p_{\nu'} + P_\nu(2)\, p_{\mu,1} + P_\nu(3)\, p_{\mu'}\Big) + p_{dcr}, \tag{3.37}$$

$$Q_{\mu}^{(2)} = Q_{\mu}^{\mathrm{USD}}\Big(P_{\mu}(0)\,p_{\nu,1}\,p_{dcr} + P_{\mu}(1)\,p_{\nu'}^{(2)} + \\ + P_{\mu}(2)\,p_{\mu,1}\,p_{dcr} + P_{\mu}(3)\,p_{\mu'}^{(2)}\Big) + p_{dcr}^{2}, \tag{3.38}$$

$$Q_{\nu}^{(2)} = Q_{\nu}^{\mathrm{USD}}\Big(P_{\nu}(0)\,p_{\nu,1}\,p_{dcr} + P_{\nu}(1)\,p_{\nu'}^{(2)} \\ + P_{\nu}(2)\,p_{\mu,1}\,p_{dcr} + P_{\nu}(3)\,p_{\mu'}^{(2)}\Big) + p_{dcr}^{2}, \tag{3.39}$$

где

$$Q_{\mu}^{\mathrm{USD}} = \left(1 - e^{-\frac{T\tilde{\mu}\eta_E}{2}}\right)\left(1 - e^{-\frac{T\tilde{\mu}\eta_E}{4}}\right)^2, \tag{3.40}$$

$$Q_{\nu}^{\mathrm{USD}} = \left(1 - e^{-\frac{T\tilde{\nu}\eta_E}{2}}\right)\left(1 - e^{-\frac{T\tilde{\nu}\eta_E}{4}}\right)^2 \tag{3.41}$$

представляют собой вероятности определенного исхода на установке для USD-измерений для информационного состояния и состояния-ловушки, соответственно;

$$P_{\mu}(k) = C_3^k\left(1 - e^{-\frac{(1-T)\tilde{\mu}\eta_E}{3}}\right)^k\left(e^{-\frac{(1-T)\tilde{\mu}\eta_E}{3}}\right)^{1-k}, \tag{3.42}$$

$$P_{\nu}(k) = C_3^k\left(1 - e^{-\frac{(1-T)\tilde{\nu}\eta_E}{3}}\right)^k\left(e^{-\frac{(1-T)\tilde{\nu}\eta_E}{3}}\right)^{1-k} \tag{3.43}$$

представляют собой биномиальные вероятности k-фотонного исхода на PPNR-детекторе для информационного состояния и состояния-ловушки, соответственно;

$$p_{\mu'} = 1 - e^{-\mu'\eta_B}, \tag{3.44}$$

$$p_{\nu'} = 1 - e^{-\nu'\eta_B} \tag{3.45}$$

представляют собой вероятности одиночных срабатываний на стороне Боба при отправке Евой лазерного импульса со средним числом фотонов μ' и ν', соответственно;

$$p_{\mu'}^{(2)} = \left(1 - e^{-\frac{\mu'\eta_B}{2}}\right)^2, \tag{3.46}$$

$$p_{\nu'}^{(2)} = \left(1 - e^{-\frac{\nu'\eta_B}{2}}\right)^2 \tag{3.47}$$

представляют собой вероятности двойных срабатываний на стороне Боба при отправке Евой лазерного импульса со средним числом фотонов μ' и ν', соответственно; η_E — квантовая эффективность ДОФ Евы. Здесь для удобства мы

предположили, что Ева использует одинаковые детекторы. Мы также пренебрегли темновыми отсчетами на стороне Евы, поскольку их вероятность много меньше вероятности срабатывания детектора под воздействием пришедшего фотона, т.к. на установку приходит свет с увеличенной интенсивностью.

Задача Евы состоит в том, чтобы подобрать такие параметры атаки (вероятности отправки одиночных фотонов, интенсивности лазерных импульсов и коэффициент пропускания светоделителя), чтобы темпы отсчетов (3.36) — (3.39) получились равными (или почти равными) ожидаемым (3.32) — (3.35). Попарно приравнивая данные выражения, мы получаем систему уравнений с четырьмя неизвестными (будем считать величину T параметром уравнения). Вычитая из второй пары уравнений первую, домножив ее на p_{dcr}, получим систему линейных уравнений, имеющую вид

$$Q_{\mu}^{\text{USD}}\,P_{\mu}(1)\left(p_{\nu'}^{(2)}-p_{\nu'}\,p_{dcr}\right)+Q_{\mu}^{\text{USD}}\,P_{\mu}(3)\left(p_{\mu'}^{(2)}-p_{\mu'}\,p_{dcr}\right)=\left(\frac{\mu\eta\eta_B}{2}\right)^2, \tag{3.48}$$

$$Q_{\nu}^{\text{USD}}\,P_{\nu}(1)\left(p_{\nu'}^{(2)}-p_{\nu'}\,p_{dcr}\right)+Q_{\nu}^{\text{USD}}\,P_{\nu}(3)\left(p_{\mu'}^{(2)}-p_{\mu'}\,p_{dcr}\right)=\left(\frac{\nu\eta\eta_B}{2}\right)^2. \tag{3.49}$$

Решим ее с помощью метода Крамера:

$$p_{\nu'}^{(2)}-p_{\nu'}\,p_{\text{dcr}}=\frac{\Delta_1}{\Delta}, \tag{3.50}$$

$$p_{\mu'}^{(2)}-p_{\mu'}\,p_{\text{dcr}}=\frac{\Delta_2}{\Delta}, \tag{3.51}$$

где Δ — определитель матрицы системы уравнений:

$$\Delta=Q_{\mu}^{\text{USD}}\,P_{\mu}(1)\,Q_{\nu}^{\text{USD}}\,P_{\nu}(3)-Q_{\mu}^{\text{USD}}\,P_{\mu}(3)\,Q_{\nu}^{\text{USD}}\,P_{\nu}(1), \tag{3.52}$$

а Δ_1 и Δ_2 — вспомогательные определители:

$$\Delta_1=\left(\frac{\mu\eta\eta_B}{2}\right)^2 Q_{\nu}^{\text{USD}}\,P_{\nu}(3)-\left(\frac{\nu\eta\eta_B}{2}\right)^2 Q_{\mu}^{\text{USD}}\,P_{\mu}(3), \tag{3.53}$$

$$\Delta_2=\left(\frac{\mu\eta\eta_B}{2}\right)^2 Q_{\mu}^{\text{USD}}\,P_{\mu}(1)-\left(\frac{\nu\eta\eta_B}{2}\right)^2 Q_{\nu}^{\text{USD}}\,P_{\nu}(1). \tag{3.54}$$

Выражения (3.50) и (3.51) дают связь между вероятностями одиночных и двойных срабатываний. С другой стороны, связь между ними дается выражениями (3.44) — (3.47):

$$p_{\mu'}=2\sqrt{p_{\mu'}^{(2)}}-p_{\mu'}^{(2)}, \tag{3.55}$$

$$p_{\nu'}=2\sqrt{p_{\nu'}^{(2)}}-p_{\nu'}^{(2)}. \tag{3.56}$$

Подставив выражения (3.55) и (3.56) в формулы (3.51) и (3.50) мы получим квадратные уравнения относительно $\sqrt{p^{(2)}_{\mu'}}$ и $\sqrt{p^{(2)}_{\nu'}}$:

$$p^{(2)}_{\mu'}\,(1+p_{\text{dcr}}) - 2\,p_{\text{dcr}}\sqrt{p^{(2)}_{\mu'}} - \frac{\Delta_2}{\Delta} = 0, \tag{3.57}$$

$$p^{(2)}_{\nu'}\,(1+p_{\text{dcr}}) - 2\,p_{\text{dcr}}\sqrt{p^{(2)}_{\nu'}} - \frac{\Delta_1}{\Delta} = 0. \tag{3.58}$$

Решая данные уравнения и отбрасывая отрицательные корни, получим:

$$\sqrt{p^{(2)}_{\mu'}} = \frac{p_{\text{dcr}} + \sqrt{p^2_{\text{dcr}} + (1+p_{\text{dcr}})\frac{\Delta_2}{\Delta}}}{1+p_{\text{dcr}}}, \tag{3.59}$$

$$\sqrt{p^{(2)}_{\nu'}} = \frac{p_{\text{dcr}} + \sqrt{p^2_{\text{dcr}} + (1+p_{\text{dcr}})\frac{\Delta_1}{\Delta}}}{1+p_{\text{dcr}}}. \tag{3.60}$$

Пользуясь выражениями (3.46) и (3.47), окончательно получим интенсивности импульсов, посылаемых Евой:

$$\mu' = -\frac{2}{\eta_B}\ln\left(1-\sqrt{p^{(2)}_{\mu'}}\right), \tag{3.61}$$

$$\nu' = -\frac{2}{\eta_B}\ln\left(1-\sqrt{p^{(2)}_{\nu'}}\right). \tag{3.62}$$

Рассмотрим теперь вторую систему линейных уравнений, образованную приравниванием выражений (3.32) и (3.33) с выражениями (3.36) и (3.37). Величины $p_{\mu'}$ и $p_{\nu'}$ теперь известны из решения первой системы и могут быть перенесены в правую часть уравнений:

$$Q^{\text{USD}}_{\mu}\Big(P_{\mu}(0)\,p_{\nu,1} + P_{\mu}(2)\,p_{\mu,1}\Big) = \mu\eta\eta_B - Q^{\text{USD}}_{\mu}\,P_{\mu}(1)\,p_{\nu'} - Q^{\text{USD}}_{\mu}\,P_{\mu}(3)\,p_{\mu'}, \tag{3.63}$$

$$Q^{\text{USD}}_{\nu}\Big(P_{\nu}(0)\,p_{\nu,1} + P_{\nu}(2)\,p_{\mu,1}\Big) = \nu\eta\eta_B - Q^{\text{USD}}_{\mu}\,P_{\nu}(1)\,p_{\nu'} - Q^{\text{USD}}_{\mu}\,P_{\nu}(3)\,p_{\mu'}. \tag{3.64}$$

Снова воспользуемся методом Крамера:

$$p_{\nu,1} = \frac{\overline{\Delta}_1}{\overline{\Delta}}, \tag{3.65}$$

$$p_{\mu,1} = \frac{\overline{\Delta}_2}{\overline{\Delta}}, \tag{3.66}$$

где $\overline{\Delta}$ — определитель матрицы системы уравнений:

$$\overline{\Delta} = Q_{\mu}^{\mathrm{USD}} P_{\mu}(0) Q_{\nu}^{\mathrm{USD}} P_{\nu}(2) - Q_{\mu}^{\mathrm{USD}} P_{\mu}(2) Q_{\nu}^{\mathrm{USD}} P_{\nu}(0), \tag{3.67}$$

а $\overline{\Delta}_1$ и $\overline{\Delta}_2$ — вспомогательные определители:

$$\overline{\Delta}_1 = C_1 Q_{\nu}^{\mathrm{USD}} P_{\nu}(2) - C_2 Q_{\mu}^{\mathrm{USD}} P_{\mu}(2), \tag{3.68}$$

$$\overline{\Delta}_2 = C_1 Q_{\mu}^{\mathrm{USD}} P_{\mu}(0) - C_2 Q_{\nu}^{\mathrm{USD}} P_{\nu}(0), \tag{3.69}$$

где C_1 и C_2 обозначают правые части уравнений (3.63) и (3.64):

$$C_1 \equiv \mu\eta\eta_B - Q_{\mu}^{\mathrm{USD}} P_{\mu}(1) p_{\nu'} - Q_{\mu}^{\mathrm{USD}} P_{\mu}(3) p_{\mu'}, \tag{3.70}$$

$$C_2 \equiv \nu\eta\eta_B - Q_{\mu}^{\mathrm{USD}} P_{\nu}(1) p_{\nu'} - Q_{\mu}^{\mathrm{USD}} P_{\nu}(3) p_{\mu'}. \tag{3.71}$$

Итак, мы полностью решили систему уравнений и нашли значения для вероятностей $p_{\nu,1}$ и $p_{\mu,1}$, а также для интенсивностей ν' и μ'. Однако, чтобы решение было физически осмысленно, должны выполнятся следующие условия:

$$p_{\mu,1} \in [0, \eta_B];\ p_{\mu'} \in [0,1];\ p_{\mu'}^{(2)} \in [0,1]; \tag{3.72}$$

$$p_{\nu,1} \in [0, \eta_B];\ p_{\nu'} \in [0,1];\ p_{\nu'}^{(2)} \in [0,1]. \tag{3.73}$$

Данные условия не могут быть выполнены для произвольного значения κ, а начинают выполняться лишь по достижении некоторого порогового значения. Заметим, однако, что на практике Еве не требуется имитировать статистику детектирования на стороне Боба идеально точно. Если имитируемые темпы отсчетов отличаются от ожидаемых лишь на некоторую небольшую величину, то легитимные пользователи, скорее всего, не заметят вмешательства нарушителя. Исходя из этого, найдем пороговые значения увеличения интенсивности κ_{PPNR}, для которых отношение имитируемых темпов отсчетов (3.36) — (3.39) к ожидаемым (3.32) — (3.35) отличается от единицы на некоторую величину, не превышающую ε.

Выполним данную процедуру численно. Для этого зададим отрезок возможных значений κ, например, от 0 дБ до 30 дБ с некоторым дискретным шагом, и для каждого из них запустим алгоритм поиска минимального значения разности отношений имитируемых к ожидаемым темпов отсчетов и единицы по параметру T, используя метод золотого сечения с условием остановки по достижении ε. При этом вероятности, входящие в выражения для имитируемых темпов отсчетов, будут вычисляться согласно решению системы

уравнений, т.е. выражениям (3.50), (3.51), (3.65) и (3.66). Если условия (3.72) и (3.73) для них не выполняются, то применим к ним операцию «обрезки», приравняв их к крайнему значению отрезка. После выполнения алгоритма, определим минимальное значение κ, для которого поиск минимума завершился успехом. Это значение и будет искомым пороговым значением κ_{PPNR}. Соответствующее ему значение коэффициента пропускания светоделителя обозначим T_o.

Численное моделирование было проведено для различных значений пропускания канала η. Результаты моделирования для идеального случая, т.е. при единичной эффективности детекторов Евы $\eta_E = 1$, а также при отсутствии темновых шумов на стороне Боба $p_{\mathrm{dcr}} = 0$, изображены на рисунке 3.6б. Невязка ε была установлена равной 10%, квантовая эффективность детекторов Боба $\eta_B = 0{,}1$. Соответствующие минимуму требуемого увеличения интенсивности величины коэффициента пропускания светоделителя T_o изображены на рисунке 3.6а. Видно, что при увеличении потерь в канале, пороговое значение κ_{PPNR} уменьшается и при малых величинах пропускания канала лежит достаточно близко к значениям, полученным при рассмотрении стандартной USD-атаки (см. таблицу 1). В окрестности нулевых потерь, напротив, Еве дополнительно требуется 2—3 дБ для достижения порога. Похожий эффект наблюдается и для стандартной USD-атаки: на рисунке 3.2 видно, что после достижения порога κ_{USD} Еве дополнительно требуется 2—3 дБ для того, чтобы сымитировать значение доли однофотонной компоненты, ожидаемой при малых потерях.

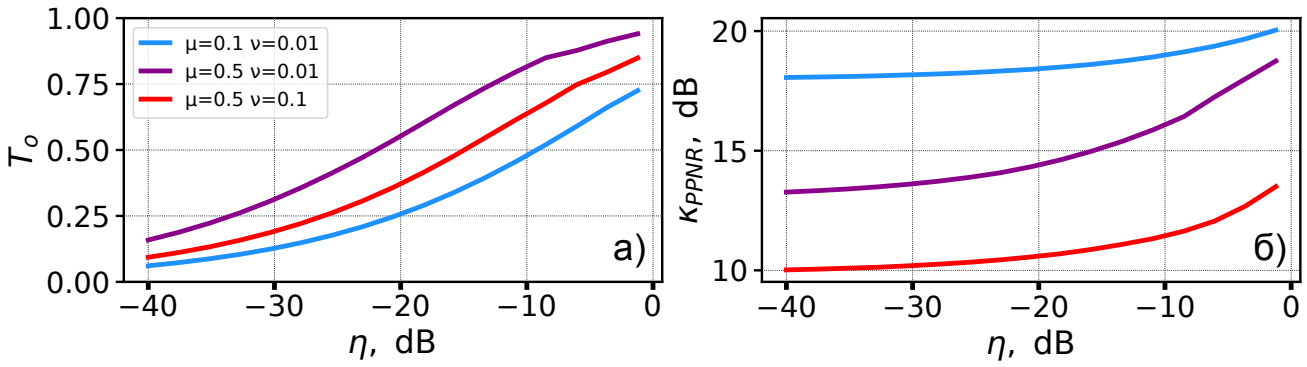


Рисунок 3.6 — а) Зависимость оптимального значения коэффициента пропускания светоделителя T_o от пропускания канала η; б) зависимость порогового значение увеличения интенсивности для PPNR USD-атаки κ_{PPNR} от пропускания канала η для различных параметров метода «decoy state»: $\mu = 0{,}5$, $\nu = 0{,}1$ (красный); $\mu = 0{,}5$, $\nu = 0{,}01$ (фиолетовый); $\mu = 0{,}1$, $\nu = 0{,}01$ (синий).

Рассмотрим, что будет происходить при учете темновых шумов на стороне Боба. Для этого повторим численные расчеты для различных значений вероятности темновых отсчетов p_{dcr}. Результаты моделирования изображены на рисунке 3.7а.

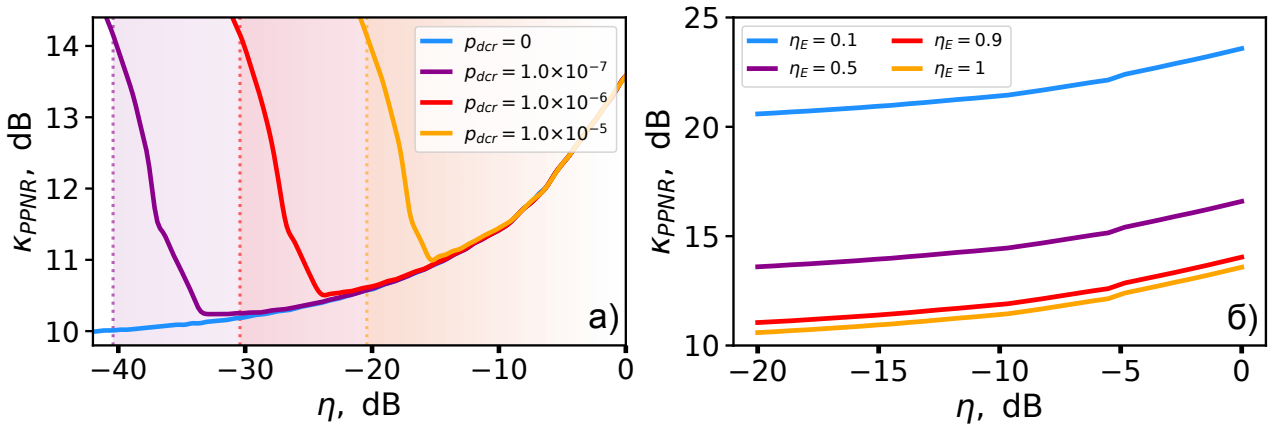


Рисунок 3.7 — а) Зависимость порогового значения увеличения интенсивности для PPNR USD-атаки κ_{PPNR} от пропускания канала η для различных вероятностей темновых отсчетов на стороне Боба ($p_{dcr} = 0$ — синий, $p_{dcr} = 10^{-7}$ — фиолетовый, $p_{dcr} = 10^{-6}$ — красный, $p_{dcr} = 10^{-5}$ — оранжевый); $\eta_E = 1$, $\eta_B = 0{,}1$; пунктирные линии для каждого значения вероятности темновых отсчетов соответствуют критическим потерям для протокола «decoy state» BB84, градиентная заливка показывает области для каждого значения вероятности темновых отсчетов, в которых возможна выработка секретного ключа; б) зависимость порогового значения увеличения интенсивности для PPNR USD-атаки κ_{PPNR} от пропускания канала η для различных квантовых эффективностей детекторов Евы ($\eta_E = 0{,}1$ — синий, $\eta_E = 0{,}5$ — фиолетовый, $\eta_E = 0{,}9$ — красный, $\eta_E = 1$ — оранжевый). Параметры метода «decoy state»: $\mu = 0{,}5$, $\nu = 0{,}1$.

Видно, что при увеличении вероятности темновых отсчетов зависимость порогового значения κ_{PPNR} от пропускания канала совпадает с идеальным случаем вплоть до некоторого критического значения потерь, после которых κ_{PPNR} начинает резко расти. Это связано с тем фактом, что при больших потерях вклад темновых отсчетов в общую статистику детектирования становится существенным и усложняет Еве задачу имитации наблюдаемых величин. Однако нетрудно показать, что данная особенность никак не усложняет проведение атаки в целом. Как следует из формулы достаточного условия секретности (1.21), выработка секретного ключа в протоколе BB84 возможна вплоть до достижения некоторого критического значения уровня ошибки QBER. В идеальном

случае, для протокола BB84 величина критического уровня ошибки составляет примерно 11%. Как следует из выражения (1.42), вероятность ошибки в однофотонной компоненте преимущественно зависит от значения QBER для состояний-ловушек. В отсутствие нарушителя при достаточно больших потерях ошибочные измерения будут производиться, в основном, из-за темновых отсчетов. Следовательно, существует критический величина пропускания канала η_c, определяющая соотношение сигнал—шум для состояний-ловушек в 1/0,11, при которой выработка секретного ключа становится в принципе невозможной:

$$\eta_c = \frac{p_{\text{dcr}}}{0{,}11\,\nu\,\eta_B}. \tag{3.74}$$

Таким образом, выработка ключа в отсутствие Евы в принципе возможна лишь в области значений пропускания канала $\eta > \eta_c$. Данные области выделены градиентной заливкой на рисунке 3.7а. В пределах этой области пороговое значение κ_{PPNR} отклоняется от идеального случая не более чем на 4 дБ в окрестности критического значения потерь, начиная испытывать рост примерно за 5 дБ до достижения η_c.

Наконец, рассмотрим влияние квантовой эффективности детекторов Евы η_E на пороговое значение κ_{PPNR}. Результаты численных расчетов для различных значений η_E изображены на рисунке 3.7б. Видно, что уменьшение квантовой эффективности детекторов Евы приводит к пропорциональному росту порогового значения κ_{PPNR}. Данный эффект обусловлен тем, что η_E входит в формулы для вероятностей детектирования Евы как множитель перед κ, т.е. уменьшение η_E эквивалентно уменьшению интенсивности излучения, приходящего на установку Евы:

$$\tilde{\mu} \to \tilde{\mu} \cdot \eta_E = \mu \cdot \kappa\eta_E, \tag{3.75}$$

$$\tilde{\nu} \to \tilde{\nu} \cdot \eta_E = \nu \cdot \kappa\eta_E. \tag{3.76}$$

При низких значениях квантовой эффективности Ева вынуждена добиваться большего увеличения интенсивности для достижения порога. Так, например, при $\eta_E = 0.5$ пороговое значение κ_{PPNR} увеличивается примерно на 10 дБ по сравнению с идеальным случаем $\eta_E = 1$. При этом форма зависимости от пропускания канала остается неизменной.

Таким образом, мы построили атаку с однозначным различением состояний, использующую детектор с псевдоразличением числа фотонов, позволяющую полностью сымитировать все наблюдаемые параметры на стороне Боба

при достижении некоторого порогового значения увеличения интенсивности излучения, приходящего на установку Евы. Мы показали, что такая атака возможна в условиях потерь в канале, неидеальных детекторов Евы, а также при темновых шумах на стороне Боба. Получив конкретные численные оценки требуемых значений увеличения интенсивности, перейдем к анализу практических рисков, связанных с возможностью проведения описанных атак.

3.3 Анализ практических рисков в условиях увеличения интенсивности легитимного излучения системы КРК

Мы рассмотрели несколько классов атак на многофотонную компоненту для протокола BB84 с использованием метода «decoy state», позволяющих нарушителю получить весь секретный ключ при повышении интенсивности легитимного излучения системы КРК. Традиционно, риски безопасности в условиях увеличения интенсивности излучения, например в следствие проведения атаки с лазерным повреждением, связывают с возможностью проведения PNS-атаки. Действительно, как было показано в разделе 3.1.2, PNS-атака приводит ошибочной оценке доли однофотонной компоненты как положительной величины начиная со сколь угодно малой степени увеличения интенсивности. Однако практическая нереализуемость данной атаки, по-видимому, приводила исследователей к выводу о том, что риски безопасности, связанные, в частности, с лазерным повреждением, не более существенны, чем остальные. Так, например, в официальном стандарте по безопасности систем КРК, опубликованным Европейским институтом по стандартизации в области телекоммуникаций (ETSI) [154], риски безопасности, связанные с лазерным повреждением, отдельно не рассматриваются, но указано, что соответствующие атаки, по мнению авторов, не относятся к более опасным, чем рассмотренные в документе.

К другим примерам можно отнести предпринятые в работе [143] попытки оценивания рисков, связанных с каждой потенциальной уязвимостью, рассмотренных при исследовании системы КРК в рамках подготовки к сертификационным исследованиям. Авторы предложили оценивать риски по трем критериям: вероятность возникновения уязвимости, технологическая возможность проведения атаки, а также величина утечки информации. Для того,

чтобы уязвимость получила максимальную оценку рисков, должны иметься сведения о ее вероятном возникновении в достаточном числе опубликованных случаев, атака должна быть практически реализуема с использованием доступных на сегодняшний день технологий, а также должна приводить к утечке всего секретного ключа. Атака LDA получила лишь 2 балла из 3, поскольку, по мнению авторов, практическая реализуемость атаки, дающей нарушителю весь секретный ключ, требует дополнительных исследований.

Вывод авторов [143] подталкивает к вопросу о том, могут ли риски, связанные с LDA, получить максимальную оценку, или же некоторые из критериев оказываются взаимоисключающими? Для ответа на этот вопрос следует рассмотреть различные сценарии проведения таких атак. Очевидно, что при значительном увеличении интенсивности легитимного излучения на несколько десятков децибел, отправляемые состояния по-существу перестанут быть квантовыми и станут полностью различимы, что безусловно приведет к полной утечке ключа при проведении классических измерений. Однако такой сценарий представляется неправдоподобным, поскольку максимальная степень просветления оптических аттенюаторов, наблюдавшаяся в экспериментах по лазерному повреждению составляла примерно 14,5 дБ, а чаще всего она не превышала 10 дБ [111]. Следовательно, такой сценарий получает 2 балла из 3 по критериям из работы [143]. Другой вариант — проведение PNS-атаки, для которой, как мы показали, достаточно лишь небольшого увеличения интенсивности излучения, которое часто достигалось в экспериментах по лазерному повреждению. Однако, как уже отмечалось, практическая реализуемость PNS-атаки вызывает серьезные сомнения, что снова вынуждает оценить данную возможность в 2 балла из 3. Наконец, существует возможность проведения атак, для которых квантовая память и неразрушающие измерения не требуются. Так, например, нарушитель мог бы воспользоваться вариантом BS-атаки, проводя измерения над излишком излучения, возникающего при увеличении интенсивности. Однако, BS-атаки не позволяют нарушителю получить весь ключ, что опять приводит к оценке в 2 балла из 3.

В настоящей работе мы показали, что атаки, удовлетворяющие всем трем критериям одновременно, на самом деле, существуют — это атаки с однозначным различением состояний. Мы показали, что при выполнении некоторых условий, данные атаки позволяют нарушителю получить весь секретный ключ. Рассмотрим эти условия подробнее и обсудим их практическую достижимость.

Во-первых, для проведения атак с однозначным различением состояний нарушителю требуется степень увеличения интенсивности излучения, превышающая некоторый порог. При использовании Евой детекторов с единичной квантовой эффективностью, данный порог для рассмотренных USD-атак лежит в диапазоне 10—20 дБ в зависимости от используемых параметров метода «decoy state». Просветление оптических аттенюаторов, используемых в системах КРК превышало величину в 10 дБ в нескольких опубликованных исследованиях по лазерному повреждению [111—113], что свидетельствует о практической достижимости данного условия.

Во-вторых, в рассмотренные нами сценарии атак предполагали возможность нарушителя подключиться непосредственно к выходу из передатчика системы КРК, во избежание дополнительных потерь при распространении излучения по оптическому каналу до измерительной станции Евы. На практике данное условие не всегда может быть соблюдено, поскольку система КРК может быть размещена внутри контролируемой зоны так, что нарушитель получит доступ к оптическому каналу лишь на некотором удалении от передатчика. Положим, эта величина составляет 10 км. При использовании стандартного волокна SMF-28 с погонными потерями приблизительно 0,2 дБ/км на длине волны 1550 нм, дополнительные потери составят около 2 дБ. Это приведет к необходимости увеличения интенсивности на дополнительные 2 дБ для достижения порога, что, однако, не представляется существенным препятствием для проведения атаки. Допущение об использовании Евой детекторов с единичной квантовой эффективностью также накладывает дополнительные ограничения на возможность проведения атаки. Так, например, типичные значения квантовой эффективности современных полупроводниковых ДОФ на базе InGaAs составляют 5—30%. Использование таких детекторов пропорционально увеличит пороговое значение степени увеличения интенсивности, т.е. приведет к его увеличению примерно на 5—15 дБ. Кажется, что при этом требуемое значение порога будет уже значительно выше экспериментально продемонстрированных 10—14 дБ. Для некоторых систем КРК такой аргумент, по-видимому, действительно может позволить оценить риск, связанный с соответствующей уязвимостью, как невысокий. Однако следует учитывать, что при некоторых условиях это может быть не так. Некоторые передатчики системы КРК содержат в оптической схеме два подряд идущих оптических аттенюатора (например, в системе, исследованной в работе [143], использовались идущие подряд

переменный и постоянный оптический аттенюаторы). Совокупная степень просветления такой конфигурации теоретически может превысить рассмотренный «прагматический» порог. Более того, ряд систем КРК (например, атмосферные системы КРК) используют излучение в видимом спектральном диапазоне, что позволяет использовать высокоэффективные кремниевые ДОФ. Наконец, Ева может использовать сверхпроводниковые ДОФ, обладающие предельно высокими значениями квантовой эффективности, достигающими 90% и выше [63].

В-третьих, успешному проведению атаки могут мешать временны́е характеристики ДОФ Евы, а именно конечная величина так называемого мертвого времени детекторов, в течение которого после срабатывания детектора он не способен регистрировать новые фотоотсчеты. Для ЛФД на базе InGaAs величина мертвого времени обычно устанавливается в диапазоне от 0,1 до 10 мкс для снижения вероятности возникновения паразитных отложенных срабатываний. Это ограничивает частоту повторения USD-измерений Евы значениями от 100 кГц до 10 МГц. Если система КРК работает на более высокой частоте повторения, Ева может попытаться уменьшить величину мертвого времени. Однако это приведет к возникновению паразитных отложенных срабатываний, которые могут вносить ошибки в измерения Евы. Для их предотвращения Еве может потребоваться использовать наилучшие из представленных на сегодняшний день ЛФД на базе InGaAs с пренебрежимо малыми вероятностями возникновения отложенных срабатываний и мертвым временем, лежащим в интервале около 3—10 нс [155]. В качестве альтернативы она может вновь обратиться к сверхпроводниковым детекторам, которые лишены эффекта отложенных срабатываний и зачастую обладают мертвым временем всего в несколько наносекунд [63]. Таким образом, рассматривая наихудший сценарий, можно предположить, что у Евы имеются достаточные ресурсы для получения требуемого ей оборудования.

Следует отметить, что USD-измерения по своему построению позволяют Еве однозначно верно идентифицировать закодированное состояния. Тем не менее Ева все равно может получить неверный результат измерений или навязать Бобу ошибочное состояние вследствие неточного приготовления или измерения состояний легитимными пользователями. Эта особенность обсуждалась в работе [45], где было заключено, что такие эффекты не требуют отдельного рассмотрения, поскольку при USD-атаках Ева получает весь ключ целиком, независимо от уровня ошибки, возникающего но стороне Боба. Более того, иногда Еве даже может быть выгодно ввести дополнительную ошибку (например,

посылая состояния, ортогональные ее результатам измерений), чтобы скрыть свое присутствие, поскольку в отсутствие атаки обычно наблюдается ненулевой QBER.

Также стоит отметить, что, согласно опубликованным экспериментальным данным [112; 113], увеличение интенсивности излучения, вызываемое LDA, по своей природе непредсказуемо. Это порождает два возможных развития событий для нарушителя. В первом случае изменение не превышает требуемого порога и атака терпит неудачу. Во втором случае степень понижения аттенюации превосходит порог, однако его точное значение остаётся неизвестным Еве. Нас интересует лишь второй сценарий, поскольку мы исследуем условия, при которых атака становится осуществимой, даже если эти условия не всегда реализуются на практике. После проведения LDA Ева может попытаться проверить успешность ее воздействия и оценить фактическое изменение аттенюации для выбора оптимальных параметров последующей USD-атаки. Это, в принципе, может быть осуществлено с помощью оптической рефлектометрии с использованием устройств, подобных рассмотренному в разделе 2.2.2, либо прямым измерением интенсивности излучения Алисы высокочувствительным ваттметром или ДОФ. После выполнения такого измерения Ева получает необходимую информацию для проведения USD-атаки и может приступить к ее выполнению в описанном выше порядке.

Таким образом, мы рассмотрели риски, связанные с увеличением интенсивности легитимного излучения для протокола BB84 с использованием метода «decoy state». Рассмотренные нами USD-атаки, в действительности, позволяют нарушителю получить весь ключ при выполнении некоторых условий, каждое из которых является практически достижимым. Основное условие состоит в преодолении некоторого порогового значения степени увеличения интенсивности излучения, которое может быть достигнуто, например, при просветлении оптических аттенюаторов под воздействием мощного излучения. Для реалистичных атак, рассмотренных в настоящей главе, эти пороговые значения оказываются, в основном, не ниже 10 дБ, что может давать определенный «запас прочности» при некоторых условиях. Так, например, использование в системах КРК оптических аттенюаторов, для которых уменьшение аттенюации на 10 дБ и более экспериментально не наблюдается, может рассматриваться как достаточная мера защиты от реалистичного нарушителя. Однако, в общем случае, существование реалистичных USD-атак устанавливает жесткие

требования к мерам защиты от атак, приводящим к увеличению интенсивности легитимного излучения. Мы показали, что для проведения простейшей USD-атаки нарушителю по существу требуется лишь установка приемника системы КРК с пассивным выбором базиса и стандартный лазерный передатчик. Такие устройства на сегодняшний день являются широко доступными. Более сложная версия USD-атаки — PPNR USD-атака дополнительно требует использования детекторов с псевдоразличением числа фотонов и однофотонных источников. Данное оборудование хоть и является более «экзотичным», тем не менее имеется в распоряжении научных лабораторий [153]. Данные обстоятельства делают невозможными допущения о технической нереализуемости атак на многофотонную компоненту при увеличении интенсивности легитимного излучения и устанавливают необходимость обеспечения мер защиты от LDA и LSA при рассмотрении любых моделей возможного нарушителя. При использовании надежных мер защиты от атак с изменением параметров системы, риски будут нивелированы, а безопасность КРК будет сохранена.

3.4 Выводы по главе

Рассмотрены атаки на многофотонную компоненту на системы КРК, использующие протокол BB84 и метод «decoy state», при увеличении интенсивности легитимного излучения, возникшего в результате атаки с лазерным повреждением или атаки с затравочным излучением. Показано, что нарушитель может получить весь секретный ключ при проведении двухфотонной PNS-атаки, начиная со сколь угодно малого увеличения интенсивности, если он способен проводить неразрушающие измерения числа фотонов, и обладает долгосрочной квантовой памятью. При проведении трехфотонной PNS-атаки нарушитель может получить весь ключ без использования квантовой памяти, если степень увеличения интенсивности легитимного излучения превысит некоторый порог $\kappa_{3\mathrm{ph}}$ — конкретное значение данного порога для метода «decoy state» с одним ослабленным и одним вакуумным состояниями-ловушками было вычислено аналитически. Было показано, что n-фотонные PNS-атаки для $n > 3$ обладают более высоким порогом степени увеличения интенсивности.

Было установлено, что нарушитель способен получить весь секретный ключ при проведении атак с однозначным различением состояний (USD-атак) без использования квантовой памяти и неразрушающих измерений, если степень увеличения интенсивности превышает пороговое значение κ_{USD}. Оптическая схема для реализации USD-измерений в случае поляризационного кодирования представляет собой установку приемника КРК с пассивным выбором базиса. Было вычислено приближенное значение κ_{USD}, которое оказалось ровно в 2 раза выше порога $\kappa_{3\mathrm{ph}}$ для трехфотонной PNS-атаки, что подчеркивает «трехфотонную» природу USD-атак. Точное значение порога было определено численно для различных параметров метода «decoy state». Была предложена модифицированная версия USD-атаки, включающая в себя дополнительное измерение «лишних» фотонов, путем отщепления части излучения с помощью светоделителя с коэффициентом пропускания T. Показано, что порог степени увеличения интенсивности κ_T для модифицированной USD-атаки стремится к пределу трехфотонной PNS-атаки при стремлении T к нулю, что, однако, приводит к значительному понижению темпов отсчетов на приемной стороне.

Была рассмотрена USD-атака с дополнительными измерениями с псевдоразличением числа фотонов и модифицированной передающей станцией, содержащей импульсный лазер и источник одиночных фотонов. Было показано, что такая атака может позволить нарушителю получить весь секретный ключ, полностью имитируя темпы отсчетов и темпы двойных срабатываний для информационных состояний и состояний ловушек, что делает невозможным детектирование нарушителя по косвенным статистическим параметрам. Численно была получена зависимость порога увеличения интенсивности κ_{PPNR} для этой атаки от потерь в канале связи между легитимными пользователями. Наконец, было рассмотрено влияние квантовой эффективности детекторов Евы и шумов детектора Боба на возможность проведения атаки. Было показано, что данные несовершенства не приводят к невозможности проведения атаки, а соответствующие пороговые значения степени увеличения интенсивности лежат в интервале, достижимом при помощи лазерного повреждения оптических аттенюаторов, которое неоднократно демонстрировалось экспериментально. Результаты главы подчеркивают необходимость использования надлежащих мер защиты от атак с лазерным повреждением и затравочным излучением при любых допущениях о возможностях нарушителя.

Результаты третьей главы опубликованы в работе [156].

Заключение

Основные результаты работы 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 без-

ошибочных 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.

Автор выражает благодарность своему научному руководителю Молоткову С. Н. за неоценимую помощь в работе над диссертацией, многочисленные плодотворные обсуждения научных проблем и переданный опыт в области квантовой теории информации.

Автор выражает благодарность своим коллегам из Центра Квантовых Технологий МГУ имени М. В. Ломоносова Кулику С. П. и Климову А. Н. за помощь при решении научных и административных задач, возникавших при работе над настоящей диссертацией.

Автор выражает благодарность руководству и сотрудниками АО «ИнфоТеКС» и ООО «СФБ Лаб» за значительный вклад, сделавший настоящую работу возможной. Отдельно хотелось бы выразить признательность Дворецкому Д. А. за переданную культуру научной работы, а также поблагодарить всех своих коллег по Инженерно-квантовой Лаборатории за помощь в экспериментальных исследованиях, в особенности, Богданова С. А., Булавкина Д. С., Бугая К. Е., Бондаря К. Д., Сидельникову А. С., Вахрушеву В. М., Лохматова Р. Ю. и Зызыкина А. П.

Автор также благодарит авторов шаблона *Russian-Phd-LaTeX-Dissertation-Template* за помощь в оформлении диссертации.

Список сокращений и условных обозначений

AGA	After-Gate Attack — атака на спаде строба
BFA	Backflash Attack — атака с переизлучением ДОФ
BS	Beam Splitting — атака со светоделителем
DBA	Detector Blinding Attack — атака с ослеплением ДОФ
Decoy state	метод состояний-ловушек, состоящий в использовании вспомогательных когерентных квантовых состояний с измененным средним числом фотонов и измерении статистики их детектирования для последующей оценки параметров протокола КРК
IPA	Induced Photorefraction Attack — атака с вынужденной фоторефрацией
LDA	Laser Damage Attack — атака с лазерным повреждением
LIDT	laser induced damage threshold — порог лазерного повреждения
LSA	Laser Seeding Attack — атака с затравочным излучением
MDI	Measurement Device Independent — протоколы КРК с недоверенными промежуточными узлами
PNS	Photon Number Splitting — атака с расщеплением по числу фотонов
POVM	positive operator-valued measure — положительно-определенная операторная мера; набор измерительных операторов
PPNR	pseudo-photon-number resolution — псевдоразличение числа фотонов
QBER	quantum bit error rate — средняя вероятность квантовой битовой ошибки
THA	Trojan Horse Attack— атака активного оптического зондирования
UM (USD)	Unambiguous Measurements (Unambiguous State Discrimination) — измерения с определеным исходом, однозначное различение состояний, или безошибочные измерения
Алиса	легитимный участник КРК, выполняющий приготовление квантовых состояний

Боб	легитимный участник КРК, выполняющий измерение квантовых состояний
ГСЧ	генератор случайных чисел
ДОФ	детектор одиночных фотонов
Ева	(нарушитель, злоумышленник) нелегитимный участник КРК, пытающийся получить информацию о распределяемом ключе
КРК	квантовое распределение ключей
ЛФД	лавинный фотодиод

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.

14. *Арбеков, И. М.* Элементарная квантовая криптография: Для криптографов, не знакомых с квантовой механикой / И. М. Арбеков. — Москва : URSS, 2022.

15. *Арбеков, И. М.* Различимость квантовых состояний и трудоемкость по Шеннону в квантовой криптографии / И. М. Арбеков, С. Н. Молотков // Журнал экспериментальной и теоретической физики. — 2017. — Т. 152, № 1. — С. 62.

16. *Portmann, C.* Cryptographic security of quantum key distribution / C. Portmann, R. Renner // arXiv preprint arXiv:1409.3525. — 2014.

17. *Miller, F.* Telegraphic code to insure privacy and secrecy in the transmission of telegrams / F. Miller. — BoD–Books on Demand, 2024.

18. *Кронберг, Д. А.* Квантовая криптография / Д. А. Кронберг, Ю. И. Ожигов, А. Ю. Чернявский. — Москва : МАКС Пресс, 2011.

19. *Heisenberg, W.* Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik / W. Heisenberg // Zeitschrift für Physik. — 1927. — Т. 43, № 3. — С. 172—198.

20. *Robertson, H. P.* The Uncertainty Principle / H. P. Robertson // Phys. Rev. — 1929. — Июль. — Т. 34, вып. 1. — С. 163—164.

21. *Deutsch, D.* Uncertainty in quantum measurements / D. Deutsch // Physical Review Letters. — 1983. — Т. 50, № 9. — С. 631.

22. *Maassen, H.* Generalized entropic uncertainty relations / H. Maassen, J. B. Uffink // Physical Review Letters. — 1988. — Т. 60, № 12. — С. 1103.

23. The uncertainty principle in the presence of quantum memory / M. Berta [и др.] // Nature Physics. — 2010. — Т. 6, № 9. — С. 659—662.

24. *Einstein, A.* Can quantum-mechanical description of physical reality be considered complete? / A. Einstein, B. Podolsky, N. Rosen // Physical Review. — 1935. — Т. 47, № 10. — С. 777.

25. *Молотков, С. Н.* Побочные каналы утечки информации в квантовой криптографии: не строго однофотонные состояния, разные квантовые эффективности детекторов, конечные передаваемые последовательности / С. Н. Молотков // Журнал Экспериментальной и Теоретической физики. — 2021. — Т. 160, № 3. — С. 327—365.

26. *Молотков, С. Н.* Квантовое распределение ключей как схема с бернуллиевскими испытаниями / С. Н. Молотков // Журнал Экспериментальной и Теоретической Физики. — 2018. — Т. 153, № 6. — С. 895—907.

27. *Shannon, C. E.* A mathematical theory of communication / C. E. Shannon // The Bell system technical journal. — 1948. — Т. 27, № 3. — С. 379—423.

28. *Dixon, A.* High speed and adaptable error correction for megabit/s rate quantum key distribution / A. Dixon, H. Sato // Scientific Reports. — 2014. — Т. 4, № 1. — С. 7275.

29. Security of quantum key distribution with imperfect devices / D. Gottesman [и др.] // International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings. — IEEE. 2004. — С. 136.

30. *Hwang, W.-Y.* Quantum key distribution with high loss: toward global secure communication / W.-Y. Hwang // Physical Review Letters. — 2003. — Т. 91, № 5. — С. 057901.

31. *Lo, H.-K.* Decoy state quantum key distribution / H.-K. Lo, X. Ma, K. Chen // Physical Review Letters. — 2005. — Т. 94, № 23. — С. 230504.

32. Practical decoy state for quantum key distribution / X. Ma [и др.] // Physical Review A—Atomic, Molecular, and Optical Physics. — 2005. — Т. 72, № 1. — С. 012326.

33. *Kulik, S.* Decoy state method for quantum cryptography based on phase coding into faint laser pulses / S. Kulik, S. Molotkov // Laser Physics Letters. — 2017. — Т. 14, № 12. — С. 125205.

34. Security of the decoy state method for quantum key distribution / A. S. Trushechkin [и др.] // Physics-Uspekhi. — 2021. — Т. 64, № 1. — С. 88.

35. *Cai, R. Y.* Finite-key analysis for practical implementations of quantum key distribution / R. Y. Cai, V. Scarani // New Journal of Physics. — 2009. — Т. 11, № 4. — С. 045024.

36. *Молотков, С. Н.* О простой квантово-статистической интерпретации критерия секретности ключей в квантовой криптографии / С. Н. Молотков // Журнал Экспериментальной и Теоретической Физики. — 2020. — Т. 158, № 3. — С. 440—458.

37. *Молотков, С. Н.* Явная атака на ключ в квантовой криптографии (протокол BB84), достигающая теоретического предела ошибки Q_c\approx11\% / С. Н. Молотков, А. В. Тимофеев // Письма в Журнал экспериментальной и Теоретической Физики. — 2007. — Т. 85, № 10. — С. 632—637.

38. *Dušek, M.* Generalized beam-splitting attack in quantum cryptography with dim coherent states / M. Dušek, O. Haderka, M. Hendrych // Optics Communications. — 1999. — Т. 169, № 1—6. — С. 103—108.

39. Limitations on practical quantum cryptography / G. Brassard [и др.] // Physical Review Letters. — 2000. — Т. 85, № 6. — С. 1330.

40. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations / V. Scarani [и др.] // Physical Review Letters. — 2004. — Т. 92, № 5. — С. 057901.

41. *Kulik, S. P.* Experimental resources needed to implement photon number splitting attack in quantum cryptography / S. P. Kulik, K. S. Kravtsov, S. N. Molotkov // Laser Physics Letters. — 2022. — Т. 19, № 2. — С. 025203.

42. Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution / W.-T. Liu [и др.] // Physical Review A—Atomic, Molecular, and Optical Physics. — 2011. — Т. 83, № 4. — С. 042326.

43. Photon Number Splitting Attack–Proposal and Analysis of an Experimental Scheme / A. Ashkenazy [и др.] // Advanced Quantum Technologies. — 2024. — Т. 7, № 7. — С. 2300437.

44. *Yuen, H. P.* Quantum amplifiers, quantum duplicators and quantum cryptography / H. P. Yuen // Quantum and Semiclassical Optics: Journal of the European Optical Society Part B. — 1996. — Т. 8, № 4. — С. 939.

45. *Dušek, M.* Unambiguous state discrimination in quantum cryptography with weak coherent states / M. Dušek, M. Jahma, N. Lütkenhaus // Physical Review A. — 2000. — Т. 62, № 2. — С. 022306.

46. *Van Enk, S.* Unambiguous state discrimination of coherent states with linear optics: Application to quantum cryptography / S. Van Enk // Physical Review A. — 2002. — Т. 66, № 4. — С. 042313.

47. *Bennett, C. H.* Quantum cryptography using any two nonorthogonal states / C. H. Bennett // Physical Review Letters. — 1992. — Т. 68, № 21. — С. 3121.

48. *Кулик, С. П.* О трудоемкости перебора в квантовой криптографии с теоретико-информационно стойкой аутентификацией / С. П. Кулик, С. Н. Молотков // Письма в Журнал экспериментальной и теоретической физики. — 2025. — Т. 121, № 6. — С. 503—512.

49. Attacks on practical quantum key distribution systems (and how to prevent them) / N. Jain [и др.] // Contemporary Physics. — 2016. — Т. 57, № 3. — С. 366—387.

50. *Долинов, Д.* Основы теории надёжности: конспект лекций / Д. Долинов, А. Долинов. — Пермь : Издательство Пермского национального исследовательского политехнического университета, 2020. — Утверждено редакционно-издательским советом университета. Рецензенты: Я.Н. Немов, В.Я. Беленький.

51. Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses / K.-i. Yoshino [и др.] // npj Quantum Information. — 2018. — Т. 4, № 1. — С. 8.

52. Patterning-effect mitigating intensity modulator for secure decoy-state quantum key distribution / G. Roberts [и др.] // Optics letters. — 2018. — Т. 43, № 20. — С. 5110—5113.

53. Information leakage via side channels in freespace BB84 quantum cryptography / S. Nauerth [и др.] // New Journal of Physics. — 2009. — Т. 11, № 6. — С. 065001.

54. Quantum key distribution with distinguishable decoy states / A. Huang [и др.] // Physical Review A. — 2018. — Т. 98, № 1. — С. 012330.

55. *Tamaki, K.* Decoy-state quantum key distribution with a leaky source / K. Tamaki, M. Curty, M. Lucamarini // New Journal of Physics. — 2016. — Т. 18, № 6. — С. 065008.

56. Partially random phase attack to the practical two-way quantum-key-distribution system / S.-H. Sun [и др.] // Physical Review A—Atomic, Molecular, and Optical Physics. — 2012. — Т. 85, № 3. — С. 032304.

57. Security bounds for decoy-state quantum key distribution with arbitrary photon-number statistics / G. Foletto [и др.] // Physical Review A. — 2022. — Т. 105, № 1. — С. 012603.

58. Security of quantum key distribution with imperfect phase randomisation / G. Currás-Lorenzo [и др.] // Quantum Science and Technology. — 2023. — Т. 9, № 1. — С. 015025.

59. Security of the decoy-state BB84 protocol with imperfect state preparation / A. Reutov [и др.] // Entropy. — 2023. — Т. 25, № 11. — С. 1556.

60. Modified BB84 quantum key distribution protocol robust to source imperfections / M. Pereira [и др.] // Physical Review Research. — 2023. — Т. 5, № 2. — С. 023065.

61. *Hadfield, R. H.* Single-photon detectors for optical quantum information applications / R. H. Hadfield // Nature photonics. — 2009. — Т. 3, № 12. — С. 696—705.

62. Detecting telecom single photons with 99.5- 2.07+ 0.5% system detection efficiency and high time resolution / J. Chang [и др.] // APL Photonics. — 2021. — Т. 6, № 3.

63. *Holzman, I.* Superconducting nanowires for single-photon detection: progress, challenges, and opportunities / I. Holzman, Y. Ivry // Advanced Quantum Technologies. — 2019. — Т. 2, № 3/4. — С. 1800058.

64. Deep-learning-based radio-frequency side-channel attack on quantum key distribution / A. Baliuka [и др.] // Physical Review Applied. — 2023. — Т. 20, № 5. — С. 054040.

65. Experimental side channel analysis of BB84 QKD source / A. Biswas [и др.] // IEEE Journal of Quantum Electronics. — 2021. — Т. 57, № 6. — С. 1—7.

66. *Genkin, D.* Acoustic cryptanalysis / D. Genkin, A. Shamir, E. Tromer // Journal of Cryptology. — 2017. — Т. 30, № 2. — С. 392—443.

67. *Lamas-Linares, A.* Breaking a quantum key distribution system through a timing side channel / A. Lamas-Linares, C. Kurtsiefer // Optics express. — 2007. — Т. 15, № 15. — С. 9388—9393.

68. Single trace side-channel attack on key reconciliation in quantum key distribution system and its efficient countermeasures / D. Park [и др.] // ICT Express. — 2021. — Т. 7, № 1. — С. 36—40.

69. The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks? / C. Kurtsiefer [и др.] // Journal of Modern Optics. — 2001. — Т. 48, № 13. — С. 2039—2047.

70. *Vakhitov, A.* Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography / A. Vakhitov, V. Makarov, D. R. Hjelme // Journal of Modern Optics. — 2001. — Т. 48, № 13. — С. 2023—2038.

71. Eavesdropping and countermeasures for backflash side channel in quantum cryptography / P. V. P. Pinheiro [и др.] // Optics Express. — 2018. — Т. 26, № 16. — С. 21020—21032.

72. Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution / A. Meda [и др.] // Light: Science & Applications. — 2017. — Т. 6, № 6. — e16261—e16261.

73. Trojan-horse attacks on quantum-key-distribution systems / N. Gisin [и др.] // Physical Review A—Atomic, Molecular, and Optical Physics. — 2006. — Т. 73, № 2. — С. 022320.

74. Practical security bounds against the trojan-horse attack in quantum key distribution / M. Lucamarini [и др.] // Physical Review X. — 2015. — Т. 5, № 3. — С. 031030.

75. Trojan-horse attacks threaten the security of practical quantum cryptography / N. Jain [и др.] // New Journal of Physics. — 2014. — Т. 16, № 12. — С. 123030.

76. Risk analysis of Trojan-horse attacks on practical quantum key distribution systems / N. Jain [и др.] // IEEE Journal of Selected Topics in Quantum Electronics. — 2014. — Т. 21, № 3. — С. 168—177.

77. Анализ эффективности методов защиты от атак активного оптического зондирования на волоконные системы квантового распределения ключей в спектральном диапазоне 1260–1650 nm / А. В. Борисова [и др.] // Оптика и Спектроскопия. — 2020. — Т. 128, № 11. — С. 1758—1766.

78. *Uhlmann, A.* The "transition probability" in the state space of a∗-algebra / A. Uhlmann // Reports on Mathematical Physics. — 1976. — Т. 9, № 2. — С. 273—279.

79. *Koashi, M.* Simple security proof of quantum key distribution based on complementarity / M. Koashi // New Journal of Physics. — 2009. — Т. 11, № 4. — С. 045018.

80. *Vinay, S. E.* Extended analysis of the Trojan-horse attack in quantum key distribution / S. E. Vinay, P. Kok // Physical Review A. — 2018. — Т. 97, № 4. — С. 042335.

81. Active sensing and side channels of information leakage in quantum cryptography / S. N. Molotkov [и др.] // Laser Physics. — 2019. — Т. 29, № 12. — С. 124001.

82. *Makarov, V.* Faked states attack on quantum cryptosystems / V. Makarov, D. R. Hjelme // Journal of Modern Optics. — 2005. — Т. 52, № 5. — С. 691—705.

83. *Makarov, V.* Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols / V. Makarov, J. Skaar // arXiv preprint quant-ph/0702262. — 2007.

84. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems / Y. Zhao [и др.] // Physical Review A—Atomic, Molecular, and Optical Physics. — 2008. — Т. 78, № 4. — С. 042333.

85. О простом способе защиты от атаки "Detectors Mismatch" в квантовой криптографии: протокол BB84 / К. А. Балыгин [и др.] // Журнал Экспериментальной и Теоретической Физики. — 2020. — Т. 157, № 2. — С. 195—205.

86. Superlinear threshold detectors in quantum cryptography / L. Lydersen [и др.] // Physical Review A—Atomic, Molecular, and Optical Physics. — 2011. — Т. 84, № 3. — С. 032320.

87. Controlling single-photon detector ID210 with bright light / V. Chistiakov [и др.] // Optics Express. — 2019. — Т. 27, № 22. — С. 32253—32262.

88. Ability of strong-pulse illumination to hack self-differencing avalanche photodiode detectors in a high-speed quantum-key-distribution system / B. Gao [и др.] // Physical Review A. — 2022. — Т. 106, № 3. — С. 033713.

89. Hacking commercial quantum cryptography systems by tailored bright illumination / L. Lydersen [и др.] // Nature Photonics. — 2010. — Т. 4, № 10. — С. 686—689.

90. After-gate attack on a quantum cryptosystem / C. Wiechers [и др.] // New Journal of Physics. — 2011. — Т. 13, № 1. — С. 013043.

91. *Lo, H.-K.* Measurement-device-independent quantum key distribution / H.-K. Lo, M. Curty, B. Qi // Physical Review Letters. — 2012. — Т. 108, № 13. — С. 130503.

92. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters / M. Lucamarini [и др.] // Nature. — 2018. — Т. 557, № 7705. — С. 400—403.

93. *Yuan, Z.* Avoiding the blinding attack in QKD / Z. Yuan, J. F. Dynes, A. J. Shields // Nature Photonics. — 2010. — Т. 4, № 12. — С. 800—801.

94. Hacking single-photon avalanche detectors in quantum key distribution via pulse illumination / Z. Wu [и др.] // Optics Express. — 2020. — Т. 28, № 17. — С. 25574—25590.

95. Automated verification of countermeasure against detector-control attack in quantum key distribution / P. Acheva [и др.] // EPJ Quantum Technology. — 2023. — Т. 10, № 1. — С. 22.

96. Study of a single-photon detector blinding attack with modulated bright light / D. Bulavkin [и др.] // Quantum and Nonlinear Optics IX. Т. 12323. — SPIE. 2023. — С. 73—78.

97. *Lizama-Pérez, L. A.* Quantum key distribution in the presence of the intercept-resend with faked states attack / L. A. Lizama-Pérez, J. M. López, E. De Carlos López // Entropy. — 2016. — Т. 19, № 1. — С. 4.

98. *Alhussein, M.* Monitoring coincident clicks in differential-quadrature-phase shift QKD to reveal detector blinding and control attacks / M. Alhussein, K. Inoue, T. Honjo // Japanese Journal of Applied Physics. — 2018. — Т. 58, № 1. — С. 012006.

99. *Shen, L.* Countering detector manipulation attacks in quantum communication through detector self-testing / L. Shen, C. Kurtsiefer // APL Photonics. — 2025. — Т. 10, № 1.

100. Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution / C. C. W. Lim [и др.] // IEEE Journal of Selected Topics in Quantum Electronics. — 2015. — Т. 21, № 3. — С. 192—196.

101. Robust countermeasure against detector control attack in a practical quantum key distribution system / Y.-J. Qian [и др.] // Optica. — 2019. — Т. 6, № 9. — С. 1178—1184.

102. Inherent security of phase coding quantum key distribution systems against detector blinding attacks / K. Balygin [и др.] // Laser Physics Letters. — 2018. — Т. 15, № 9. — С. 095203.

103. *Sushchev, I. S.* Point-to-point quantum key distribution resistant to fake-state attacks / I. S. Sushchev // APL Quantum. — 2025. — Т. 2, № 2.

104. Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption / A. Huang [и др.] // IEEE Journal of Quantum Electronics. — 2016. — Т. 52, № 11. — С. 1—11.

105. Comment on"Inherent security of phase coding quantum key distribution systems against detector blinding attacks"[Laser Phys. Lett. 15, 095203 (2018)] / A. Fedorov [и др.] // arXiv preprint arXiv:1809.03911. — 2018.

106. Robust countermeasure against detector control attack in a practical quantum key distribution system: comment / Z. Wu [и др.] // Optica. — 2020. — Т. 7, № 10. — С. 1391—1393.

107. External magnetic effect for the security of practical quantum key distribution / H. Tan [и др.] // Quantum Science and Technology. — 2022. — Т. 7, № 4. — С. 045008.

108. Practical security of continuous-variable quantum key distribution with an optical amplifier / Y. Zheng [и др.] // Physical Review A. — 2024. — Т. 109, № 2. — С. 022424.

109. *Garcia-Escartin, J. C.* Attacking quantum key distribution by light injection via ventilation openings / J. C. Garcia-Escartin, S. Sajeed, V. Makarov // PloS one. — 2020. — Т. 15, № 8. — e0236630.

110. Laser damage helps the eavesdropper in quantum cryptography / A. N. Bugge [и др.] // Physical Review Letters. — 2014. — Т. 112, № 7. — С. 070503.

111. Laser-damage attack against optical attenuators in quantum key distribution / A. Huang [и др.] // Physical Review Applied. — 2020. — Т. 13, № 3. — С. 034017.

112. *Alferov, S. V.* Study of the vulnerability of neutral optical filters used in quantum key distribution systems against laser damage attack / S. V. Alferov, K. E. Bugai, I. A. Pargachev // JETP Letters. — 2022. — Т. 116, № 2. — С. 123—127.

113. Laser Damage Attack on a Simple Optical Attenuator Widely Used in Fiber-based QKD Systems / K. Bugai [и др.] // 2022 International Conference Laser Optics (ICLO). — IEEE. 2022. — С. 1—1.

114. Vulnerabilities in the quantum key distribution system induced under a pulsed laser attack / D. D. Ruzhitskaya [и др.] // Journal Scientific and Technical Of Information Technologies, Mechanics and Optics. — 2021. — Т. 136, № 6. — С. 837.

115. Protecting fiber-optic quantum key distribution sources against light-injection attacks / A. Ponosova [и др.] // PRX Quantum. — 2022. — Т. 3, № 4. — С. 040307.

116. Pulsed laser attack at 1061 nm potentially compromises quantum key distribution / A. Ponosova [и др.] // arXiv preprint arXiv:2506.19091. — 2025.

117. Protection method against powerful emission attacks based on optical-fiber fuse element / K. Bugai [и др.] // 2024 International Conference Laser Optics (ICLO). — IEEE. 2024. — С. 446—446.

118. Optical fuse as a countermeasure against light injection attacks on quantum key distribution systems / E. Borisova [и др.] // 2024 International Conference Laser Optics (ICLO). — IEEE. 2024. — С. 103—103.

119. Fiber-optic power limiter device based on carbon nanotubes / E. Borisova [и др.] // arXiv preprint arXiv:2510.09301. — 2025.

120. Laser-seeding attack in quantum key distribution / A. Huang [и др.] // Physical Review Applied. — 2019. — Т. 12, № 6. — С. 064043.

121. Induced-photorefraction attack against quantum key distribution / P. Ye [и др.] // Physical Review Applied. — 2023. — Т. 19, № 5. — С. 054052.

122. Effect of light injection on the security of practical quantum key distribution / L. Han [и др.] // Physical Review Applied. — 2023. — Т. 20, № 4. — С. 044013.

123. Laser-pumping attack on QKD sources / M. Fadeev [и др.] // 2024 International Conference Laser Optics (ICLO). — IEEE. 2024. — С. 562—562.

124. Optical-pumping attack on a quantum key distribution laser source / M. Fadeev [и др.] // arXiv preprint arXiv:2503.11239. — 2025.

125. Effect of source tampering in the security of quantum cryptography / S.-H. Sun [и др.] // Physical Review A. — 2015. — Т. 92, № 2. — С. 022304.

126. Quantified effects of the laser-seeding attack in quantum key distribution / V. Lovic [и др.] // Physical Review Applied. — 2023. — Т. 20, № 4. — С. 044005.

127. *Lo, H.-K.* Security of quantum key distribution using weak coherent states with nonrandom phases / H.-K. Lo, J. Preskill // arXiv preprint quant-ph/0610203. — 2006.

128. *Lydersen, L.* Security of quantum key distribution with bit and basis dependent detector flaws / L. Lydersen, J. Skaar // arXiv preprint arXiv:0807.0767. — 2008.

129. *Holevo, A. S.* Bounds for the quantity of information transmitted by a quantum communication channel / A. S. Holevo // Problemy Peredachi Informatsii. — 1973. — Т. 9, № 3. — С. 3—11.

130. *Holevo, A. S.* Coding theorems for quantum channels / A. S. Holevo // arXiv preprint quant-ph/9809023. — 1998.

131. *Holevo, A. S.* The capacity of the quantum channel with general signal states / A. S. Holevo // IEEE Transactions on Information Theory. — 2002. — Т. 44, № 1. — С. 269—273.

132. *Roga, W.* Universal Bounds for the Holevo Quantity, Coherent Information, and the Jensen-Shannon Divergence / W. Roga, M. Fannes, K. Życzkowski // Physical Review Letters. — 2010. — Т. 105, № 4. — С. 040505.

133. *Wilde, M.* Quantum information theory / M. Wilde. — Cambridge university press, 2013.

134. *Müller, A.* A simplified expression for quantum fidelity / A. Müller // arXiv preprint arXiv:2309.10565. — 2023.

135. Sub-and super-fidelity as bounds for quantum fidelity / J. A. Miszczak [и др.] // Quantum Information & Computation. — 2009. — Т. 9, № 1. — С. 103—130.

136. "Plug and play" systems for quantum cryptography / A. Muller [и др.] // Applied physics letters. — 1997. — Т. 70, № 7. — С. 793—795.

137. *Молотков, С. Н.* О эквивалентности фазовых и поляризационных преобразований в квантовой оптике / С. Н. Молотков, И. С. Сущев // Письма в ЖЖурнал экспериментальной и теоретической физики. — 2024. — Т. 120, № 7. — С. 505—510.

138. Invisible Trojan-horse attack / S. Sajeed [и др.] // Scientific Reports. — 2017. — Т. 7, № 1. — С. 8403.

139. Analyzing transmission spectra of fiber-optic elements in the near IR range to improve the security of quantum key distribution systems / B. Nasedkin [и др.] // Bulletin of the Russian Academy of Sciences: Physics. — 2022. — Т. 86, № 10. — С. 1164—1167.

140. Loopholes in the 1500–2100-nm range for quantum-key-distribution components: Prospects for trojan-horse attacks / B. Nasedkin [и др.] // Physical Review Applied. — 2023. — Т. 20, № 1. — С. 014038.

141. Vulnerability analysis of spectral-selective components in Quantum Key Distribution systems / O. Solomatin [и др.] // OpticaOpen preprint 29430320. — 2025.

142. Optical time domain reflectometer / M. Barnoski [и др.] // Applied Optics. — 1977. — Т. 16, № 9. — С. 2375—2379.

143. Preparing a commercial quantum key distribution system for certification against implementation loopholes / V. Makarov [и др.] // Physical Review Applied. — 2024. — Т. 22, № 4. — С. 044076.

144. Influence of QKD apparatus parameters on the backflash attack / S. A. Bogdanov [и др.] // Quantum Technologies 2022. Т. 12133. — SPIE. 2022. — С. 90—95.

145. Measuring the "backflash" probability of a single-photon detector with a time correlator / S. A. Bogdanov [и др.] // 2022 International Conference Laser Optics (ICLO). — IEEE. 2022. — С. 01—01.

146. Trojan-horse attack on a real-world quantum key distribution system: Theoretical and experimental security analysis / I. S. Sushchev [и др.] // Physical Review Applied. — 2024. — Т. 22, № 3. — С. 034032.

147. Broadband optical time-domain reflectometry for security analysis of quantum key distribution / K. D. Bondar [и др.] // Physical Review Applied. — 2025. — Т. 24, № 1. — С. 014010.

148. *Jorstad, N. D.* Cryptographic algorithm metrics / N. D. Jorstad, T. Landgrave // 20th National Information Systems Security Conference. — 1997. — С. 1—38.

149. *Calsamiglia, J.* Conditional beam-splitting attack on quantum key distribution / J. Calsamiglia, S. M. Barnett, N. Lütkenhaus // Physical Review A. — 2001. — Т. 65, № 1. — С. 012312.

150. *Coles, P. J.* Numerical approach for unstructured quantum key distribution / P. J. Coles, E. M. Metodiev, N. Lütkenhaus // Nature Communications. — 2016. — Т. 7, № 1. — С. 11712.

151. *Winick, A.* Reliable numerical key rates for quantum key distribution / A. Winick, N. Lütkenhaus, P. J. Coles // Quantum. — 2018. — Т. 2. — С. 77.

152. Gaussian boson sampling with pseudo-photon-number-resolving detectors and quantum computational advantage / Y.-H. Deng [и др.] // Physical Review Letters. — 2023. — Т. 131, № 15. — С. 150601.

153. Heralded generation of programmable two-qubit entangled states on a linear-optical platform / N. Skryabin [и др.] // Optica Quantum. — 2025. — Т. 3, № 2. — С. 162—167.

154. Implementation Security of Quantum Cryptography : White Paper No. 27 / M. Lucamarini [и др.] ; European Telecommunications Standards Institute (ETSI). — 2018. — WP 27. — URL: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf.

155. *Restelli, A.* Single-photon detection efficiency up to 50% at 1310 nm with an InGaAs/InP avalanche diode gated at 1.25 GHz / A. Restelli, J. C. Bienfang, A. L. Migdall // Applied Physics Letters. — 2013. — Т. 102, № 14.

156. Realistic vulnerabilities of decoy-state quantum key distribution / I. S. Sushchev [и др.] // Scientific reports. — 2025. — Т. 15, № 1. — С. 44820.