

УДК 004.942:001.57

МОДЕЛИРОВАНИЕ ПОВЕДЕНИЯ ЭЛЕМЕНТОВ ЗАЩИТЫ ПРИ СТОРОННЕМ ВОЗДЕЙСТВИИ НА ПАССИВНЫЕ КОМПОНЕНТЫ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Е. В. Борисова, аспирант РГРТУ, Рязань, Россия;
orcid.org/0000-0002-0198-377X, e-mail: Ekaterina21333@yandex.ru.

Безопасность в криптографии может быть реализована путем обмена секретным ключом между двумя пользователями, их называют Алисой (источник) и Бобом (приёмник). Квантовое распределение ключей – протокол, который гарантированно надежен и посредством которого биты закрытого ключа могут быть созданы в процессе коммуникации двух сторон по открытому каналу [1]. В квантовой криптографии распределение ключей происходит по квантовому каналу. Безопасность основана на факте, что любое измерение квантовой системы неизбежно изменит её состояние. Таким образом, третье лицо, Ева, может получить информацию из квантового канала, выполнив измерение, но легитимные пользователи обнаружат стороннее воздействие и этот ключ не будет использован. Основным элементом квантовой системы является одиночный фотон, перемещающийся по оптическому волокну, а ключ может быть закодирован по его поляризации или по его фазе, как впервые было предложено Беннеттом и Brassаром [2]. В 1992 году квантовая криптография была впервые экспериментально продемонстрирована на высоте более 30 см с поляризованными фотонами, средой распространения был воздух [3]. С тех пор несколько групп представили реализации как поляризации [4], так и схемы фазового кодирования в оптических волокнах [5, 6].

Однако, современные реализации систем КРК не соответствуют своим модельным представлениям в связи с несовершенством оборудования, и злоумышленник имеет возможность перехватить секретный ключ и остаться незамеченным [7-12].

Протоколы квантовой коммуникации считаются безопасными при условии, что все входящие в систему устройства полностью охарактеризованы, а побочные каналы закрыты. Однако в результате воздействия лазерного излучения возможно изменение характеристик компонентов систем квантовой коммуникации, что приводит к появлению уязвимостей в системе квантового распределения ключей.

Целью работы является возможность применения выводов из данной статьи при практической оценке безопасности систем квантовой коммуникации – оценке безопасности систем квантового распределения ключа. Работа содержит рекомендации по усилению безопасности блока источника сигнала в системах квантовой коммуникации. В качестве контрмер по защите от воздействия лазерного излучения предложено использовать оптические предохранители с заданной предельной пороговой мощностью, детекторы для мониторинга входной мощности оптического излучения и узкополосные оптические фильтры на входе в систему квантовой коммуникации. [13]. В данной статье собраны данные и приведены характеристики при использовании этих компонентов в качестве элементов защиты.

Ключевые слова: квантовая связь, квантовая коммуникация, квантовая криптография, уязвимости систем квантовой связи, атака лазерным повреждением, системы квантового распределения ключей.

DOI: 10.21667/1995-4565-2022-82-118-135

Введение

Квантовый взлом раскрывает практические показатели безопасности систем квантового распределения ключей (КРК), что затем стимулирует сообщество к повышению надежности данных систем [14]. К сожалению, квантовые хакеры изобретательны. Есть достаточное количество работ, в которых было показано, что они могут изучать или даже манипулировать характеристиками компонентов в исходном блоке с помощью различного типа атак с впрыском света.

В настоящее время известно около 25 уязвимостей, для борьбы с которыми созданы соответствующие контрмеры, способные не дать злоумышленнику перехватить ключ.

Для защиты источника систем КРК от атак затравочным лазерным излучением [15], троянским конем [16, 17] и лазерным повреждением [18, 19], при вводе излучения в источник, во многих практических реализациях волоконных и интегральных устройств на выходе из источника устанавливаются волоконные изоляторы. В работах [20, 21] выполнено исследование данных элементов при атаке мощным непрерывным лазером и установлено, что волоконный изолятор является эффективной контрмерой, если его дополнительная копия, неучтенная в доказательстве безопасности, устанавливается на выходе источника КРК.

Теоретическая часть

Для противодействия атаке импульсным лазерным излучением возможны три принципиальных подхода: сертификация крайних элементов системы, добавление пассивного предохраняющего элемента или же добавление активного наблюдения за состоянием элементов либо системы.

Сертификация крайних элементов системы. Элемент защиты может не изменять свои свойства аттенюации либо же выгорать под действием излучения. Оба этих результата считаются положительными для безопасности системы. Однако проведенное исследование показало, что успешно провести атаку лазерным повреждением с применением импульсного лазера возможно, правильно подобрав не только энергетические и временные характеристики излучения, но и его спектральный состав. Следовательно, элемент сам по себе может считаться надежным при условии прохождения всестороннего рассмотрения для сертификации.

Возможно использование следующих элементов для защиты систем КРК:

- изоляторы – пассивные оптические элементы, пропускающие свет в одном направлении и не пропускающие в обратном;
- циркуляторы – пассивные оптические элементы с тремя портами: из 1-го порта свет идет во 2-й порт, из 2-го в 3-й, из 3-го в 1-й;
- узкополосные фильтры – пассивные оптические элементы, пропускающие излучение конкретной длины волны;
- также в последнее время широко обсуждается внедрение в КРК оптических предохранителей. Оптический предохранитель – это пассивный оптический элемент с нелинейным отношением мощности пропусканием.

Вначале будут рассмотрены узкополосные фильтры. Данные компоненты являются коммерчески доступными и необходимый можно подобрать, исходя из требований системы.

В качестве узкополосных фильтров в аппаратуре КРК возможно использование таких элементов, как DWDM, и брэгговских решёток.

Брэгговские решетки в настоящее время широко используются в оптических волокнах и планарных световодах для уплотнения каналов по длине волны, оптической фильтрации сигналов, как резонаторные зеркала в волоконных и полупроводниковых лазерах, как сглаживающие фильтры в оптических усилителях, для компенсации дисперсии в магистральных каналах связи. [22, 23].

Известно, что для системы КРК с несколькими оптическими источниками следует строго проверять единообразие между различными источниками во всех степенях свободы, кроме той, которая кодируется, чтобы избежать атак по побочным каналам. Как правило, для фотонов следует учитывать следующие степени свободы: спектр, временную структуру, поляризацию, пространственный режим и интенсивность. Спектр светодиода намного шире, чем у лазерного диода. В системе, которая описана в статье [23], хорошая спектральная неразличимость достигается без каких-либо мер контроля температуры, просто пропуская оптические импульсы от разных светодиодов через волокно брэгговской решетки с полной шириной около 0,2 нм, поскольку отфильтрованные спектры гораздо больше зависят от фильтра, чем от основных спектров светодиодов, которые очень широки и обычно имеют полную ши-

рину около 30 нм. Спектры между различными светодиодами, используемые в данной системе, очень сильно отличаются друг от друга перед фильтрацией. Но после фильтрации через брэгговскую решётку их спектры практически совпадают.

Это дает системам КРК со светодиодами в качестве оптических источников потенциальное преимущество с точки зрения сложности, размера и энергопотребления системы.

Узкополосные фильтры Dense Wavelength Division Multiplexing (DWDM)

Также особый интерес представляют изучение узкополосного фильтра Dense Wavelength Division Multiplexing (DWDM). К данному моменту были проведены измерения его спектров передачи.

Уровни передаваемой мощности нельзя сравнивать, так как вносимые потери могут быть разными.

1. DWDM 1558 nm.

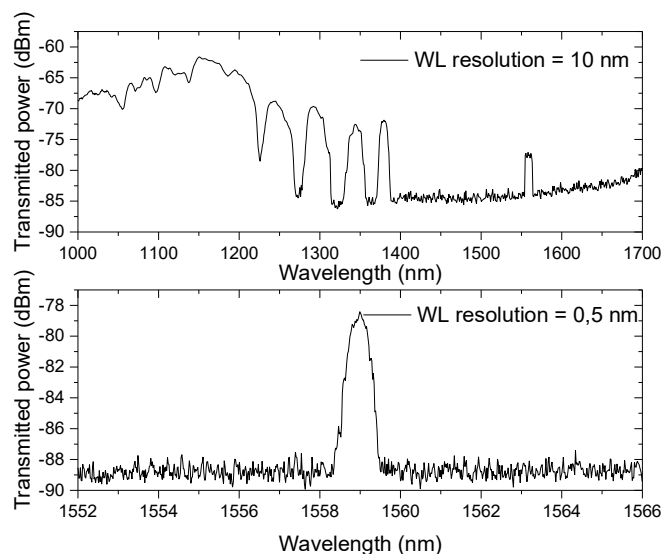


Рисунок 1 – Из порта «Common» в «Pass»

Figure 1 – From «Common» port to «Pass»

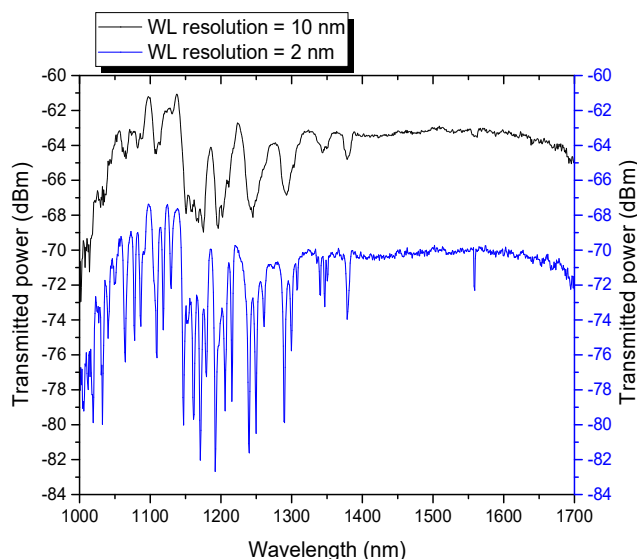


Рисунок 2 – Из порта «Common» в «Reflect»

Figure 2 – From «Common» port to «Reflect»

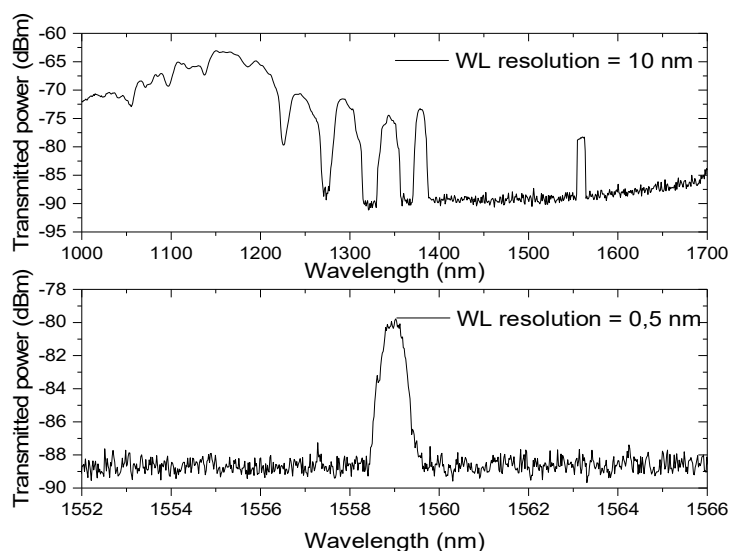


Рисунок 3 – Из порта «Pass» в «Common»
Figure 3 – From «Pass» port to «Common»

На рисунке 4 представлены спектры передачи от «Common» порта к «Pass» порту и обратно.

Уровни передаваемой мощности нельзя сравнивать, так как вносимые потери могут быть разными. (Для сравнения уровней мощности необходимы входной источник света с более высокой плотностью мощности, оптический анализатор спектра с большим диапазоном амплитуд, а DWDM должен быть соединен с источником света и оптическим анализатором спектра через фиксированные входные и выходные волокна. В этом случае коннекторы APC должны быть отрезаны, а свободные концы волокон должны быть соединены с фиксированными входными и выходными волокнами с помощью сварочного аппарата.) Однако можно видеть, что диапазон передаваемых длин волн одинаков в обоих направлениях, и кажется, что нет изоляции от порта «Pass» до порта «Common».

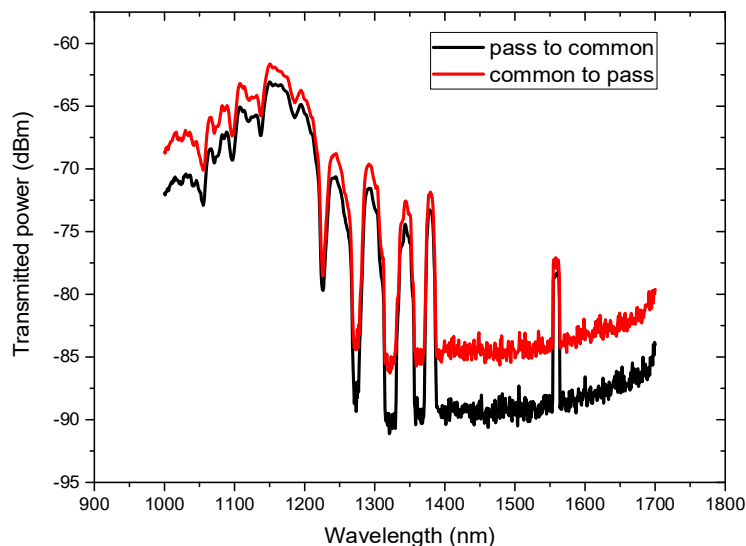


Рисунок 4 – Из порта «Pass» в «Common»
Figure 4 – From «Pass» port to «Common»

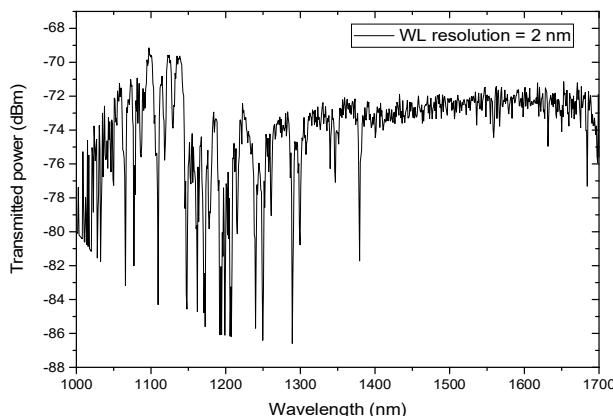


Рисунок 5 – Из порта «Reflect» в «Common»
Figure 5 – From «Reflect» port to «Common»

Далее представлены результаты, полученные в ходе эксперимента, в котором производилось воздействие мощным постоянным лазером на DWDM.

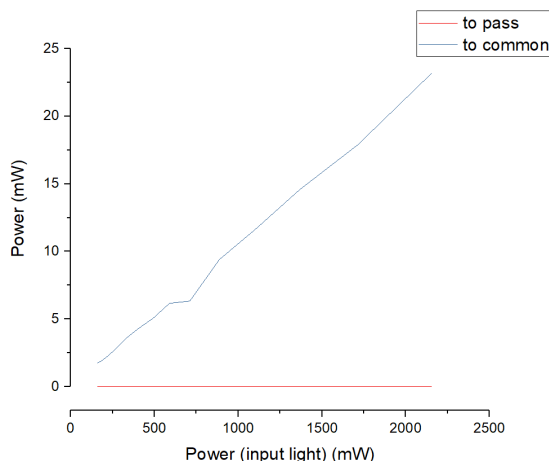


Рисунок 6 – Мощность, передаваемая через плечо Common и через плечо Pass
Figure 6 – Power passed through Common shoulder and through Pass shoulder

Далее представлены результаты исследования на спектроанализаторе DWDM до и после эксперимента. На рисунке 7 можно увидеть сравнение изменений характеристик пассивного элемента из плеча Common в плечо Pass до и после воздействия мощным лазером.

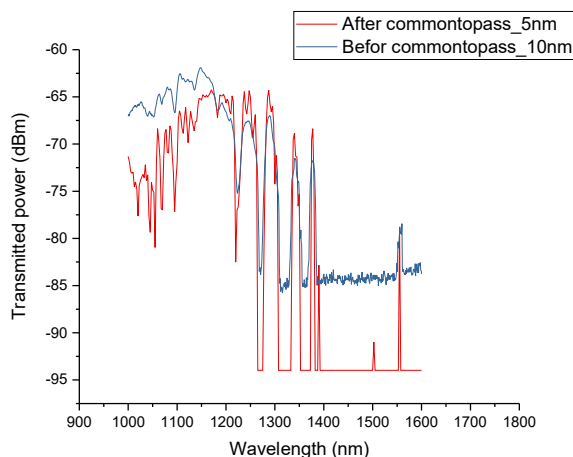


Рисунок 7 – Сравнение изменений характеристик DWDM из плеча Common в плечо Pass до и после воздействия мощным лазером
Figure 7 – Comparison of changes in DWDM characteristics from the Common shoulder to the Pass shoulder be-fore and after exposure to a powerful laser

Далее на рисунках 8, 9, 10 приведены результаты аналогичных исследований воздействия мощным лазером на разные плечи DWDM.

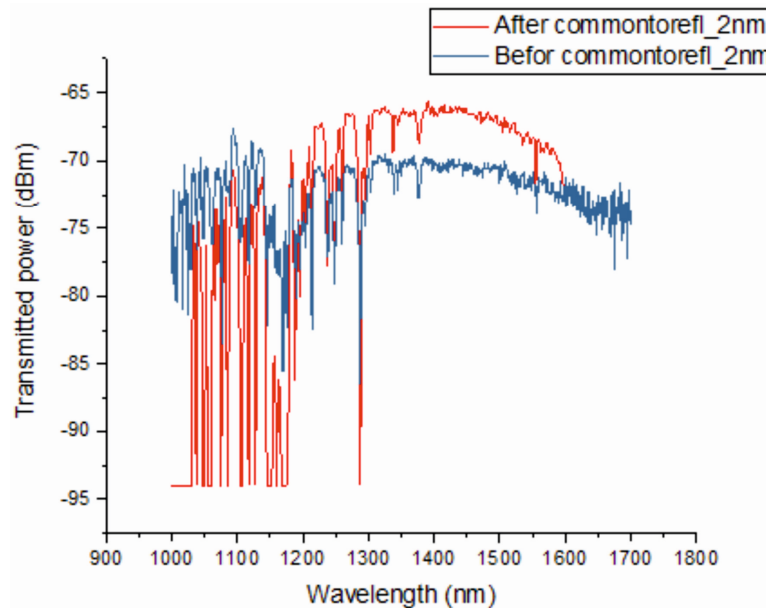


Рисунок 8 – Сравнение изменений характеристик DWDM из плеча Common в плечо Reflect до и после воздействия мощным лазером

Figure 8 – Comparison of changes in DWDM characteristics from the Common shoulder to the Reflect shoulder before and after exposure to a powerful laser

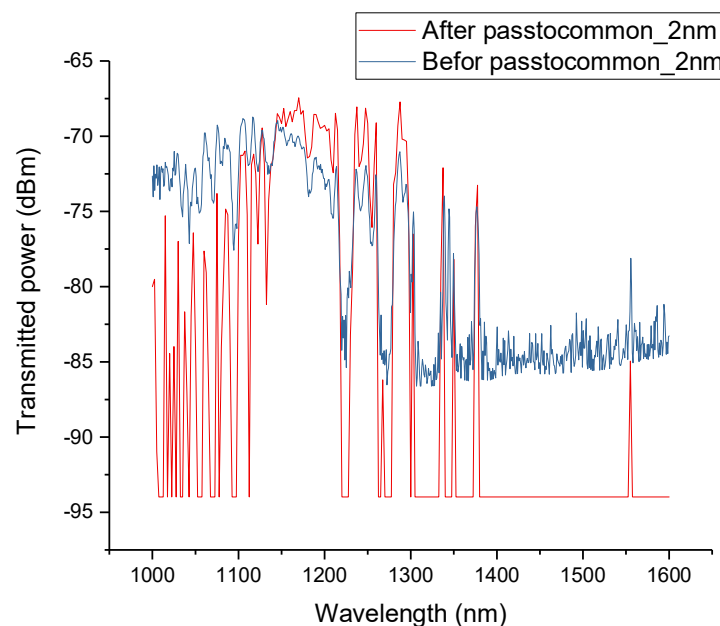


Рисунок 9 – Сравнение изменений характеристик DWDM из плеча Pass в плечо Common до и после воздействия мощным лазером

Figure 9 – Comparison of changes in DWDM characteristics from the Pass shoulder to the Common shoulder before and after exposure to a powerful laser

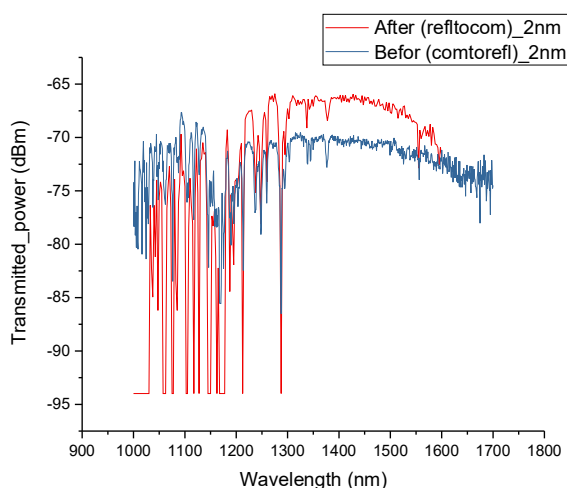


Рисунок 10 – Сравнение изменений характеристик DWDM из плеча Reflect в плечо Common до и после воздействия мощным лазером
Figure 10 – Comparison of changes in DWDM characteristics from the Reflect shoulder to the Common shoulder before and after exposure to a powerful laser

Рассматривать воздействие из плеча Pass в плечо Reflect не имеет смысла, видимых изменений на спектрограмме не выявлено.

Таким образом, было показано, что происходит с DWDM при воздействии мощного лазера через плечо. Были представлены графики сравнения спектрограммы до и после эксперимента. По этим графикам можно сделать вывод, что изменения в характеристиках были минимальными.

Работы по изучению данных элементов продолжаются. Более полный анализ возможен после получения результатов всех экспериментов.

Ультратонкие оптические ограничители

Также есть работы, в которых анализируются ультратонкие оптические ограничители, необходимые для защиты светочувствительных компонентов в миниатюрных оптических системах. Однако достижение достаточно низкого оптического предельного порога оказалось сложной задачей. Показано, что ультратонкий оптический ограничитель с низкой пороговой интенсивностью может быть реализован с использованием нелинейной зонной пластины. Зонная пластина заполнена нелинейными насыщаемыми поглощающими материалами, которые позволяют устройству фокусировать свет низкой интенсивности, в то время как свет высокой интенсивности передается в виде плоской волны без фокального пятна. Основываясь на этом предложенном механизме, используем метод конечных разностей во временной области для вычислительного проектирования зонной пластины, встроенной в квантовые точки InAs в качестве насыщаемого поглощающего материала. Устройство имеет толщину всего 0,5 мкм и демонстрирует хорошие характеристики оптического ограничения с пороговой интенсивностью всего 0,45 кВт/см², что на несколько порядков ниже, чем у современных ультратонких оптических ограничителей на основе плоской оптики. Показано, что нелинейная зонная пластина, состоящая из диэлектрика, заполненного чередующимися зонами насыщаемого поглощающего материала, может выступать в качестве оптического ограничителя малой мощности. Используя квантовые точки в качестве примера насыщаемого поглотителя, авторы статьи с помощью вычислений разработали ультратонкий оптический ограничитель с пороговой интенсивностью всего 0,45 кВт/см². Этот порог на несколько порядков меньше, чем те, которые наблюдаются в современных оптических ограничителях на основе плоской оптики. Конструкция нелинейной зонной пластины может позволить создавать ультратонкие оптические ограничители и потенциально найти широкое применение там, где требуется нелинейная фокусировка [24].

Проанализирована работа об оптическом ограничителе на кремниевой фотонике на основе ультракомпактного волновода VO_2/Si . Данное экспериментальное устройство длиной 20 мкм имеет тепловую перестраиваемую пороговую мощность всего $\sim 3,5$ мВт, будучи спектрально широкополосным. В работе предлагается новый путь для создания интегральных оптических ограничителей для плотных и маломощных фотонных интегральных схем. Сильный оптический нелинейный отклик VO_2 может быть использован для достижения ультракомпактных и широкополосных оптических ограничителей на кремниевой фотонике с перестраиваемой производительностью. Эффективное тепловое смещение на кристалле может быть легко достигнуто с помощью микронагревателей с низкими потерями, в то время как пороговая мощность устройства может быть сконструирована путем легирования VO_2 с целью изменения температуры перехода. С другой стороны, ожидается, что время включения такого устройства при фототермическом возбуждении составит около нескольких микросекунд. Начиная с VO_2 является CMOS-совместимым материалом, данное исследование открывает возможности для включения такого строительного блока в плотные, с низким энергопотреблением и DWDM-фотонные интегрированные приложения [25].

На основании анализа работ в сфере изучения узкополосных фильтров можно сделать вывод, что в контексте предлагаемых контрмер к атаке импульсным лазерным излучением наиболее оптимальным на данный момент является продолжение исследований в области изучения DWDM и брэгговских решёток.

В основе оптического ограничителя располагается среда, обладающая нелинейностями третьего порядка, которые изменяют показатель преломления среды или ее поглощение при прохождении мощного света. Так как квантовая криптография основана на пересылке одиночных фотонов, но при этом большинство атак на системы используют как раз яркий свет, идея использовать оптические предохранители кажется очень логичной. Однако на рынке сегодня не существует коммерчески доступных оптических предохранителей.

Кроме того, как показано в работе [26], параметры нелинейного показателя преломления составляют $10^{-16} - 10^{-6} \text{ см}^2/\text{Вт}$ при временах реакции порядка $10^{-15} - 10^{-3} \text{ с}$. Причем самый слабый эффект дает самый быстрый процесс электронной поляризации, а самый сильный эффект дает самый медленный процесс термического расширения. И даже лучшие на сегодняшний день оптические ограничители [25, 27] не способны закрыть проблему полностью.

Нелинейный компонент оптического ограничителя из работы [27] основан на термическом эффекте, то есть часть приходящего света поглощается в компоненте, он разогревается и меняет свой показатель преломления. Основным минусом ограничителя можно считать заложенные в нем аттенюации в однофотонном режиме (20 дБ), низкую скорость реакции (порядка десятков мс) и высокий порог нелинейности (порядка мВт). Дополнительная аттенюация компонента может значительно понизить скорость передачи ключа. Обсуждался вариант его установки в передатчик, где согласно протоколу и так должно быть значительное ослабление лазера до однофотонных импульсов. Однако, если использовать термический элемент, как аттенюатор, то для безопасности системы нужно также вводить и замерять дополнительный параметр – температуру в помещении. Напрашивается атака, где злоумышленник через вентиляцию охлаждает температуру в помещении на 1-2 градуса, что изменяет показатель преломления и уменьшает потери на ограничителе, а значит, система генерирует уже не однофотонные импульсы.

И хотя оптические ограничители показывают себя сегодня как довольно не стабильный компонент для коммерческого использования, активно ведутся работы по снижению их чувствительности. Работа ведется по двум направлениям: синтез новых материалов с улучшенными свойствами нелинейности [28, 29] и средствам уплотнения излучения. Уплотнением в основном занимаются в одномодовом волокне [30] и в так называемых фотонных кристаллах [31]. В работе [32] показано, что с помощью одномерного фотонного кристалла можно повысить чувствительность оптического ограничителя в 20-30 раз в сравнении с нелинейной средой. Есть технические возможности заказать изготовление одномерных фотонных кри-

сталлов для создания на их основе оптических ограничителей, расчет технических параметров данного проекта сейчас ведется. После проверки их свойств пропускания, будут также проведены тесты на лазерное повреждение.

Использование пассивного предохраняющего элемента

Это может быть дополнительный аттенюатор либо компонент, сгорающий при атаке лазерным повреждением, тем самым разрывая квантовую связь. С одной стороны, может казаться, что добавление элемента усложняет схему, с другой стороны, это, напротив, разгружает функциональность крайнего компонента. Так, аттенюатор, циркулятор или узкополосный фильтр могут защищать систему от атак Троянским конем, засевом лазера и т.д., тогда как предохранитель будет защищать только от лазерного повреждения. Однако такие устройства являются в своем большинстве экспериментальными (например, [33-35]), поэтому подбор такого предохранителя для каждой системы КРК требует индивидуального подхода, зависящего от параметров системы.

В качестве предохранителей используют добавочный аттенюатор, либо приваренный участок легированного волокна. Интересно, что в легированном волокне на длине волны 1550 нм (телекоммуникационный стандарт для квантовой криптографии) поглощение порядка десятков дБ/см. Поэтому его использование разумно применять только в отправителе и учитывать его потери.

Здесь аналогично предыдущему пункту нужно убедиться, что:

- предохранитель работает независимо от длины волны подаваемого света.
- предохранитель работает независимо от длительности подаваемого импульса. Если с постоянным светом почти всегда нагревается крайний элемент схемы, то короткий импульс может пройти крайний компонент и повредить следующий за ним. Это наблюдалось, например, в работе [36];
- аналогично оптическим ограничителям легированное волокно следует проверить на предмет ослепления. Так, если при некоторой мощности волокно начинает пропускать больше света, чем изначально, то посылки перестают быть однофотонными, а значит, нарушается доказательство безопасности всей системы.
- также довольно сложно подобрать размер волокна, пока что в экспериментах это значение плюс минус 1 см, то есть плюс минус несколько дБ, что очень грубо для доказательства безопасности. Вероятно, потребуется алгоритм подстройки аттенюации в отправителе исходя из аттенюации в предохранителе. Этот алгоритм (пока даже не начатый) также потребуется тестировать на возможность вмешательства злоумышленника.

Проводились эксперименты с дополнительными аттенюаторами в качестве предохранителей. Так, в работе [37] было показано, что некоторые аттенюаторы выгорают при действии яркого света.

В качестве оптических предохранителей возможно использование оптического волокна, легированного редкоземельными элементами (РЗЭ). Наличие работ по данной теме крайне ограничено [38-42].

Для определения наиболее перспективных легирующих добавок были рассмотрены исследования спектров поглощения световодов, легированных РЗЭ, в широком диапазоне длин волн.

Использование Tm^{3+} -световода с диаметрами сердцевины/оболочки 105/125 мкм позволяет эффективно устранить (на 15 – 40 дБ) нежелательное излучение на длине волны 1530 – 1600 нм мощностью как минимум до 10 Вт при низких (менее 0,5 дБ) потерях на длине волны накачки (915 – 981 нм). 064, 915 или 1400 нм при длине волны накачки 808 нм. Световоды, легированные ионами Tm^{3+} , могут обеспечить защиту в случае эрбиевых и эрбий-иттербиевых лазеров, излучающих в спектральном диапазоне 1530 – 1600 нм при накачке в области 915 – 981 нм.

Использование Tm³⁺-световода с диаметрами сердцевины/оболочки 105/125 мкм позволяет эффективно устранить (на 15 – 40 дБ) нежелательное излучение на длине волны 1530 – 1600 нм мощностью как минимум до 10 Вт при низких (менее 0,5 дБ) потерях на длине волны накачки (915 – 981 нм) [38].

Дополнительные выводы возможны после проведения соответствующих экспериментов и обработки результатов.

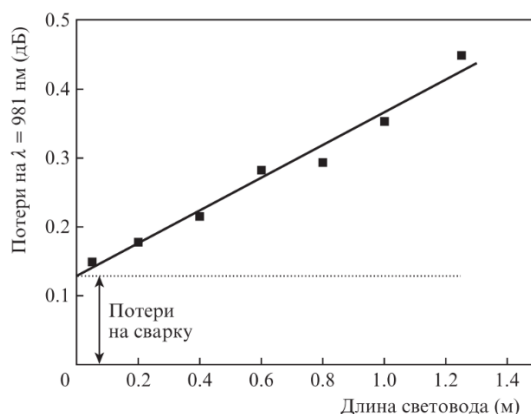


Рисунок 11 – Зависимость внесенных Tm³⁺-световодом потерь на распространение от его длины, измеренная при максимальной мощности излучения на 981 нм.

Точки – эксперимент, сплошная линия – линейная аппроксимация

Figure 11 – The dependence of the propagation losses introduced by Tm³⁺ fiber on its length, measured at maximum radiation power of 981 nm.

Points – experiment, solid line – linear approximation

Температурная зависимость постоянной Верде и изоляции в волоконно-оптических изоляторах

Оптический изолятор – это компонент, который допускает только однонаправленную передачу оптического сигнала. Он состоит из входного поляризатора, вращателя Фарадея и выходного поляризатора, называемого анализатором.

Оптическая ось второго поляризатора ориентирована под углом $\beta = 45^\circ$ по отношению к первому поляризатору. В этой конфигурации оптический сигнал, поступающий с левой стороны, проходит через первый поляризатор, оптическая ось которого находится в вертикальном направлении, что соответствует поляризации входного оптического сигнала. Затем вращатель Фарадея поворачивает поляризацию оптического сигнала на 45° по часовой стрелке. Если имеется введенный лазерный луч из оптической схемы на правой стороне, этот оптический сигнал должен проходить через вращатель Фарадея справа налево.

Поскольку ротатор Фарадея является невзаимным устройством, состояние поляризации отраженного оптического сигнала будет вращаться еще на 45° в том же направлении, что и входной сигнал, становясь, таким образом, перпендикулярным к оптической оси первого поляризатора.

Как показано выше, оптический изолятор основан на эффекте Фарадея [42]. Плоскость поляризации линейно поляризованный световой пучок при распространении в магнитооптическом кристалле поворачивается на угол θ . Направление вращения зависит от направления магнитного поля, а не от направления распространения света. Связь между углом поворота поляризации и магнитным полем в кристалле равна

$$\Theta = V(\lambda, T)BL, \quad (1)$$

где B – продольная составляющая магнитного поля в Т, L – длина пути, на котором свет и магнитное поле взаимодействуют в м, а $V(\lambda, T)$ – постоянная Верде, зависящая от длины волны распространяющегося света λ и температуры магнитооптического кристалла T в рад/(Т*м). Далее рассмотрим только температурную зависимость.

Температурная зависимость постоянной Верде и, следовательно, угла поворота Фарадея приводит к изменению коэффициента изоляции в зависимости от температуры. Современные одномодовые изоляторы обладают высокой стабильностью изоляции в диапазоне температур от 5 до 70 °С. Тепловыми эффектами можно пренебречь для типичных оптических схем, таких как системы QKD, с мощностью лазера менее 300-500 МВт. Однако когда мощный лазер подается в обратном направлении, его излучение частично поглощается внутри изолятора и вызывает нагрев магнитооптического кристалла. Температурная зависимость константы Верде вызывает изменение угла поворота плоскости поляризации [см. уравнение (1)]. Для оптических изоляторов это означает уменьшение коэффициента изоляции в обратном направлении и потерю мощности и ухудшение качества луча в прямом направлении. Тепловые эффекты могут быть смягчены тщательным выбором магнитооптического материала в компоненте [36]. Наиболее распространенными материалами для одноступенчатого волоконного изолятора в ближнем инфракрасном диапазоне являются редкоземельные гранаты. Здесь будут рассмотрены следующие различные типы гранатов: железо-иттриевый гранат (YIG), тербий-галлиевый гранат (TGG) и железо-иттриевый гранат, замещенный висмутом (Bi:YIG).

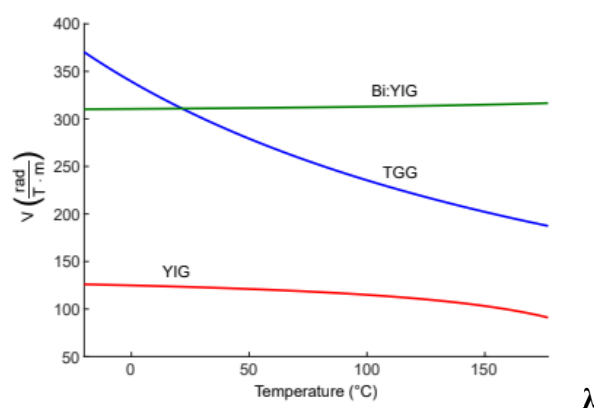


Рисунок 12 – Температурная зависимость константы Верде для TGG, YIG и Bi:YIG при длине волны 1550 нм

Figure 12 – Temperature dependence of the Verde constant for TIG, TIG and Bi:YIG at a wavelength of 1550 nm

В общем случае на константу Верде редкоземельного граната влияют несколько различных вкладов. В данном случае рассматриваются только зависящие от температуры вклады: парамагнитный вклад V_{pm} и частотно-независимый гиромагнитный член V_{gm} .

Постоянная Верде как функция температуры имеет вид

$$V(T) = V_{pm}V_{gm} = -\frac{A\lambda_0^2}{(T - T_\omega)} + \frac{B}{T - T_\omega} + C, \quad (2)$$

где λ_0^2 – длина волны доминирующего электронного перехода, T_ω – температура Кюри, а A, B, C – константы, зависящие от свойств выбранного материала.

С учетом данных получена зависимость постоянной Верде в диапазоне температур от -20 до 175 °С, как показано на рисунке 12. Эти зависимости были рассчитаны при фиксированной рабочей длине волны $\lambda = 1550$ нм. Как показано на рисунке 12, кристалл TGG продемонстрировал наименьшую стабильность в зависимости от температуры. Это означает, что изоляторы на основе TGG являются наиболее чувствительными к тепловым воздействиям при $\lambda = 1550$ нм.

Изоляторы на основе YIG или Bi:YIG должны быть более термостойкими.

Модель изоляции

Далее мы анализируем изменение изоляции при изменении температуры кристалла в предложенной модели с идеальным поляризатором и анализатором. Плоскости поляризации

поляризатора и анализатора ориентированы относительно друг друга под углом β , а вращатель Фарадея обеспечивает угол 45° вращение плоскости поляризации распространяющегося света с центральной длиной волны 1550 нм. В данной модели магнитное поле является постоянным и не зависит от температуры (но в реальных системах магнитное поле может вносить изменения в изоляцию). Согласно закону Малюса, после прохождения через вращатель Фарадея и поляризатор интенсивность пучка плоскополяризованного света изменяется как $I = I_0 \cos^2(\theta + \beta)$, где I_0 – начальная интенсивность. Затем коэффициент изоляции определяется как $\alpha = -10 \log \cos^2(\beta + \theta)$. (Вносимые потери могут быть найдены по аналогичной формуле с использованием углов поворота, равных $(\beta - \theta)$). После подстановки значения θ из уравнения (1) температурная зависимость будет равна

$$\alpha(T) = -10 \log \left[\beta + \frac{V(T)}{V(25^\circ \text{C})} \cdot k \right], \quad (3)$$

где k – коэффициент, зависящий от начального значения изоляции при температуре 25°C . Далее используется начальное значение изоляции 40 дБ, как типичное значение для одноступенчатых изоляторов при комнатной температуре в диапазоне от 32 до 40 дБ в соответствии с их спецификацией. Изоляция 40 дБ соответствует углу поворота плоскости поляризации во вращателе Фарадея либо $\theta = 44,43^\circ$, либо $\theta = 45,57^\circ$, в зависимости от направления вращения. Результаты расчета изоляции и вносимых потерь представлены на рисунке 16.

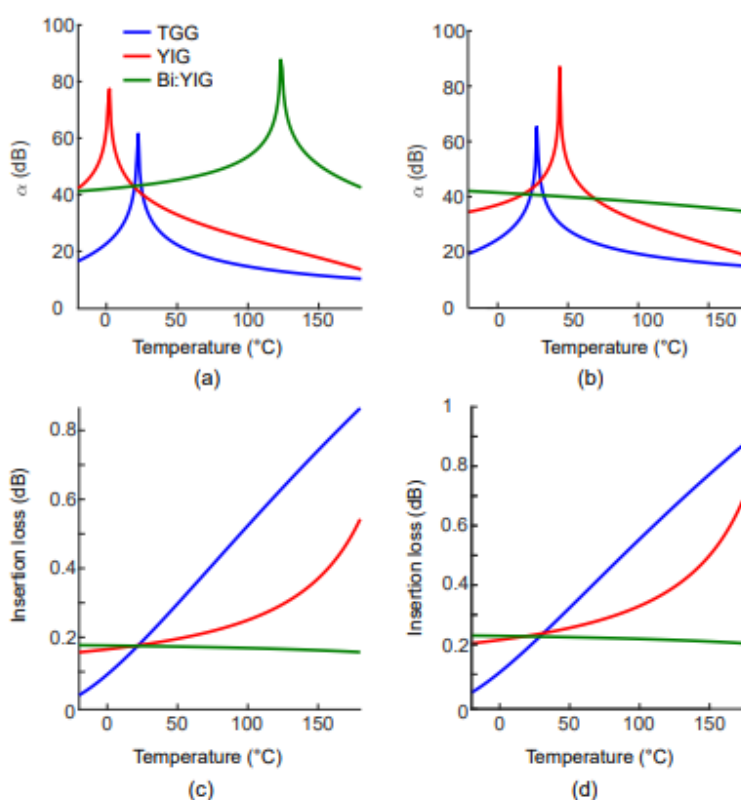


Рисунок 13 – Зависимость коэффициента изоляции (a) и (b) и вносимых потерь (c) и (d) от температуры для TGG, YIG и Bi:YIG. (a) и (c) соответствуют $\theta = 44,43^\circ$; (b) и (d) соответствуют $\theta = 45,57^\circ$
Figure 13 – The dependence of insulation coefficient (a) and (b) and insertion losses (c) and (d) on temperature for TGG, YIG and Bi:YIG. (a) and (c) correspond to $\theta = 44,43^\circ$; (b) and (d) correspond to $\theta = 45,57^\circ$

Модель предсказывает резкие пики значения изоляции. Следует отметить, что, как правило, в данных экспериментальных результатах нет выраженных пиков коэффициента изоляции при нагреве компонентов лазером. Это может быть объяснено внутренним рассеянием

в кристалле, которое приводит к частичному изменению плоскости поляризации. Однако этот фактор не учитывается в данной модели.

Результаты моделирования

Данная модель показывает, что изменение коэффициента изоляции с температурой сильно зависит от материала магнитооптического кристалла, хотя каждый гранат может обеспечивать одинаковое значение изоляции при комнатной температуре. Кристалл TGG продемонстрировал самое резкое снижение коэффициента изоляции в рабочем температурном диапазоне изоляторов. Это связано с тем, что рабочий диапазон длин волн для этого граната составляет от 700 до 1100 нм. Кристалл Bi:YIG специально разработан для применений, требующих высоких значений коэффициента изоляции в широком диапазоне температур. Согласно расчетам, коэффициент изоляции составляет более менее 40 дБ в диапазоне температур от -20 до 180 °С. Такая высокая стабильность изолятора достигается благодаря оптимальному кристаллическому составу [38]. Дополнительное легирование создает несколько подрешеток в кристаллической структуре, которые компенсируют температурную зависимость константы Верде (и изоляции соответственно) друг от друга. В YIG эта модель предсказывает, что изоляция уменьшается примерно на 10 дБ при 70 °С. При значительном повышении температуры (до 175°С) уровень изоляции падает примерно до 15 дБ.

Полученный результат хорошо согласуется с экспериментальными данными для ISO PM 2. Сравнение эксперимента с моделью показано на рисунке 17.

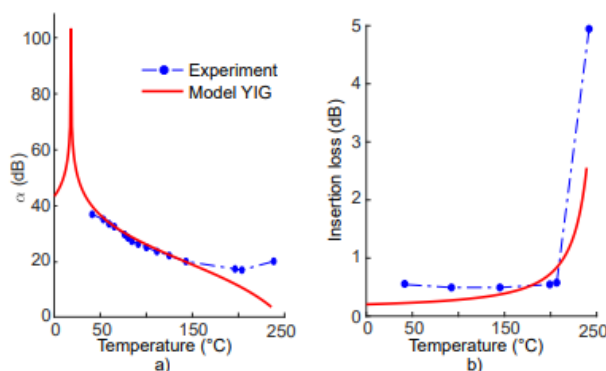


Рисунок 14 – Сравнение экспериментальных результатов для ISO PM 2 и модель для YIG с $\theta = 44,43^\circ$, для (а) коэффициента изоляции и (б) вносимых потерь
Figure 14 – Comparison of experimental results for ISO PM 2 and model for YIG with $\theta = 44.43^\circ$, for (a) insulation coefficient and (b) insertion loss

Таким образом, данная модель показывает, что Bi:YIG имеет самую слабую зависимость коэффициента изоляции от температуры и, следовательно, гранат является наиболее оптимальным для изоляторов, устойчивых к лазерному повреждению. Кроме того, можно предположить, что магнитооптический кристалл в изоляторе ISO PM 2 является YIG [21].

Заключение

Системы квантового распределения ключей требуют дополнительного уровня защиты в виде одного или нескольких компонентов, которые могут ограничивать спектральный состав проходящего в системе квантового распределения ключей излучения. В работе рассмотрены конкретные контрмеры, обеспечивающие защиту систем квантового распределения ключа от атак импульсным лазерным излучением.

Выводы.

В качестве мер защиты от атак лазерного повреждения для систем квантового распределения ключей возможно использование следующих компонентов:

– изоляторы – пассивные оптические элементы, пропускающие свет в одном направлении и не пропускающие в обратном;

- циркуляторы – пассивные оптические элементы с тремя портами: из 1-го порта свет идет во 2-й порт, из 2-го в 3-й, из 3-го в 1-й;
- узкополосные фильтры – пассивные оптические элементы, пропускающие излучение конкретной длины волны;
- оптический предохранитель – это пассивный оптический элемент с нелинейным отношением мощности пропусканием;
- добавление активного наблюдения за лазерным излучением.

Применение данных компонентов целесообразно при атаках на передающее и приёмное оборудование легитимных пользователей.

Библиографический список

1. **Nielsen M., Chang I.**, «Quantum computing and quantum information», М. «Mir», 2006.
2. **Bennett C.H., Brassard G.**, Quantum Cryptography: Public key distribution and cointossing, Proc. Int. Conf. Computer systems and Signal Processing, pp. 175-179, Bangalore 1984.
3. **Bennett C. H., Bessette F., Brassard G., Salvail L. and Smolin J.**, Experimental Quantum Cryptography, J. Cryptol. 5 (3), 1992.
4. **Muller A., Zbinden H., Gisin N.**, Quantum cryptography over 23 km in installed under lake Telecom fiber, Europhys. Lett. 33 (5), pp. 335-339, (1996).
5. **Marand Ch. and Townsend P. D.**, Quantum key distribution over distances as long as 30 km, Opt. Lett. 20 (16), pp. 1695-1697, 1995.
6. **Hughes R. J., Alde D. M., Dyer P., Luther G. G., Morgan G.L. and Schauer M.**, quantum cryptography, Contemporary Phys. 36 (3), pp. 149-163, 1995.
7. **Wiechers C., Lydersen L., Wittmann C., Elser D., Skaar J., Marquardt C., Makarov V., Leuchs G.** After-gate attack on a quantum cryptosystem. New Journal of Physics. 2011, vol. 13, no. 1, pp. 013043. doi: 10.1088/1367-2630/13/1/013043
8. **Bugge A. N., Sauge S., Ghazali A. M. M., Skaar J., Lydersen L., Makarov V.** Laser Damage Helps the Eavesdropper in Quantum Cryptography. Physical Review Letters. 2014, vol. 112, no. 7, pp. 070503. doi: 10.1103/PhysRevLett.112.070503
9. **Pang X.-L., Yang A.-L., Zhang C.-N., Dou J.-P., Li H., Gao J., Jin X.-M.** Hacking Quantum Key Distribution via Injection Locking. Physical Review Applied. 2020, vol. 13, no. 3, pp. 034008. doi: 10.1103/PhysRevApplied.13.034008
10. **Sun S.-H., Xu F., Jiang M.-S., Ma X.-C., Lo H.-K., Liang L.-M.** Effect of source tampering in the security of quantum cryptography. Physical Review A. 2015, vol. 92, no. 2, pp. 022304. doi: 10.1103/PhysRevA.92.022304
11. **Jain N., Anisimova E., Khan I., Makarov V., Marquardt C., Leuchs G.** Trojan-horse attacks threaten the security of practical quantum cryptography. New Journal of Physics. 2014, vol. 16, no. 12, pp. 123030. doi: 10.1088/1367-2630/16/12/123030
12. **Huang A., Navarrete Á., Sun S.-H., Chaiwongkhot P., Curty M., Makarov V.** Laser-Seeding Attack in Quantum Key Distribution. Physical Review Applied. 2019, vol. 12, no. 6, pp. 064043. doi: 10.1103/PhysRevApplied.12.064043
13. **Ruzhitskaya D., Ponomova A., Johlinger F., Chaiwongkhot P., Egorov V., Aktas D., Rarity J. G., Erven C., Makarov V., Huang A.** Protecting QKD sources against light-injection attacks. [Электронный ресурс]. URL: <http://www.vadl.com/publications/ruzhitskaya2020>. QCrypt-subm43.pdf, свободный. Яз. англ. (дата обращения 20.10.2021).
14. **Lucamarini M., Yuan Z. L., Dynes J. F., and Shields A. J.** «Overcoming the rate-distance limit of quantum key distribution without quantum repeaters», Nature 557, 400 (2018).
15. **Sun S.-H., Xu F., Jiang M.-S., Ma X.-C., Lo H.-K., Liang L.-M.** Effect of source tampering in the security of quantum cryptography. Physical Review A. 2015, vol. 92, no. 2, pp. 022304. doi: 10.1103/PhysRevA.92.022304
16. **Lucamarini M., Choi I., Ward M. B., Dynes J. F., Yuan Z. L., Shields A. J.** Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution. Physical Review X. 2015, vol. 5, no. 3, pp. 031030. doi: 10.1103/PhysRevX.5.031030
17. **Tan H., Li W., Zhang L., Wei K., Xu F.** Chip-Based Quantum Key Distribution against Trojan-Horse Attack. Physical Review Applied. 2021, vol. 15, no. 6, pp. 064038. doi: 10.1103/PhysRevApplied.15.064038

18. **Makarov V., Bourgoin J.-P., Chaiwongkhot P., Gagné M., Jennewein T., Kaiser S., Kashyap R., Legré M., Minshull C., Sajeed S.** Creation of backdoors in quantum communications via laser damage // *Physical Review A*. 2016, vol. 94, no. 3, pp. 030302. doi: 10.1103/PhysRevA.94.030302
19. **Huang A., Li R., Egorov V., Tchouragoulov S., Kumar K., Makarov V.** Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution. *Physical Review Applied*. 2020, vol. 13, no. 3, pp. 034017. doi: 10.1103/PhysRevApplied.13.034017
20. **Ponosova A., Ruzhitskaya D., Chaiwongkhot P., Egorov V., Makarov V., Huang A.** Protecting fiber-optic quantum key distribution sources against light-injection attacks [Электронный ресурс]. URL: <https://arxiv.org/pdf/2201.06114.pdf>,
21. **Ruzhitskaya D., Ponosova A., Johlinger F., Chaiwongkhot P., Egorov V., Aktas D., Rarity J. G., Erven C., Makarov V., Huang A.** Protecting QKD sources against light-injection attacks. [Электронный ресурс]. URL: <http://www.vad1.com/publications/ruzhitskaya2020.QCrypt-subm43.pdf>
22. **Hui Liu, Zong-Wen Yu, Mi Zou, Yan-Lin Tang, Yong Zhao, Jun Zhang, Xiang-Bin Wang, Teng-Yun Chen, and Jian-Wei Pan** Experimental 4-intensity decoy-state quantum key distribution with asymmetric basis-detector efficiency *Phys. Rev. A* 100, 042313 (2019)
23. **Xiu-Xiu Xia, Zhen Zhang, Hong-Bo Xie, Xiao Yuan, Jin Lin, Sheng-Kai Liao, Yang Liu, Cheng-Zhi Peng, Qiang Zhang, and Jian-Wei Pan** LED-based fiber quantum key distribution: toward low-cost applications *Photonics Research*, vol. 7, is. 10, pp. 1169-1174 (2019)
24. **Yuqi Zhao, Hamidreza Chalabi, and Edo Waks** A Low Power Threshold, Ultrathin Optical Limiter Based on a Nonlinear Zone Plate Optics *Express*, vol. 29, Is. 21, pp. 33144-33154 (2021)
25. **Jorge Parra, Juan Navarro-Arenas, Mariela Menghini, Maria Recaman, Jean Pierre-Locquet, and Pablo Sanchis** Low-threshold power and tunable integrated optical limiter based on an ultracompact VO₂/Si waveguide *APL Photonics* 6, 121301 (2021)
26. **Peter Gunter**, *Nonlinear Optical Effects and Materials*. Springer Series in Optical Sciences, vol. 72, 2000.
27. **Gong Zhang, Ignatius William Primaatmaja, Jing Yan Haw, Xiao Gong, Chao Wang, and Charles Ci Wen Lim.** «Securing practical quantum communication systems with optical power limiters», *PRX Quantum* 2,030304 (2021).
28. **Ziyue Guo, Kailin Hu, Tao Cao, Shaozhen Liu, Jikun Yan, Zhou Li, Qi Xu, Paul B. Corkum, and Jiahui Peng**, «Energy deposition and incubation effects of nonlinear absorption of ultrashort laser pulses in dielectrics», *Opt. Express* 30, 10317-10328 (2022).
29. **Diego S. Manoel, André G. Pelosi, Leandro H. Zucolotto Cocca, Gustavo F.B. Almeida, Lucas F. Sciuti, Ruben D.F. Rodriguez, Luizmar Adriano Junior, Rosa S. Lima, Caridad Noda-Perez, Felipe T. Martins, Marcio A.R. Souza, Pablo J. Gonçalves, Tertius L. Fonseca, Leonardo de Boni, Cleber R. Mendonça**, «Second- and third-order nonlinear optical properties of mono-substituted terpenoid-like chalcones», *J. Photochem. Photobiol. A Chem.*, vol. 429, 113898, 2022.
30. **Chao Liu, Guoru Li, Yiran Wang, Xiancui Su, Yiyang Xie, Feilong Gao, Santosh Kumar, Bingyuan Zhang**, «Near-infrared All-fiber Mode-locked laser Based on Vanadium Carbide Nanosheets», *Optik*, 168792, 2022.
31. **Reena Gadhwal, Parul Kaushik, Ambika Devi**, «A review on 1D photonic crystal based reflective optical limiters», *Critical Reviews in Solid State and Materials Sciences*, 2022.
32. **Ryzhov, A. A.** «Optical Limiting Performance of a GaAs/AlAs Heterostructure Microcavity in the nearInfrared», *Appl. Opt.* 2017, 56, pp. 5811-5816.
33. **Anwar S., M. Raja A., Qazi S., Ilyas M.** *Nanotechnology for Telecommunications* (1st. ed.). 2017. CRC Press, Inc., USA.
34. **Mizuno Y., Hayashi N., Tanaka H., Nakamura K., Todoroki Sh.-ic.** Observation of polymer optical fiber fuse. *Appl. Phys. Lett.* 104. 043302. 2014. <https://doi.org/10.1063/1.4863413>
35. **Tomlinson R. G.** United States Patent US3433555A March 18, 1969.
36. **Makarov Vadim, Bourgoin Jean-Philippe, Chaiwongkhot Poompong, Gagné Mathieu, Jennewein Thomas, Kaiser Sarah, Kashyap Raman, Legré Matthieu, Minshull Carter, and Sajeed Shihan**, «Creation of backdoors in quantum communications via laser damage», *Phys. Rev. A* 94, 030302, 2016.
37. **Ruzhitskaya D. D., Zhluktova I. V., Petrov M. A., Zaitsev K. A., Acheva P. P., Zunikov N. A., Shilko A. V., Aktas D., Johlinger F., Trefilov D. O., Ponosova A. A. Kamynin V. A., and Makarov V. V.** «Vulnerabilities in the quantum key distribution system induced under a pulsed laser attack», *Sci. Tech. J. Inf. Technol. Mech. Opt.* 21, 837 p. (2021).

38. Кочергина Т. А., Алешкина С. С., Худяков М. М., Яшков М. В., Липатов Д. С., Абрамов А. Н., Исхакова Л. Д., Бубнов М. М., Гурьянов А. Н., Лихачев М. Е. «Использование редкоземельных элементов для создания спектрально-селективного поглощения в мощных волоконных лазерах», Квантовая электроника, 48:8 (2018), с. 733-737.

39. Грux Д. А., Курков А. С., Раздобреев И. М., Фотиади А. А. Квантовая электроника, 32, 1017 (2002) [Quantum Electron., 32, 1017 (2002)]

40. Kotov L. V., Aleshkina S. S., Khudyakov M. M., Bubnov M. M., Medvedkov O. I., Lipatov D. S., Guryanov A. N., Likhachev M. M. J. Lightwave Technol., 35, 4540 (2017)

41. Aleshkina S. S., Levchenko A. E., Medvedkov O. I., Bobkov K. K., Bubnov M. M., Lipatov D. S., Guryanov A. N., Likhachev M. E. IEEE Photon. Technol. Lett., 30, 127 (2018)

42. Denker B. I., Egorova O. N., Galagan B. I., Kamynin V. A., Ponomova A. A., Sverchkov S. E., Semjonov S. L., Tsvetkov V. B. Laser Phys. Lett., 14, 075101 (2017).

UDC 004.942:001.57

MODELING OF THE BEHAVIOR OF SECURITY ELEMENTS UNDER THIRD-PARTY INFLUENCE ON THE PASSIVE COMPONENTS OF QUANTUM KEY DISTRIBUTION SYSTEM

E. V. Borisova, postgraduate student, RSREU, Ryazan, Russia;
orcid.org/0000-0002-0198-377X, e-mail: Ekaterina21333@yandex.ru

In cryptography, security can be ensured by exchanging a secret key between two users, who are called Alice (the source) and Bob (the receiver). In quantum cryptography, key exchange is carried out via a quantum channel. Its security is based on the fact that any measurement of a quantum system will inevitably change the state of this system. Consequently, a third party, Eva, can get information from the quantum channel by performing a measurement, but legitimate users will detect it and, therefore, will not use the key. In practice, a quantum system is a single photon propagating through an optical fiber, and the key can be encoded by its polarization or by its phase, as was first proposed by Bennett and Brassard [1]. In 1992, quantum cryptography was first experimentally demonstrated at a height of more than 30 cm in the air with polarized photons [2]. Since then, several groups have presented implementations of both polarization [3] and phase coding schemes in optical fibers [4-5].

However, modern implementations of KRC systems do not correspond to their model concepts, and an attacker has the opportunity to intercept the secret key and remain unnoticed [6-11].

Quantum communication protocols are considered secure provided that all devices included in the system are fully characterized and side channels are closed. However, as a result of exposure to laser radiation, it is possible to change the characteristics of components of quantum communication systems, which leads to vulnerabilities in quantum key distribution system.

The aim of the work is the possibility of applying the conclusions from this article in the practical assessment of the security of quantum communication systems – the assessment quantum key distribution systems security. The work contains recommendations on strengthening the security of signal source block in quantum communication systems. As countermeasures to protect against the effects of laser radiation, it is proposed to use optical fuses with a given threshold power limit, detectors for monitoring the input power of optical radiation and narrow-band optical filters at the entrance to the quantum communication system [12]. This article collects data and provides characteristics when using these components as security elements.

Key words: quantum connection, quantum communication, quantum cryptography, vulnerabilities of quantum communication systems, laser damage attack, quantum key distribution systems.

DOI: 10.21667/1995-4565-2022-82-118-135

References

1. Nielsen M., Chang I. *Quantum computing and quantum informatio*. M. «Mir», 2006.
2. Bennett C.H., Brassard G., Quantum Cryptography: Public key distribution and cointossing, Proc. Int. Conf. Computer systems and Signal Processing, pp. 175-179, Bangalore 1984.

3. **Bennett C. H., Bessette F., Brassard G., Salvail L. and Smolin J.** *Experimental Quantum Cryptography*, J. Cryptol. 5 (3), 1992.
4. **Muller A., Zbinden H., Gisin N.**, Quantum cryptography over 23 km in installed under lake Telecom fiber, *Europhys. Lett.* 33 (5), pp. 335-339, (1996).
5. **Marand Ch. and Townsend P. D.**, Quantum key distribution over distances as long as 30 km, *Opt. Lett.* 20 (16), pp. 1695-1697, 1995.
6. **Hughes R. J., Alde D. M., Dyer P., Luther G. G., Morgan G.L. and Schauer M.**, quantum cryptography, *Contemporary Phys.* 36 (3), pp. 149-163, 1995.
7. **Wiechers C., Lydersen L., Wittmann C., Elser D., Skaar J., Marquardt C., Makarov V., Leuchs G.** After-gate attack on a quantum cryptosystem. *New Journal of Physics*. 2011, vol. 13, no. 1, pp. 013043. doi: 10.1088/1367-2630/13/1/013043
8. **Bugge A. N., Sauge S., Ghazali A. M. M., Skaar J., Lydersen L., Makarov V.** Laser Damage Helps the Eavesdropper in Quantum Cryptography. *Physical Review Letters*. 2014, vol. 112, no. 7, pp. 070503. doi: 10.1103/PhysRevLett.112.070503
9. **Pang X.-L., Yang A.-L., Zhang C.-N., Dou J.-P., Li H., Gao J., Jin X.-M.** Hacking Quantum Key Distribution via Injection Locking. *Physical Review Applied*. 2020, vol. 13, no. 3, pp. 034008. doi: 10.1103/PhysRevApplied.13.034008
10. **Sun S.-H., Xu F., Jiang M.-S., Ma X.-C., Lo H.-K., Liang L.-M.** Effect of source tampering in the security of quantum cryptography. *Physical Review A*. 2015, vol. 92, no. 2, pp. 022304. doi: 10.1103/PhysRevA.92.022304
11. **Jain N., Anisimova E., Khan I., Makarov V., Marquardt C., Leuchs G.** Trojan-horse attacks threaten the security of practical quantum cryptography. *New Journal of Physics*. 2014, vol. 16, no. 12, pp. 123030. doi: 10.1088/1367-2630/16/12/123030
12. **Huang A., Navarrete Á., Sun S.-H., Chaiwongkhot P., Curty M., Makarov V.** Laser-Seeding Attack in Quantum Key Distribution. *Physical Review Applied*. 2019, vol. 12, no. 6, pp. 064043. doi: 10.1103/PhysRevApplied.12.064043
13. **Ruzhitskaya D., Ponomova A., Johlinger F., Chaiwongkhot P., Egorov V., Aktas D., Rarity J. G., Erven C., Makarov V., Huang A.**, *Protecting QKD sources against light-injection attacks*. [Elektronnyj resurs]. URL: http://www.vad1.com/publications/ruzhitskaya2020_QCrypt-subm43.pdf, свободный. Яз. англ. (дата обращения 20.10.2021).
14. **Lucamarini M., Yuan Z. L., Dynes J. F., and Shields A. J.** «Overcoming the rate-distance limit of quantum key distribution without quantum repeaters», *Nature* 557, 400 (2018).
15. **Sun S.-H., Xu F., Jiang M.-S., Ma X.-C., Lo H.-K., Liang L.-M.** Effect of source tampering in the security of quantum cryptography. *Physical Review A*. 2015, vol. 92, no. 2, pp. 022304. doi: 10.1103/PhysRevA.92.022304
16. **Lucamarini M., Choi I., Ward M. B., Dynes J. F., Yuan Z. L., Shields A. J.** Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution. *Physical Review X*. 2015, vol. 5, no. 3, pp. 031030. doi: 10.1103/PhysRevX.5.031030
17. **Tan H., Li W., Zhang L., Wei K., Xu F.** Chip-Based Quantum Key Distribution against Trojan-Horse Attack. *Physical Review Applied*. 2021, vol. 15, no. 6, pp. 064038. doi: 10.1103/PhysRevApplied.15.064038
18. **Makarov V., Bourgoin J.-P., Chaiwongkhot P., Gagné M., Jennewein T., Kaiser S., Kashyap R., Legré M., Minshull C., Sajeed S.** Creation of backdoors in quantum communications via laser damage. *Physical Review A*. 2016, vol. 94, no. 3, pp. 030302. doi: 10.1103/PhysRevA.94.030302
19. **Huang A., Li R., Egorov V., Tchouragoulov S., Kumar K., Makarov V.** Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution. *Physical Review Applied*. 2020, vol. 13, no. 3, pp. 034017. doi: 10.1103/PhysRevApplied.13.034017
20. **Ponomova A., Ruzhitskaya D., Chaiwongkhot P., Egorov V., Makarov V., Huang A.** *Protecting fiber-optic quantum key distribution sources against light-injection attacks* [Elektronnyj resurs]. URL: <https://arxiv.org/pdf/2201.06114.pdf>,
21. **Ruzhitskaya D., Ponomova A., Johlinger F., Chaiwongkhot P., Egorov V., Aktas D., Rarity J. G., Erven C., Makarov V., Huang A.**, *Protecting QKD sources against light-injection attacks*. [Elektronnyj resurs]. URL: http://www.vad1.com/publications/ruzhitskaya2020_QCrypt-subm43.pdf
22. **Hui Liu, Zong-Wen Yu, Mi Zou, Yan-Lin Tang, Yong Zhao, Jun Zhang, Xiang-Bin Wang, Teng-Yun Chen, and Jian-Wei Pan** Experimental 4-intensity decoy-state quantum key distribution with asymmetric basis-detector efficiency *Phys. Rev. A* 100, 042313 (2019).

23. Xiu-Xiu Xia, Zhen Zhang, Hong-Bo Xie, Xiao Yuan, Jin Lin, Sheng-Kai Liao, Yang Liu, Cheng-Zhi Peng, Qiang Zhang, and Jian-Wei Pan. LED-based fiber quantum key distribution: toward low-cost applications *Photonics Research*, vol. 7, is. 10, pp. 1169-1174 (2019)
24. Yuqi Zhao, Hamidreza Chalabi, and Edo Waks *A Low Power Threshold, Ultrathin Optical Limiter Based on a Nonlinear Zone Plate Optics Express*, vol. 29, Is. 21, pp. 33144-33154 (2021)
25. Jorge Parra, Juan Navarro-Arenas, Mariela Menghini, Maria Recaman, Jean Pierre-Locquet, and Pablo Sanchis. Low-threshold power and tunable integrated optical limiter based on an ultracompact VO₂/Si waveguide *APL Photonics* 6, 121301 (2021)
26. Peter Gunter, Nonlinear Optical Effects and Materials. *Springer Series in Optical Sciences*, vol. 72, 2000.
27. Gong Zhang, Ignatius William Primaatmaja, Jing Yan Haw, Xiao Gong, Chao Wang, and Charles Ci Wen Lim. «Securing practical quantum communication systems with optical power limiters», *PRX Quantum* 2,030304 (2021).
28. Ziyue Guo, Kailin Hu, Tao Cao, Shaozhen Liu, Jikun Yan, Zhou Li, Qi Xu, Paul B. Corkum, and Jiahui Peng, «Energy deposition and incubation effects of nonlinear absorption of ultrashort laser pulses in dielectrics», *Opt. Express* 30, 10317-10328 (2022).
29. Diego S. Manoel, André G. Pelosi, Leandro H. Zucolotto Cocca, Gustavo F.B. Almeida, Lucas F. Sciuti, Ruben D.F. Rodriguez, Luizmar Adriano Junior, Rosa S. Lima, Caridad Noda-Perez, Felipe T. Martins, Marcio A.R. Souza, Pablo J. Gonçalves, Tertius L. Fonseca, Leonardo de Boni, Cleber R. Mendonça, «Second- and third-order nonlinear optical properties of mono-substituted terpenoid-like chalcones», *J. Photochem. Photobiol. A Chem.*, vol. 429, 113898, 2022.
30. Chao Liu, Guoru Li, Yiran Wang, Xiancui Su, Yiyang Xie, Feilong Gao, Santosh Kumar, Bingyuan Zhang, «Near-infrared All-fiber Mode-locked laser Based on Vanadium Carbide Nanosheets», *Optik*, 168792, 2022.
31. Reena Gadhwal, Parul Kaushik, Ambika Devi, «A review on 1D photonic crystal based reflective optical limiters», *Critical Reviews in Solid State and Materials Sciences*, 2022.
32. Ryzhov, A. A. «Optical Limiting Performance of a GaAs/AlAs Heterostructure Microcavity in the nearInfrared», *Appl. Opt.* 2017, 56, pp. 5811-5816.
33. Anwar S., M. Raja A., Qazi S., Ilyas M. *Nanotechnology for Telecommunications* (1st. ed.). 2017. CRC Press, Inc., USA.
34. Mizuno Y., Hayashi N., Tanaka H., Nakamura K., Todoroki Sh.-ic. Observation of polymer optical fiber fuse. *Appl. Phys. Lett.* 104. 043302. 2014. <https://doi.org/10.1063/1.4863413>
35. Tomlinson R. G. United States Patent US3433555A March 18, 1969.
36. Makarov Vadim, Bourgoin Jean-Philippe, Chaiwongkhot Poompong, Gagné Mathieu, Jennewein Thomas, Kaiser Sarah, Kashyap Raman, Legré Matthieu, Minshull Carter, and Sajeed Shihan, «Creation of backdoors in quantum communications via laser damage», *Phys. Rev. A* 94, 030302, 2016.
37. Ruzhitskaya D. D., Zhlyuktova I. V., Petrov M. A., Zaitsev K. A., Acheva P. P., Zunikov N. A., Shilko A. V., Aktas D., Johlinger F., Trefilov D. O., Ponosova A. A. Kamynin V. A., and Makarov V. V. «Vulnerabilities in the quantum key distribution system induced under a pulsed laser attack», *Sci. Tech. J. Inf. Technol. Mech. Opt.* 21, 837 p. (2021).
38. Kochergina T. A., Aleshkina S. S., Khudyakov M. M., Yashkov M. V., Lipatov D. S., Abramov A. N., Iskhakova L. D., Bubnov M. M., Guryanov A. N., Likhachev M. E. «The use of rare-earth elements to create spectral-selective absorption in high-power fiber lasers», *Quantum Electronics*, 48:8 (2018), 733-737.
39. Gruk D. A., Kurkov A. S., Razdobreev I. M., Fotiadi A. A. *Quantum Electronics*, 32, 1017 (2002) *Quantum Electron.*, 32, 1017 (2002).
40. Kotov L. V., Aleshkina S. S., Khudyakov M. M., Bubnov M. M., Medvedkov O. I., Lipatov D. S., Guryanov A. N., Likhachev M. M. *J. Lightwave Technol.*, 35, 4540 (2017).
41. Aleshkina S. S., Levchenko A. E., Medvedkov O. I., Bobkov K. K., Bubnov M. M., Lipatov D. S., Guryanov A. N., Likhachev M. E. *IEEE Photon. Technol. Lett.*, 30, 127 (2018)
42. Denker B. I., Egorova O. N., Galagan B. I., Kamynin V. A., Ponosova A. A., Sverchkov S. E., Semjonov S. L., Tsvetkov V. B. *Laser Phys. Lett.*, 14, 075101 (2017).