Исследование уязвимости систем квантового распределения ключей от атак с лазерным повреждением элементов на основе нейтральных светофильтров

С. В. Алферов[+1)], *К. Е. Бугай*[*×], *И. А. Паргачев*[+]

[+]*АО ИнфоТеКС, 127273 Москва, Россия*

[*]*ООО СФБ Лаб, 127273 Москва, Россия*

[×]*МГТУ им. Н. Э. Баумана, 105005 Москва, Россия*

Поступила в редакцию 23 мая 2022 г.
После переработки 2 июня 2022 г.
Принята к публикации 4 июня 2022 г.

Системы квантового распределения ключей (КРК) являются открытыми для нарушителя в том смысле, что помимо атаки на квантовые состояния, нарушитель может проводить атаку на оборудование. И если в первом случае уязвимости устраняются фундаментальными ограничениями (например, теорема о запрете клонирования) или есть теоретические обоснования к их устранению, то во втором случае уязвимость зависит от практической реализации аппаратуры. Атака с лазерным повреждением оптических компонентов, именуемая в литературе как “Laser Damage Attak” (LDA), может позволить нарушителю уменьшить ослабление оптических элементов и привести к компрометации распределяемых ключей. В данной работе рассмотрен способ защиты от атаки с лазерным повреждением оптических компонентов на основе нейтральных светофильтров. Изложена схема, имитирующая действия злоумышленника во время проведения атаки LDA. Показан подход, позволяющий рассчитывать параметры оптических элементов в результате воздействия атаки. Проанализированы процессы, происходящие в образцах под действием мощного лазерного излучения. На основе экспериментальных данных был сделан вывод об устойчивости и ограничениях нейтральных светофильтров при использовании в системах КРК как средство противодействия от атаки LDA.

DOI: 10.31857/S1234567822140099, EDN: izmicg

1. Введение. Секретность КРК традиционно ассоциируется с фундаментальными законами квантовой механики. Однако зачастую практическая реализация имеет недостатки, которые создают уязвимость. Существует целый ряд работ, в которых описываются подобные уязвимости [1–3]. Часто системы КРК используют оптические импульсы, ослабленные до квазиоднофотонного уровня. Это достигается с помощью оптического аттенюатора, который может быть различных конфигураций. Так, в работе [4] было показано, что некоторые виды аттенюаторов устойчивы к атаке LDA, но с оговоркой на ограниченность длительности и мощности лазерного воздействия. В работе [5] показано, что нейтральный светофильтр с двухсторонним покрытием, выполняющий функцию аттенюатора, уязвим к атаке с лазерным повреждением элементов при мощности выше 34 дБм. Уязвимость систем КРК в результате атаки LDA возникает от того, что под действием мощного лазерного излучения (со стороны ВОЛС) меняются характеристики оптических элементов, а именно, уменьшается их коэффициент ослабления. В результате открываются возможности для атаки с отщеплением фотонов (PNS) или для атаки с активным зондированием электрооптических элементов (THA). В свою очередь увеличение коэффициента ослабления уменьшает скорость выработки квантового ключа, приводит к росту ошибок QBER вплоть до полного прекращения генерации. Таким образом, существует актуальная задача поиска и создания оптических элементов, устойчивых к атакам с лазерным повреждением.

2. Тестирование на устойчивость к LDA. Тестирование оптического аттенюатора осуществлялось согласно схеме, продемонстрированной на рис. 1. Излучение контрольного лазера проходило в прямом направлении через изолятор и вводилось в волоконный светоделитель с коэффициентом деления света 90/10. Мощность контрольного лазера составляла 18 дБм и не менялась на протяжении все-

[1)]e-mail: Sergey.Alferov@infotecs.ru

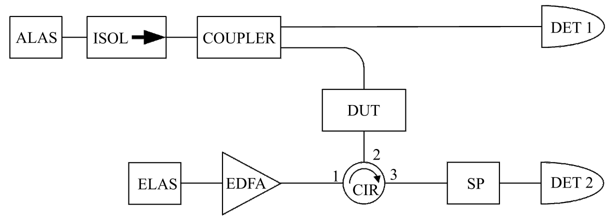

Рис. 1. Экспериментальная схема измерения. ALAS – контрольный лазер; ISOL – изолятор для мощного лазерного излучения; COUPLER – светоделитель 90/10; DET1 – измеритель мощности # 1 для детектирования излучения контрольного лазера; DUT – исследуемый образец; ELAS – атакующий лазер, EDFA – усилитель лазерного излучения; CIR – циркулятор (цифрами обозначены порты); SP – спектральный фильтр; DET2 – измеритель мощности # 2 для детектирования излучения контрольного лазера; прошедшего через образец

го эксперимента для того, чтобы можно было оценивать изменение ослабления исследуемых образцов. В измеритель мощности # 1 отводилось 10 % мощности излучения контрольного лазера, остальные 90 % мощности направлялись к исследуемому образцу. Изолятор предназначался для блокирования излучения, распространяющегося от светоделителя к выходу контрольного лазера. Измеритель мощности # 1 предназначался для контроля поступающей на исследуемый образец мощности от контрольного лазера. Излучение, имитирующее LDA (так называемое “атакующее излучение”), формировалось атакующим лазером и усилителем. Мощность атакующего излучения регулировалась коэффициентом усиления и варьировалась от 25 до 37.4 дБм. Излучение высокой мощности от усилителя вводилось в исследуемый образец через циркулятор, который, помимо маршрутизации, также служил для блокирования излучения, распространяющегося в обратном направлении от исследуемого образца к выходу усилителя.

Излучение контрольного лазера, прошедшее через исследуемый образец, направлялось с помощью циркулятора к измерителю мощности # 2. Кроме излучения контрольного лазера, к измерителю мощности # 2 также распространялось отраженное и рассеянное от элементов схемы излучение лазера, имитирующего атаку. С помощью спектрального фильтра излучение мощного лазера блокировалось, а излучение контрольного лазера проходило к измерителю мощности # 2. Согласно спектральной характеристике пропускания фильтра, подавление атакующего излучения составляло не менее 50 дБ. Длины волн атакующего и контрольного лазера устанавливались равными 1561 и 1547.3 нм. Исследуемый образец состоял из оснастки с двумя коллимирующими линзами с числовой апертурой 0.13 для ввода и вывода излучения из волокна в свободное пространство и обратно. Коллимированный пучок ослаблялся с помощью нейтрального светофильтра. Светофильтр представлял собой стеклянную пластину из стекла, окрашенного в массе (марка стекла СЗС-16). Исследовались светофильтры с оптической плотностью OD = 2.0 и 3.0 с диаметром 12 мм, толщиной 1.25 и 2 мм соответственно.

Ключевая идея использования предложенного аттенюатора заключается в снижении плотности мощности на светофильтре за счет коллиматоров, что, соответственно, повышает стойкость системы КРК к мощному излучению. Вторым важным обстоятельством является то, что у используемых светофильтров спектральная характеристика пропускания является плоской, что обеспечивает защиту в широком спектральном диапазоне [6]. Также к достоинствам исследуемого образца относится возможность быстрой замены и отсутствие дополнительных доработок при установке. К недостаткам можно отнести большие габариты оснастки и достаточно высокую стоимость по сравнению с другими вариантами защиты от атаки LDA.

Последовательность измерений проходила в несколько этапов:

1. Измерение начального ослабления света образцом до воздействия на него излучением высокой мощности.

2. Оценка шумовой составляющей, возникающей вследствие отражения и рассеяния атакующего излучения.

3. Измерение ослабления света образцом во время воздействия на него излучением высокой мощности.

При измерении начального ослабления образца определялась мощность контрольного лазера (полезный сигнал) в отсутствии атакующего излучения. Сбор данных с детекторов (здесь и далее) производился в течении одной минуты с периодом измерения 10 мс, с последующим вычислением среднего значения мощности в единицах дБм на обоих детекторах – P_1 и P_2 соответственно. Далее рассчитывалось ослабление (дБ):

$$A = P_1 + K_c - P_2 - A_s, \quad (1)$$

где K_c – коэффициент деления мощности между выходами светоделителя в дБ, A_s – потери на пути “выход светоделителя-Дет.2” в отсутствии исследуемого образца (дБ).

Для определения уровня шумовой составляющей, вследствие отражения и рассеяния атакующего излучения, контрольный лазер блокировался и в схему подавалось лазерное излучение мощностью 37.4 дБм. Наибольшая мощность шумовой составляющей для всех образцов светофильтров на детекторе # 2 составляла 79 дБм. Отличие полезного сигнала от шума составляло как минимум 41.4 дБ, поэтому шумовой составляющей в расчетах можно было пренебречь. Таким образом, расчет ослабления для каждого значения мощности атакующего излучения производился аналогичным образом по формуле (1). После оценки шумовой составляющей, излучение контрольного лазера разблокировалось и проводились измерения ослабления светофильтров при разных мощностях атакующего излучения, а именно, от 25 до 37.4 дБм с шагом 1 дБ.

На рисунке 2 представлен график ослабления нейтральных светофильтров # 1, 2 (OD = 2.0, толщина 1.25 мм) в зависимости от мощности атакующего излучения. Значение на оси ординат (здесь и далее) соответствует начальному значению ослабления. Из графика видно, что ослабление светофильтров не постоянно. На рисунке 3 показано изменение ослабления светофильтров # 1, 2 (так называемое “просветление”) относительно начального значения. При мощности атакующего излучения от 25 до 27 дБм ослабление относительно начального положительно, т.е. наблюдается уменьшение ослабления (увеличение пропускания) светофильтра. При дальнейшем росте мощности атакующего лазера от 27 до 37.4 дБм наблюдается увеличение ослабления светофильтра относительно начального. На рисунке 4 показан график ослабления светофильтра # 3 (OD = 3.0, толщина 2 мм) в зависимости от мощности атакующего излучения. На рисунке 5 показано изменение ослабления светофильтра относительно начального ослабления. Из графиков видно, что для данного образца наблюдается увеличение ослабления светофильтра во всем диапазоне мощности атакующего излучения.

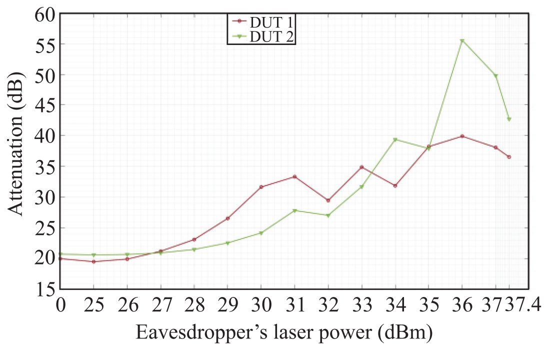

Рис. 2. (Цветной онлайн) Ослабления светофильтров # 1, 2 в зависимости от мощности атакующего излучения

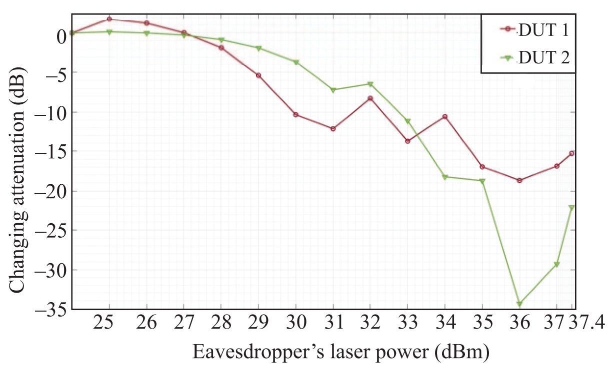

Рис. 3. (Цветной онлайн) Изменение ослабления светофильтров # 1, 2 относительно начального значения

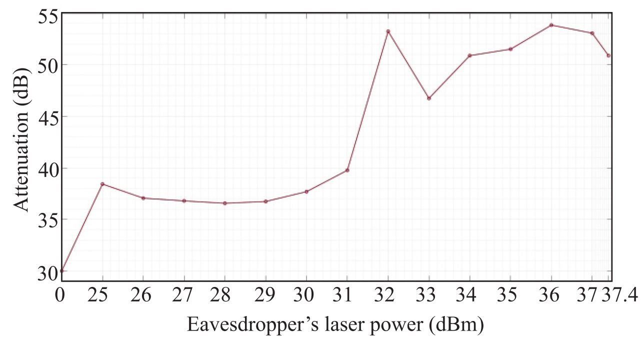

Рис. 4. (Цветной онлайн) Ослабление светофильтра # 3 в зависимости от мощности атакующего излучения

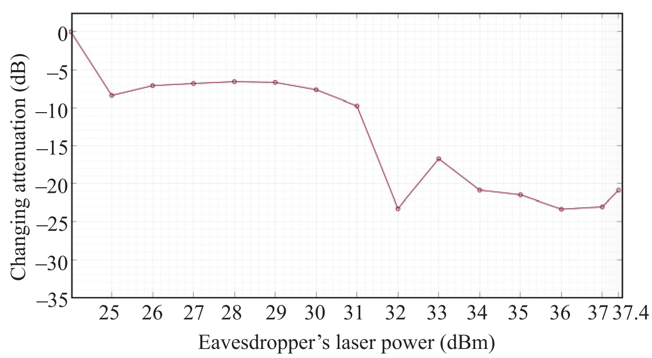

Рис. 5. (Цветной онлайн) Изменение ослабления светофильтра # 3 относительно начального значения

Уменьшение ослабления образцов # 1, 2 можно объяснить следующим образом. Согласно паспортным данным, потери оснастки в отсутствии светофильтра составляют порядка 1.5 дБ. При малых мощностях $(25 \div 26)$ дБм еще не происходит резкой деградации светофильтра, однако из-за нагрева возникает термооптический эффект, приводящий к формированию тепловой линзы [7]. Из-за этого происходит изменение траектории излучения внутри исследуемого образца. В результате такой “разъюстировки” потери в схеме уменьшаются, что интерпретируется как уменьшение ослабления. Другим возможным объяснением может быть то, что при нагреве светофильтра возникает смещение коротковолновой границы и полос поглощения в область более длинных волн, а также размывание полос поглощения [8]. Дальнейшее увеличение ослабления по мере возрастания мощности атакующего излучения, вероятно, связано с деформацией светофильтра, а именно, плавлением, образованием кратера и растрескиванием. Виден кратер круглой формы размером порядка 900 мкм (рис. 6), а также образовавшаяся трещина (рис. 7). На рисунке 8 показан увеличенный фрагмент, где видны неоднородности на границе оплавления кратера.

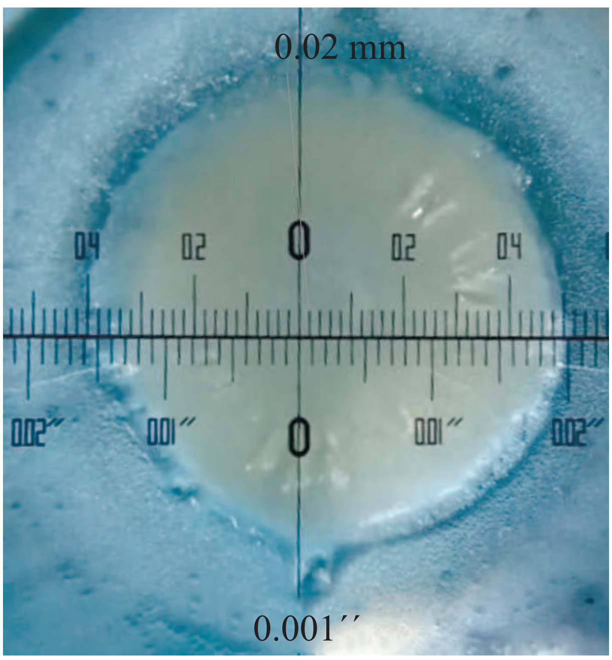

Рис. 6. (Цветной онлайн) Кратер в масштабе

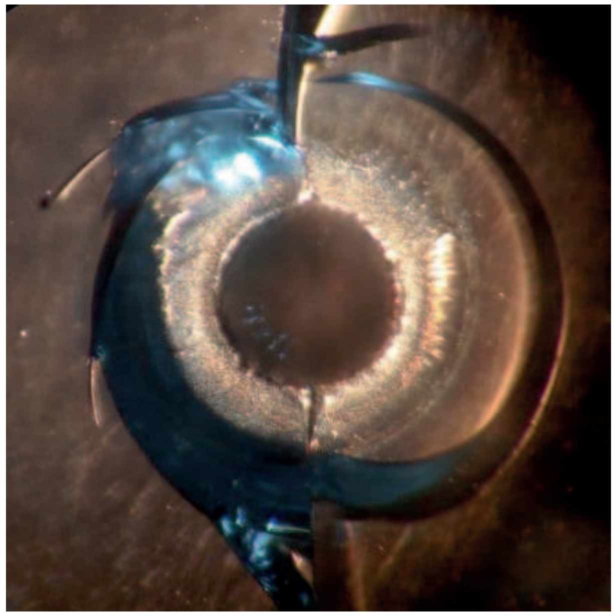

Рис. 7. (Цветной онлайн) Трещина вокруг кратера

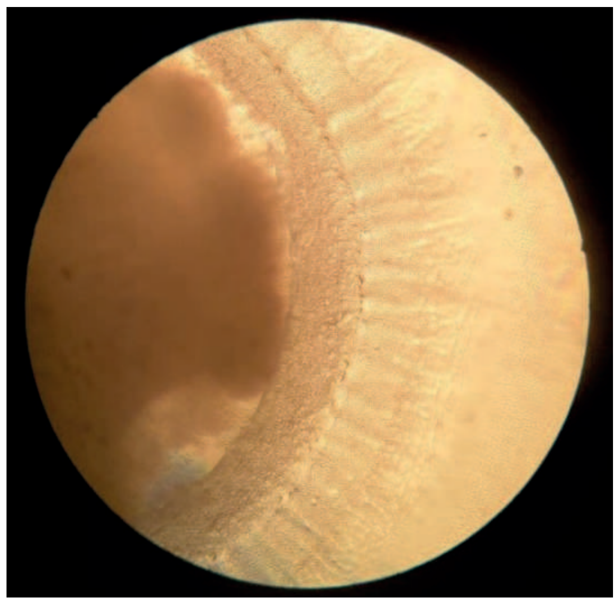

Рис. 8. (Цветной онлайн) Граница кратера

Для понимания процессов, происходящих с образцом во время воздействия атакующего излучения, оценим плотность мощности на его поверхности. Согласно [9] порог повреждения вследствие воздействия лазерного излучения (LIDT) для непрерывного излучения удобнее выражать в линейной плотности мощности (Вт/см), поскольку в таком случае этот порог не зависит от размера освещающего пучка. Для стекла СЗС-16 (зарубежный аналог KG3 Schott) порог повреждения составляет 25 Вт/см для длины волны 1064 нм. Согласно [10] пересчет порога повреждения для другой длины волны выражается через соотношение длин волн, поэтому для интересующей нас длины волны порог разрушения будет равен 36.4 Вт/см.

Оценим минимальную и максимальную плотности мощности, достигнутые в экспериментах. Для этого необходимо разделить мощность излучения на размер поперечного сечения пучка на поверхности светофильтра. С учетом числовой апертуры коллиматоров 0.13 и расстояния от коллиматора до светофильтра размер пучка составил порядка 1.3 мм, что хорошо согласуется с рис. 6. Подаваемый диапазон мощности, с учетом потерь в волоконном тракте равен $(24.5 \div 36.9)$ дБм, что соответствует $(0.3 \div 4.9)$ Вт. В таком случае линейная плотность мощности составляет $(2.2 \div 37.7)$ Вт/см, что свидетельствует о достижении порога повреждения на верхней границе диапазона. Отметим, что приведенные значения носят качественный характер, поскольку порог пробоя зависит от факторов, которые не учитывались в расчете, например, загрязнение поверхности образца.

Заключение. Проведенные эксперименты показали, что нейтральные светофильтры, окрашенные в массе, уязвимы к атаке с лазерным повреждением элементов (LDA) при мощности в диапазоне $(25 \div 27)$ дБм, поскольку в этом диапазоне наблюдается уменьшение ослабления. При дальнейшем росте мощности атакующего излучения происходит увеличение ослабления светофильтров. Была выявлена необратимая деградация светофильтра под действием мощного лазерного излучения, что на наш взгляд является причиной увеличения ослабления светофильтров. На основе экспериментальных данных было показано, что достигаемая в ходе эксперимента линейная плотность мощности превышает порог разрушения данной марки стекла. Отметим, что описанная атака является простейшей с точки зрения реализации, в том смысле что возможны гораздо более тонкие и малозаметные способы необратимо повредить оптические компоненты аппаратной части КРК.

Дальнейшая работа будет направлена на повышение стойкости светофильтров к мощному излучению. На наш взгляд наиболее оптимальными и действенными являются следующие соображения. Во-первых, следует увеличить теплоотвод с поверхности светофильтров с помощью принудительного или пассивного охлаждения. Второй способ заключается в увеличении пятна воздействия на светофильтр. Этого можно достичь увеличением числовой апертуры коллиматоров, либо увеличением расстояния между входным коллиматором и светофильтром. Третий способ заключается в подборе светофильтров с более высокими параметрами стойкости к лазерному воздействию. И последний фактор, который следует учитывать, это собственные потери оснастки – следует использовать оснастку с минимальными потерями.

1. A. Lamas-Linares, J. Opt. Express. **15**, 9388 (2007).
2. S. Sajeed, Phys. Rev. A **91**, 032326 (2015).
3. F. Xu, New J. Phys. **12**, 113026 (2010).
4. V. Makarov, Phys. Rev. Appl. **13**, 034017 (2020).
5. *POSTER SESSION (# 16)* [В Интернете]. Available: http://qutes.org/wp-content/uploads/2021/11/Poster_session.pdf [Дата обращения: 04 04 2022].
6. *Спектральные характеристики пропускания светофильтров из цветного стекла* [В Интернете]. Available: http://www.elektrosteklo.ru/Elektrosteklo_Color_Glass_Spectral_Transmittance.pdf, [Дата обращения: 04 04 2022].
7. J. Peñano, Ph. Sprangle, A. Ting, R. Fischer, B. Hafizi, and Ph. Serafim, J. Opt. Soc. Am. B **26**, 3 (2009).
8. В. А. Зверев, Е. В. Криповустова, Т. В. Точилина, *Оптические материалы*, Учебное пособие для конструкторов оптических систем и приборов, СПб НИУ ИТМО, СПб. (2013).
9. R. M. Wood, Optics and Laser Tech. **29**, 517 (1998).
10. *Unmounted NIR Absorptive ND Filters* [В Интернете] Available: https://www.thorlabs.com, [Дата обращения: 04 04 2022].