09.2;09.5;09.7

Исследование уязвимости систем квантового распределения ключей от атак с лазерным повреждением оптических компонентов на основе устройства с разрушающимся зеркалом

© *С.В. Алфёров*[1], *К.Е. Бугай*[2,3], *И.А. Паргачёв*[1], *Ю.В. Иванова*[2]

[1] АО „ИнфоТеКС“, Москва, Россия
[2] Московский государственный технический университет им. Н.Э. Баумана (Национальный исследовательский университет), Москва, Россия
[3] ООО „СФБ Лаборатория“, Москва, Россия
E-mail: Kirill.Bugay@sfblaboratory.ru

Поступило в Редакцию 20 октября 2022 г.
В окончательной редакции 20 октября 2022 г.
Принято к публикации 29 декабря 2022 г.

Атака на оборудование с лазерным повреждением оптических компонентов, именуемая в литературе „laser damage attack“, может позволить нарушителю уменьшить ослабление оптических элементов и привести к компрометации распределяемых ключей. Рассмотрен способ защиты от этой атаки на основе устройства с разрушающимся зеркалом. На основе экспериментальных данных сделан вывод об эффективности предложенного способа защиты.

Ключевые слова: квантовое распределение ключей, laser damage attack, злоумышленник, симметричная криптография.

DOI: 10.21883/PJTF.2023.05.54671.19399

В теории секретность систем квантового распределения ключей (КРК) гарантируется фундаментальными законами квантовой механики [1]. Однако на практике эти системы имеют различные уязвимости, которые зависят от архитектуры и используемого оборудования [2]. Любые действия нелегитимного пользователя, направленные на получение ключа шифрования, называются атакой. В большинстве систем КРК для формирования квантовых состояний используются оптические импульсы, ослабленные до квазиоднофотонного уровня с помощью оптического аттенюатора. Среднее число фотонов (СЧФ) в квантовых состояниях не должно превышать значения, заданного условиями безопасности протокола КРК, лежащего в основе секретности вырабатываемого ключа. Атака с лазерным повреждением оптических компонентов (laser damage attack, LDA) позволяет увеличить пропускание аттенюатора, что приводит к увеличению СЧФ в квантовых состояниях. В результате злоумышленник может узнать ключ и остаться незамеченным [3].

Отметим, что в ряде работ [4,5] были показаны некоторые виды аттенюаторов, которые демонстрируют устойчивость к LDA. Однако авторы отмечают, что устойчивость против LDA может быть нарушена при бóльших мощностях излучения или более длительном воздействии. Действительно, поскольку принцип работы указанных аттенюаторов основан на ослаблении пропускаемого излучения, потенциально блокирующий элемент может при упомянутых условиях разрушиться таким образом, что это приведет к возрастанию пропускания.

В настоящей работе предложено устройство ослабления излучения, которое может быть выполнено исключительно из оптоволоконных элементов. В отличие от упомянутых аттенюаторов описываемое нами устройство основано на отражении от зеркала, которое в процессе LDA разрушается, тем самым атакующее излучение выходит через зеркало наружу и не попадает на защищаемую аппаратуру. Схема устройства для противодействия LDA представлена на рис. 1.

При формировании квантовых состояний оптические импульсы поступают на вход устройства (*Input*) и направляются на входной порт волоконного оптического разветвителя 2×2 (*1* на рис. 1), разделяющего свет на две части. Первая часть света, прошедшего через разветвитель, направляется в поглотитель *2* и рассеивается в виде тепла. Вторая часть направляется к зеркалу *3*. Отраженный от зеркала свет возвращается к оптическому разветвителю, часть его направляется к выходу устройства (*Output*), а другая часть направляется в обратном направлении ко входу устройства.

Независимо от направления распространения света (от входа устройства к его выходу или наоборот) ослабление света составляет (в dB):

$$A = -10\lg\big((0.25 - \Delta k^2)(R_a + R + \Delta R)\big), \qquad (1)$$

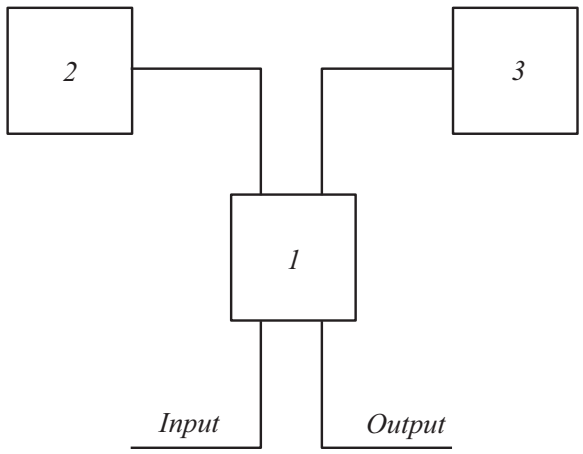

Рис. 1. Схема устройства с разрушающимся зеркалом. *1* — волоконный оптический разветвитель 2×2; *2* — поглотитель; *3* — разрушающееся зеркало.

где $\Delta k \in (-0.5; 0.5)$ — отклонение коэффициента деления света в оптическом разветвителе от 0.5; $R \in (0; 1]$ — коэффициент отражения мощности от зеркала; $\Delta R \in (-R; 1-R]$ — возможное изменение коэффициента отражения мощности от зеркала при проведении атаки злоумышленником; $R_a \in [0; 1]$ — коэффициент отражения мощности от поглотителя. Описанное устройство является интерферометром Майкельсона, в одном плече которого находится зеркало, а в другом — поглотитель. Однако отметим, что длительность квантовых состояний ограничена во времени. Таким образом, обеспечив достаточную разницу оптических длин путей света разветвитель–зеркало и разветвитель–поглотитель, можно добиться того, что отражения от зеркала и поглотителя не будут интерферировать. Это позволяет не брать в рассмотрение интерференционный член при выводе формулы (1). Далее будем считать, что до воздействия мощным излучением $\Delta k \neq 0$, $R_a = 0$ и $\Delta R = 0$. Соответственно при проведении LDA указанные параметры могут меняться таким образом, что это приведет к уменьшению ослабления устройства и откроет уязвимость для злоумышленника. Это означает, что при проектировании устройства необходимо оценить экспериментально или теоретически границы, которые могут принимать указанные параметры, затем с учетом этих границ на основе формулы (1) рассчитать ослабление A и сравнить его с ослаблением при отсутствии воздействия A_0. Если разница $\Delta A = A - A_0$ удовлетворяет заданному проектировщиком аппаратуры критерию (например, $\Delta A \geqslant 0$), то устройство считается стойким к LDA. В противном случае требуется поменять оптические элементы, отвечающие за параметры Δk, R_a и ΔR, с тем, чтобы выполнить условия заданного критерия.

Отметим, что ослабление света устройством тем меньше, чем ближе отклонение Δk к нулю, поэтому для увеличения стойкости к LDA значение начального коэффициента деления должно быть как можно ближе к 0.5 для длины волны, используемой в квантовых состояниях. Описанное устройство может дополняться другими аттенюаторами для получения необходимого СЧФ в квантовых состояниях на выходе передатчика.

В рамках исследования уязвимости систем КРК от LDA были изготовлены четыре образца устройств с разрушающимися металлическими зеркалами. Зеркала для образцов были изготовлены методом магнетронного напыления хрома на торец ферулы оптоволоконного коннектора (рис. 2, *a*). Толщина зеркальной металлической пленки составляла 150 ± 50 nm, при этом коэффициенты отражения излучения с длиной волны $\lambda = 1550$ nm были примерно равными $R \approx \{0.14; 0.12; 0.1; 0.1\}$ для образцов № 1–4 соответственно. Вносимое устройством ослабление составляло около 16 dB.

К положительным свойствам зеркал из хрома можно отнести то, что их спектральная характеристика отражения и поглощения является плоской [6] в широком диапазоне длин волн, что уменьшает возможности нарушителя повлиять на работу устройства, манипулируя длиной волны излучения. Также становится возможным использование одинаковых зеркал в устройствах, рассчитанных на работу с разными длинами волн, при этом ослабление света устройствами в нормальных условиях будет сохраняться. Кроме того, устройство выполнено без вывода излучения из волокна, что снижает технологические требования к изготовлению устройства и позволяет уменьшить его габариты.

Для проведения испытаний образцов использовались схема и последовательность измерений, соответствующие описанным в работах [4,5]. Основным отличием была меньшая мощность контрольного лазера, которая не вызывала разрушения зеркал при измерении начального ослабления образцов. Снимки торца ферулы с напыленным зеркалом до и после воздействия приведены на рис. 2, *b*, *c*.

На рис. 3 представлены зависимости ослабления исследуемых образцов от мощности атакующего излучения. Значения на оси ординат соответствуют начальному ослаблению, измеренному при выключенном атакующем лазере. Видно, что ослабление всех образцов увеличилось не менее чем на 24 dB и не уменьшалось ниже начального значения ослабления во всем диапазоне мощности атакующего излучения.

Таким образом, исследование показало, что для устройств с разрушающимся зеркалом наблюдается увеличение ослабления во всем диапазоне мощности атакующего излучения от 25 до 37.4 dBm. Отметим, что описанная атака является простейшей с точки зрения реализации в том смысле, что возможны гораздо более

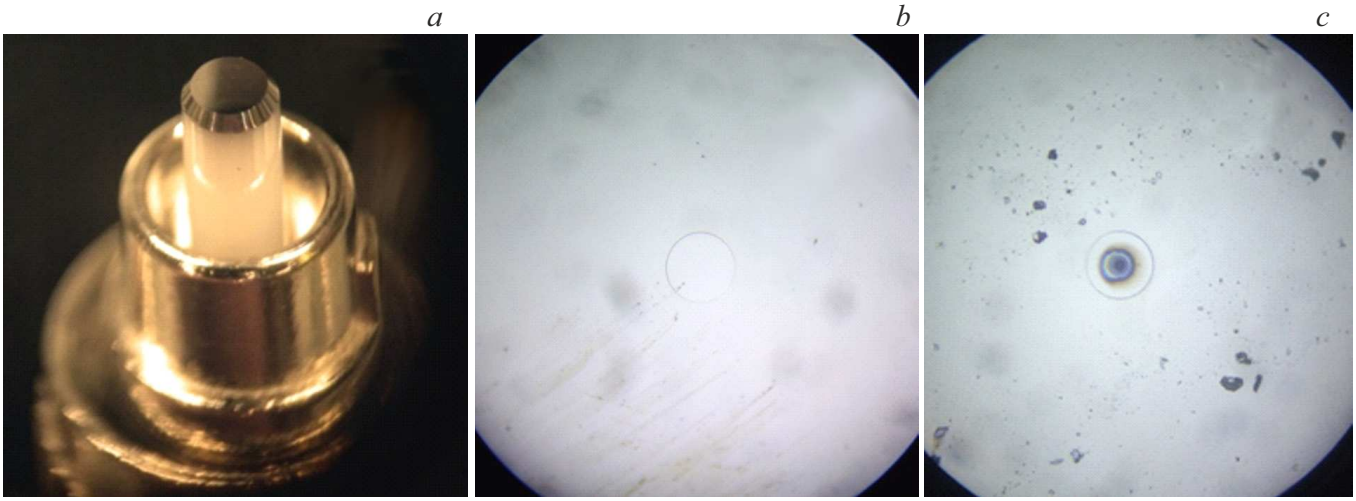

Рис. 2. *a* — металлическое зеркало на торце ферулы с прямой полировкой (PC); *b* — снимок зеркала под микроскопом до испытаний; *c* — снимок зеркала под микроскопом после испытаний.

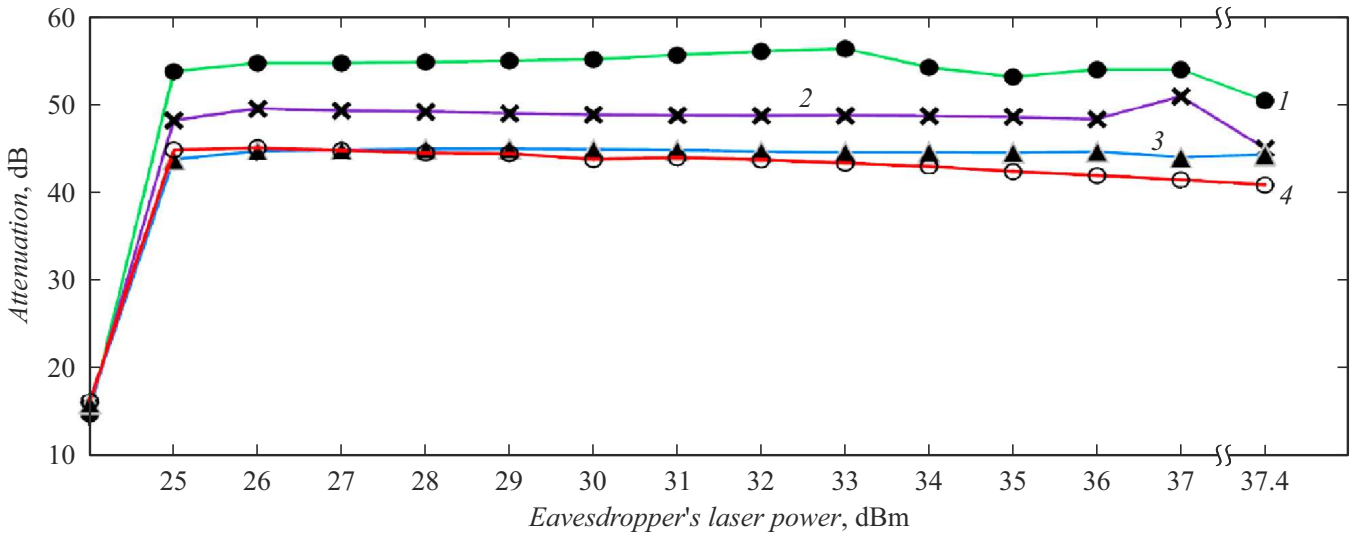

Рис. 3. Зависимость ослабления устройств с различными коэффициентами отражения зеркал от мощности атакующего излучения. Номера кривых соответствуют номерам образцов.

тонкие и малозаметные способы воздействия на оптические компоненты аппаратной части КРК.

Благодарности

Авторы выражают благодарность коллективу АО „ИнфоТеКС“ (Отделу квантовых технологий и Центру научных исследований и перспективных разработок), коллективу ООО „СФБ Лаборатория“ (Отделу специальных исследований и разработок), а также МГТУ им. Н.Э. Баумана (кафедрам „Математическое моделирование“ и „Лазерные и оптико-электронные системы специального назначения“) за полезные обсуждения.

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Список литературы

[1] И.М. Арбеков, *Элементарная квантовая криптография для криптографов, не знакомых с квантовой механикой* (URSS, M., 2022), с. 21.

[2] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, V. Makarov, Phys. Rev. Appl., **13** (3), 034017 (2020). DOI: 10.1103/PhysRevApplied.13.034017

[3] С.Н. Молотков, ЖЭТФ, **160** (3), 327 (2021). DOI: 10.31857/S0044451021090029 [S.N. Molotkov, JETP, **133** (3), 272 (2021). DOI: 10.1134/S1063776121080136].

[4] K.E. Bugai, A.P. Zyzykin, D.S. Bulavkin, S.A. Bogdanov, I.S. Sushchev, D.A. Dvoretskiy, in *2022 Int. Conf. Laser Optics (ICLO)* (St. Petersburg, 2022), p. 1. DOI: 10.1109/ICLO54117.2022.9839749
[5] С.В. Алфёров, К.Е. Бугай, И.А. Паргачёв, Письма в ЖЭТФ, **116** (2), 123 (2022). DOI: 10.31857/S1234567822140099 [S.V. Alferov, K.E. Bugai, I.A. Pargachev, JETP Lett., **116** (2), 123 (2022). DOI: 10.1134/S0021364022601117].
[6] A. Sytchkova, A. Belosludtsev, L. Volosevičienė, R. Juškėnas, R. Simniškis, Opt. Mater., **121**, 111530 (2021). DOI: 10.1016/j.optmat.2021.111530