17

Анализ эффективности методов защиты от атак активного оптического зондирования на волоконные системы квантового распределения ключей в спектральном диапазоне 1260—1650 nm

© А.В. Борисова[1], Б.Д. Гармаев[2], И.Б. Бобров[2], С.С. Негодяев[2], И.В. Синильщиков[2]

[1] ОАО „ИнфоТеКС“,
127287 Москва, Россия
[2] Центр квантовых технологий, Физический факультет МГУ имени М.В. Ломоносова,
119991 Москва, Россия

e-mail: borisova_alina_95@mail.ru, borisgar4481@mail.ru

Поступила в редакцию 14.01.2020 г.
В окончательной редакции 04.07.2020 г.
Принято к публикации 16.07.2020 г.

Представлены результаты исследования спектральных характеристик некоторых пассивных волоконно-оптических компонентов, таких как оптические изоляторы, циркуляторы, спектральные фильтры и мультиплексоры, используемых в системах квантового распределения ключей (КРК) и вносящих вклад в защиту аппаратуры квантового распределения ключей от атак активного оптического зондирования. Также приведена оценка требуемой степени изоляции, обеспечивающей надежную защиту системы КРК от атаки Trojan-horse при наименее благоприятных условиях для легитимных пользователей. На основе сформулированных требований и результатов измерений проанализирована эффективность защиты с помощью исследованных пассивных изолирующих компонентов. На примере расчета изоляции для приведенной в работе схемы системы КРК показано достижение требуемого уровня подавления излучения (150 dB) во всем рассматриваемом спектральном диапазоне.

Ключевые слова: квантовое распределение ключей, атака Trojan-horse, безопасность систем квантового распределения ключей, изоляция, спектры пропускания.

DOI: 10.21883/OS.2020.11.50182.4-20

Введение

Системы квантового распределения ключей (КРК) решают одну из задач классической криптографии — обеспечивают безопасную передачу ключа двум легитимным пользователям [1]. Абсолютная секретность распределения ключа основывается на фундаментальных законах квантовой физики [2,3]: невозможно извлечь информацию о квантовом состоянии (состоянии одиночного фотона), не нарушив это состояние и не скомпрометировав себя. Однако на практике безопасность ограничивается неидеальностями реализации систем КРК, что открывает возможность для осуществления различного рода атак [4]. Все атаки принято делить на атаки на протокол КРК и на техническую реализацию. Атаки на протокол оперируют с квантовыми состояниями, тогда как атаки на техническую реализацию направлены на элементы, входящие в состав аппаратуры. Чтобы избежать утечки информации к нарушителю (Еве) для каждого вида атаки разрабатываются специальные меры защиты.

В настоящей работе рассматриваются меры защиты от следующих атак на техническую реализацию: Trojan-horse и атаки с регистрацией переизлучений лавинных детекторов (Backflash) [5]. Атака Trojan-horse представляет собой оптическое зондирование кодирующего устройства (модулятора) и последующий анализ излучения, отраженного от разъемных соединений и других контактов оптических поверхностей внутри аппаратуры КРК [6]. При атаке Backflash нарушителем регистрируются фотоны, излученные детектором при регистрации квантовых состояний. Защита от этих атак осуществляется путем установки изолирующих пассивных оптических компонентов. Так как при атаке Trojan-horse используются импульсы высокой мощности, то требования к защитным изолирующим элементам более жесткие, чем к компонентам, блокирующим переизлучение детектора, поэтому далее эффективность защиты рассматривается на примере атаки Trojan-horse.

Для реализации атаки Trojan-horse нарушитель (Ева) каким-либо способом подсоединяется к оптической линии и посылает зондирующие лазерные импульсы таким образом, чтобы они проходили через кодирующее устройство в момент его работы, т. е. во время кодирования квантовых состояний (рис. 1). Часть этого импульса отражается от разъемных соединений и других контактов оптических поверхностей и направляется обратно к нарушителю. Ева проводит измерения зарегистрированных отраженных сигналов на предмет внесенной разности фаз (в случае зондирования фазового модулятора — PM) или амплитуды (в случае зондирования модулятора интенсивности) и в результате получает информацию о передаваемом состоянии.

Для обнаружения действий атакующего необходимо контролировать мощность входящего в систему излуче-

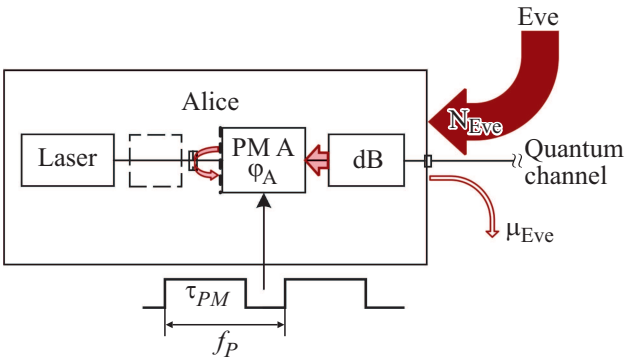

Рис. 1. Принцип реализации атаки Trojan-horse на систему КРК: Laser — источник излучения, PM A — кодирующее устройство (фазовый модулятор), dB — оптический аттенюатор (ATT), блок штриховой линией — вспомогательные элементы.

ния с помощью сторожевых детекторов (Guard PIN на рис. 2). В свою очередь, для защиты от зондирования, как говорилось ранее, устанавливаются изолирующие пассивные оптические компоненты (изоляторы (OI), циркуляторы (CIRC) и т. п.) между кодирующим устройством и выходом в квантовый канал. Однако так как технические возможности нарушителя (в данном случае уровень мощности и спектральный состав излучения) ограничены только законами физики, то для построения эффективных мер защиты необходимо знать минимальный требуемый уровень изоляции и учитывать спектральные характеристики пропускания оптических компонентов.

В работах [6,7] приведены спектральные характеристики некоторых оптических элементов, из анализа которых сделан вывод, что использование одиночного OI или CIRC для защиты от зондирования в широком спектральном диапазоне неэффективно. Поэтому требуется дополнительный спектрально селективный элемент, например полосовой спектральный фильтр, для подавления излучения с длинами волн, лежащими вне рабочего диапазона OI. При этом рассмотрены спектры только двух оптических элементов: OI и CIRC. При подборе элементной базы для защиты от атаки Trojan-horse помимо характеристик основных защитных элементов стоит учитывать спектры пропускания остальных оптических компонентов, расположенных на пути зондирующих импульсов. Такими элементами могут быть аттенюаторы (ATT), разветвители, спектральные мультиплексоры (WDM), контроллеры поляризации и др. Стоит также отметить, что характеристики оптических элементов различных производителей могут значительно отличаться. Наибольшие вариации наблюдаются в характеристиках спектральных фильтров: меняются не только ширина полосы пропускания, но и уровень подавления близких частот и наличие побочных максимумов пропускания.

В настоящей работе мы приводим оценку степени изоляции, требуемой для защиты от атаки Trojan-horse и результаты измерения спектров пропускания различных оптических элементов и их комбинаций: OI, CIRC, полосовых фильтров, WDM. Выбор конкретных моделей оптических элементов обоснован наличием этих моделей в исследовательской лаборатории. Представленные характеристики могут использоваться для подбора элементной базы и для оценки эффективности используемых мер защиты от атак оптического зондирования.

Требования к уровню изоляции

Для оценки эффективности мер защиты нужно определить минимальный уровень регистрируемого Евой сигнала, из которого она может извлечь достаточно информации о ключе. Затем необходимо рассчитать требуемый уровень суммарных потерь на прямом и обратном проходе, ослабляющих излучение до уровня ниже рассчитанного для Евы порога. Суммарные потери на двойном проходе будем называть уровнем изоляции (ISO).

Принято считать, что Ева обладает максимальными техническими возможностями, не нарушающими законы физики. Однако можно выделить диапазон длин волн и диапазон мощностей зондирующих импульсов, при которых атака Евы в принципе имеет смысл. Спектральный диапазон излучения Евы при зондировании PM ограничен снизу длиной волны отсечки оптического волокна (OB), равной 1260 nm (для излучения более коротких длин волн OB не является одномодовым). В случае многомодового режима извлечение информации о фазе представляется невозможным, так как наблюдаемый выходной сигнал является результатом интерференции между различными модами, непредсказуемым в силу непостоянства внешних условий (температурных и механических воздействий) [8,9]. Однако данная граница актуальна только для фазового кодирования, для других типов кодирования возможна реализация атаки и в многомодовом режиме, т. е. при меньших длинах волн. Ограничением сверху, в свою очередь, является длина волны вблизи 2000 nm: для излучения с большей длиной волны характерно возрастание поглощения в диоксиде кремния и перетекание энергии в оболочку оптоволокна, а значит, большие потери на изгибах [10].

Для эффективного проведения атаки зондирующие импульсы должны иметь высокую мощность, но не приводить при этом к разрушению оптической системы. Иными словами, максимальная мощность зондирующих импульсов ограничена порогом разрушения волокна или волоконно-оптических компонентов системы. Известно, что с уменьшением времени воздействия излучения данный порог снижается [11,12]. При увеличении длительности импульса появляется часть излучения, не содержащая информацию о фазе. Следовательно, оптимальная длительность зондирующих импульсов совпадает с длительностью импульса PM, $\tau_E = \tau_{PM}$. При этом наиболее благоприятные условия для нарушителя возникают, если PM работает в непрерывном режиме.

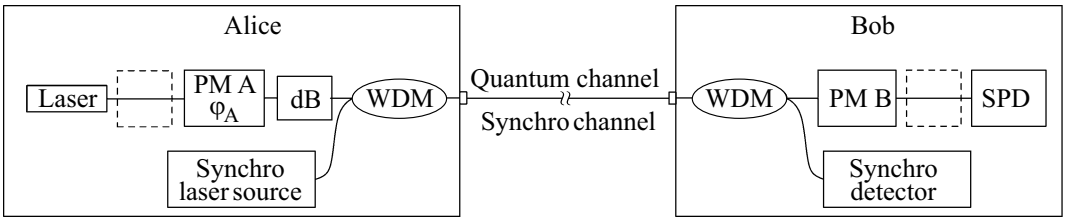

Рис. 2. Оптическая схема передающей системы КРК с защитными элементами против атаки Trojan horse (THA).

По данным последних исследований [13] пороговая мощность разрушения волокна составляет 9–10 W, что соответствует $N_{\text{th}} = (7.0–7.8) \cdot 10^{19}$ ph/s/50 μm^2, где 50 μm^2 — площадь сечения сердцевины волокна. Для удобства расчетов и для учёта наиболее жёстких условий округлим пороговое значение до целого в большую сторону, т. е. $N = 10^{20}$ ph/s/50 μm^2.

Таким образом, далее рассматривается наихудший для легитимных пользователей вариант реализации атаки и наиболее благоприятный для нарушителя, при котором:

— Ева посылает в систему зондирующие импульсы мощностью, близкой к порогу разрушения;

— PM в системе КРК работает в непрерывном режиме, т. е. длительность импульсов обратно пропорциональна частоте их следования f_p:

$$\tau_{\text{PM}} = \frac{1}{f_p}.$$

Для оценки необходимой степени подавления оптического сигнала помимо максимальной мощности зондирующих импульсов необходимо знать максимальное среднее число фотонов в зондирующем импульсе, регистрируемом нарушителем. В работе [11] показано, что при максимальном среднем числе фотонов в зондирующем импульсе на выходе системы КРК, равном $\mu_{\text{E}} = 10^{-6}$ ph/pulse, скорость выработки секретного квантового ключа на линиях более 100 km для протоколов BB84 и BB84 с состояниями-ловушками практически не отличается от скорости выработки ключа при отсутствии зондирующего импульса ($\mu_{\text{E}} = 0$).

На рис. 3 представлена упрощенная схема однопроходной системы КРК с фазовым кодированием и спектральным мультиплексированием квантового канала и канала синхронизации. Для защиты от атаки Trojan-horse необходимо, чтобы степень изоляции, обеспечиваемая компонентами системы, находящимися на пути зондирующих импульсов, т. е. между PM и оптическим выходом, удовлетворяла условию

$$iso > \frac{N\tau_{\text{PM}}R}{\mu}, \qquad (1)$$

где R — коэффициент отражения на соединениях.

Для каждой конкретной системы КРК необходимо рассчитывать требуемый уровень изоляции отдельно. Далее мы приводим оценку минимальной требуемой изоляции в наиболее жестких условиях для легитимных

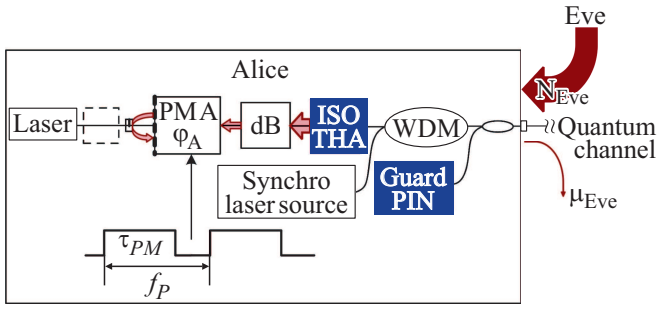

Рис. 3. Обобщенная оптическая схема однопроходной системы КРК. Здесь Laser — источник когерентного излучения, PM A — устройство кодирования квантовых состояний в передающем модуле, dB — оптический аттенюатор (ATT), WDM — спектральный мультиплексор, Synchro laser source — лазерный источник импульсов синхронизации, PM B — устройство кодирования квантовых состояний в приёмной модуле, SPD — детектор одиночных фотонов, Synchro detector — детектор импульсов синхронизации, блок в штриховой линии — вспомогательные элементы.

пользователей. Как показано в работах [13,14], наибольшие отражения наблюдаются от разъемных соединений, тогда как коэффициент отражения от сварных соединений или стыков оптоволокна с оптическими компонентами на один-два порядка ниже. Максимальный уровень отражения для разъемов типа FC/PC — $r = -40$ dB ($R = 10^{-4}$) [13–15]. С учетом непрерывного режима работы PM ($\tau_{\text{PM}} = 1/f_p$) выражение (1) приобретает вид

$$ISO > \frac{NR}{\mu f_p} = \frac{10^{20} \cdot 10^{-4}}{10^{-6} f_p} = \frac{10^{22}}{f_p}.$$

Для удобства расчетов будем оперировать уровнем изоляции, выраженным в dB:

$$iso > 10 \lg \left(\frac{10^{22}}{f_p} \right) = 220 - 10 \lg f_p. \qquad (2)$$

Таким образом, чем выше частота работы системы (частота посылки квантовых состояний и соответственно переключения PM), тем ниже требования к степени изоляции. Частота работы систем КРК варьируется от 10 MHz до 1 GHz, следовательно, минимальный требуемый уровень изоляции системы составляет

$$ISO_{\text{min}} = 220 - 10 \lg 10^7 = 150 \text{ dB}.$$

В большинстве случаев достигнуть подавления 150 dB на двойном проходе без дополнительных изолирующих элементов не представляется возможным, за исключением случаев использования фиксированного оптического ATT с коэффициентом ослабления более 70 dB. Поэтому оптические схемы включают в себя специальные защитные элементы (ISOTHA на рис. 2), требования к которым формируются с учетом параметров и характеристик уже установленных элементов схемы после модулятора.

Таким образом, чтобы рассчитать уровень изоляции, необходимо учесть потери на каждом элементе оптической схемы при прохождении сигнала от выхода в квантовый канал до PM и обратно. В приведенных далее расчетах мы пренебрегли вносимыми потерями меньше 3 dB. Такие потери вносят, например, разъёмные соединения (менее 0.3 dB), PM и т. п. [16,17]. Также известно, что коэффициенты пропускания PM и управляемого МЭМС ATT (аттенюатора, изготовленного на основе технологии микроэлектромеханических систем) ATT практически не зависят от длины волны [7].

Для оптической схемы на рис. 2 с учетом спектральных характеристик и сделанных допущений формула степени изоляции, выраженной в dB, принимает следующий вид:

$$ISO_{\text{tot}}(\lambda) = \big(2WDM(\lambda) + 2ATT + ISO_{\text{THA}}(\lambda)\big). \quad (3)$$

где $WDM(\lambda)$ — потери, вносимые спектральным WDM, $ATT(\lambda)$ — показатель ослабления излучения ATT, $ISO_{\text{THA}}(\lambda)$ — потери, вносимые частью оптической схемы, предназначенной для защиты от атаки Trojan-horse.

Используя приведенные выражения (1)–(3) для каждой конкретной оптической схемы и режима работы, необходимо сформировать требования к спектру пропускания защитного изолирующего блока. При наиболее жестких условиях, описанных выше, спектр пропускания изолирующего блока при двойном проходе (спектр изоляции) должен удовлетворять условию

$$ISO_{\text{THA}}(\lambda) > 220 - 10\lg f_p - 2WDM(\lambda) - 2ATT. \quad (4)$$

Измерительный стенд

Для измерения спектров пропускания различных волоконно-оптических элементов обычно используется мощный широкополосный источник излучения (суперконтинуума) и оптический анализатор спектра, либо источник суперконтинуума совместно с перестраиваемым спектральным фильтром и измерителями мощности [7]. В связи с отсутствием широкополосного источника излучения достаточной мощности нами был собран стенд (рис. 4), включающий набор перестраиваемых лазеров EXFO OSICS T100, переключатель и оптический анализатор спектра EXFO OSA20. Синхронизация и согласование работы перечисленных блоков осуществлялись с помощью специально разработанного программного обеспечения.

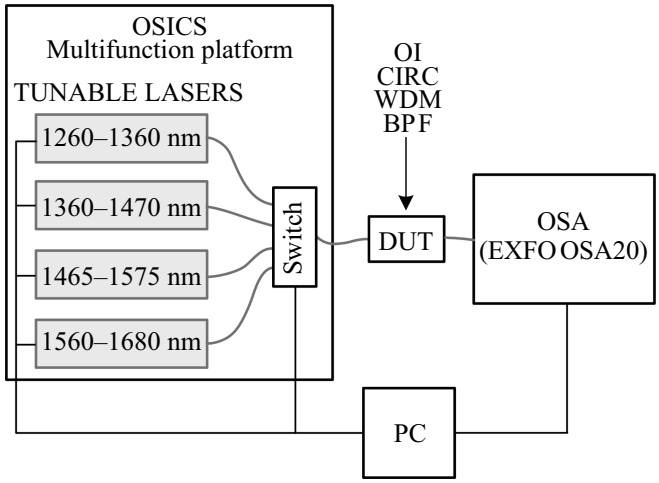

Рис. 4. Стенд для измерения спектральных характеристик пропускания оптических компонентов: Tunable lasers — перестраиваемые лазеры OSICS T100, Switch — оптический переключатель, DUT — исследуемый компонент, OSA — оптический анализатор спектра, PC — персональный компьютер.

Спектральные характеристики OI

OI является наиболее часто используемым элементом, применяемым для защиты от атаки Trojan-horse. Поляризационно-независимый OI почти без потерь пропускает сигнал в прямом рабочем направлении и значительно (около 40 dB) подавляет в обратном. Поэтому мы провели измерения спектральных характеристик OI от различных производителей, результаты которых представлены на рис. 5.

Из графиков видно, что степень пропускания сигнала OI в обратном направлении сильно зависит от длины волны излучения и имеет ярко выраженный минимум (более — 45 dB) в рабочей области (1550 nm). При этом вблизи длины волны 1260 nm степень изоляции составляет не более 15 dB, что создает благоприятные условия для реализации атаки. Также видно, что характеристики OI различных производителей сильно отличаются. Например, OI Thorlabs IO-H-1550APC имеет очень узкую полосу подавления от 1510 до 1580 nm, но за пределами этой полосы коэффициент пропускания достаточно высок, в то время как OI DK Photonics ISO-IU-15-A-L-90-10-FA вне рабочей полосы вносит большие потери (более 15 dB) и имеет широкую полосу подавления излучения от 1400 до 1640 nm.

Таким образом, для удовлетворения требования, описанного формулой (4), применения одного OI недостаточно. Необходим спектрально-селективный элемент, позволяющий выровнять суммарный коэффициент пропускания до требуемого уровня. Наиболее очевидным решением данной задачи является применение OI совместно с полосовыми спектральными фильтрами или их комбинациями.

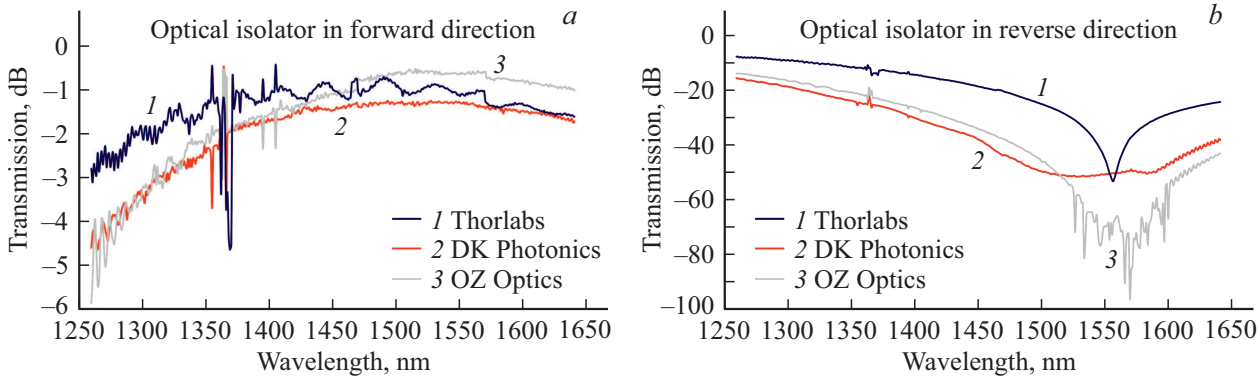

Рис. 5. Спектры пропускания волоконных OI в прямом (*a*) и обратном (*b*) направлениях: DK Photonics ISO-IU-15-A-L-90-10-FA, OZ Optics FOPI-21-11-1550-9/125-S-55-3U3U-1-1-55, Thorlabs: IO-H-1550APC.

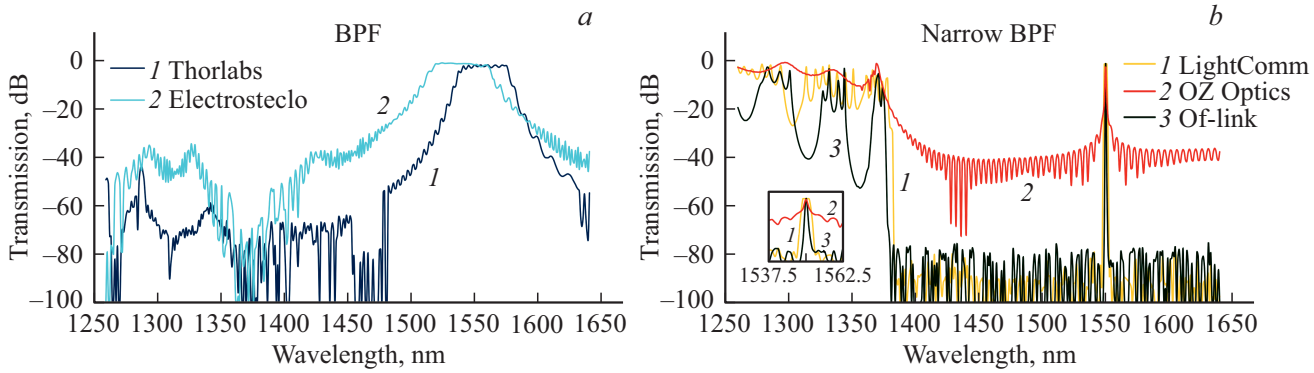

Рис. 6. Спектры пропускания полосовых фильтров: (*a*) широкополосных: Thorlabs FL051550-40, электростекло (выполнено на заказ), (*b*) узкополосных: LightComm BPF-1*2-T1550±1-0-007-FC/APC*2-5.5*34-1m; Of-Link BPF-1550-0.6-2.6-L-10-FA; OZ Optics FF-21-1550-9/125-S-60-3A3A-1-1-.

Спектральные характеристики полосовых фильтров

Спектральные фильтры по типу исполнения можно разделить на два класса: узкополосные интегральные (NBPF), являющиеся чисто интерференционными, и пространственные (BPF), представляющими из себя подложку из цветного стекла (ИК стекла) с нанесенными многослойными интерференционными покрытиями. В настоящей работе мы исследовали спектры пропускания спектральных фильтров обоих типов от разных производителей. Результаты показаны на рис. 6. По графикам видно, что узкополосные фильтры (Narrow BPF или NBPF) имеют окно прозрачности до 1370 nm, тогда как широкополосные блокируют излучение ниже 1450 nm. Таким образом, наиболее подходящими для работы совместно с OI в большинстве случаев являются спектральные фильтры на подложке из ИК стекла.

Зная спектры пропускания фильтров и OI, можно подобрать комбинацию с требуемыми характеристиками для различных применений. На рис. 7 показаны суммарные спектральные характеристики различных сочетаний фильтров и OI. Наиболее эффективным с точки зрения защиты от атаки Trojan-horse сочетанием элементов (из рассмотренных) является OI OZ Optics FOPI-21-11-1550-9/125-S-55-3U3U-1-1-55 и фильтр Thorlabs FL051550-40, суммарный уровень пропускания которых составляет около -80 dB во всем рассматриваемом спектральном диапазоне.

Спектральные характеристики оптических CIRC

Для защиты от активного зондирования также могут использоваться оптические CIRC, принцип работы которых аналогичен OI, не зависящим от поляризации. Мы исследовали спектры пропускания CIRC в обратном направлении от выхода 2 к выходу 1 и от выхода 3 к выходу 2. Измеренные зависимости (рис. 8, *a*) аналогичны спектрам OI в обратном ходе: CIRC также характерно слабое подавление излучения с длинами волн до 1350 nm.

Для усиления подавления обратного излучения целесообразно использовать обе траектории через CIRC: 3-2 и 2-1. Это легко реализуется путем подключения зеркала (M) к выходу 2 CIRC (рис. 8, *b*). Данная схема практически без потерь пропускает излучение в прямом направлении (от порта 1 к порту 3), а при

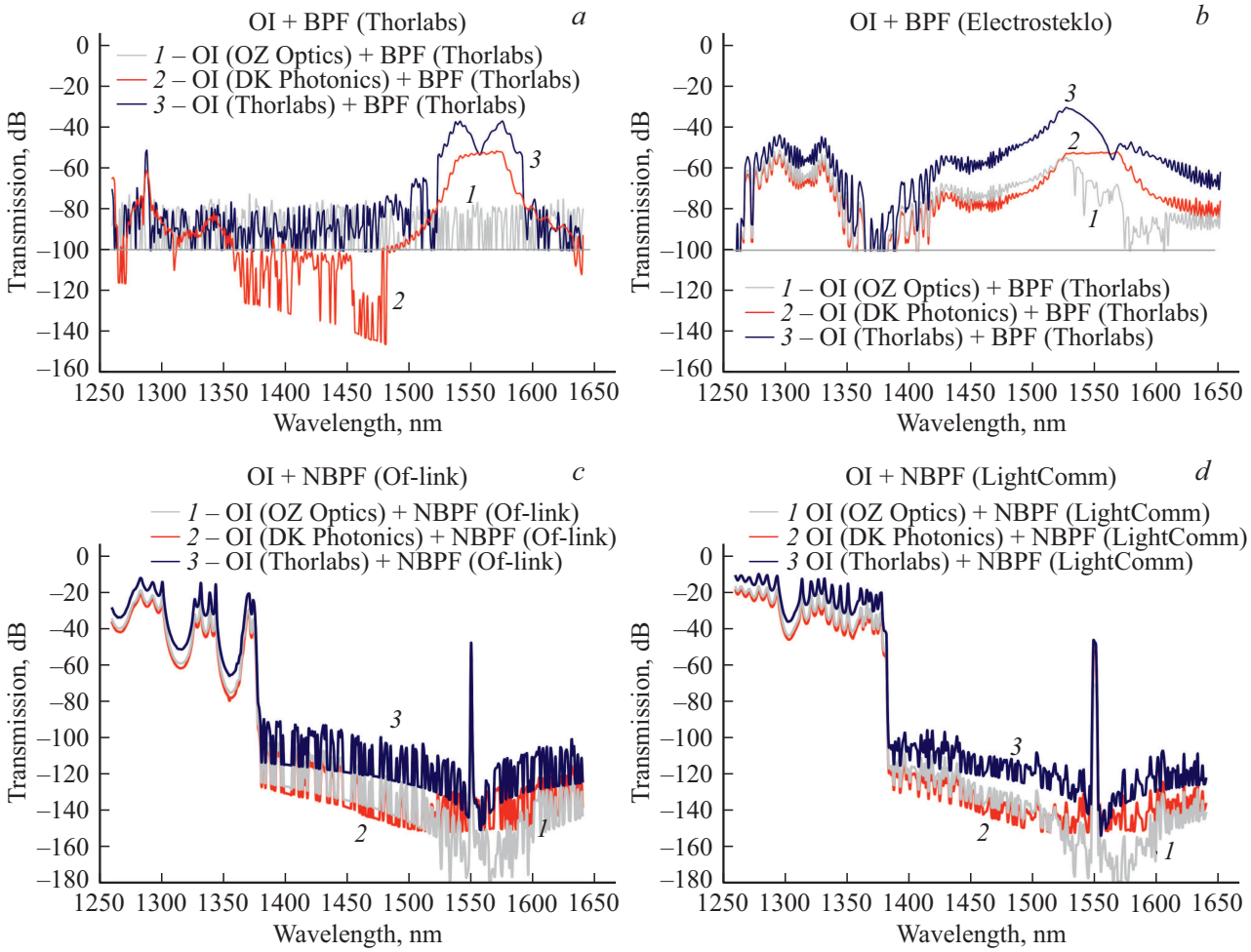

Рис. 7. Спектры пропускания различных комбинаций OI с широкополосными спектральными фильтрами производителей Thorlabs (*a*), электростекло (*b*) и с узкополосными Of-link (*c*), LightComm (*d*).

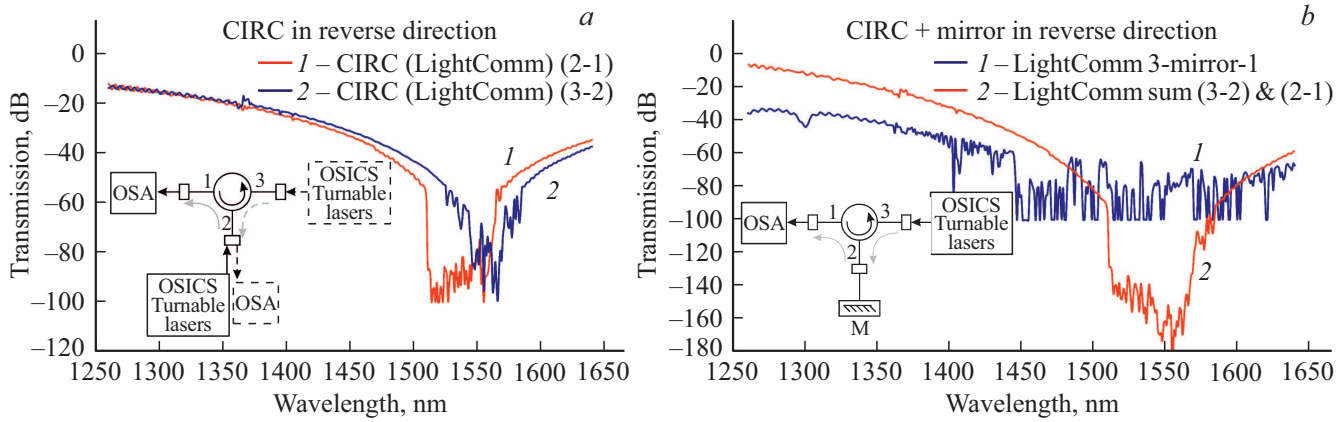

Рис. 8. (*a*) Схема и результаты измерения спектров пропускания оптического CIRC LightComm PICIR-1550-12-L в обратном направлении; (*b*) схема и результаты измерения спектральных характеристик комбинации из оптического CIRC (LightComm PICIR-1550-12-L) и зеркала (синий график) и суммарный спектр пропускания от порта 3 к порту 1 CIRC (красный график), рассчитанный на основе результатов измерений (рис. 8, *a*).

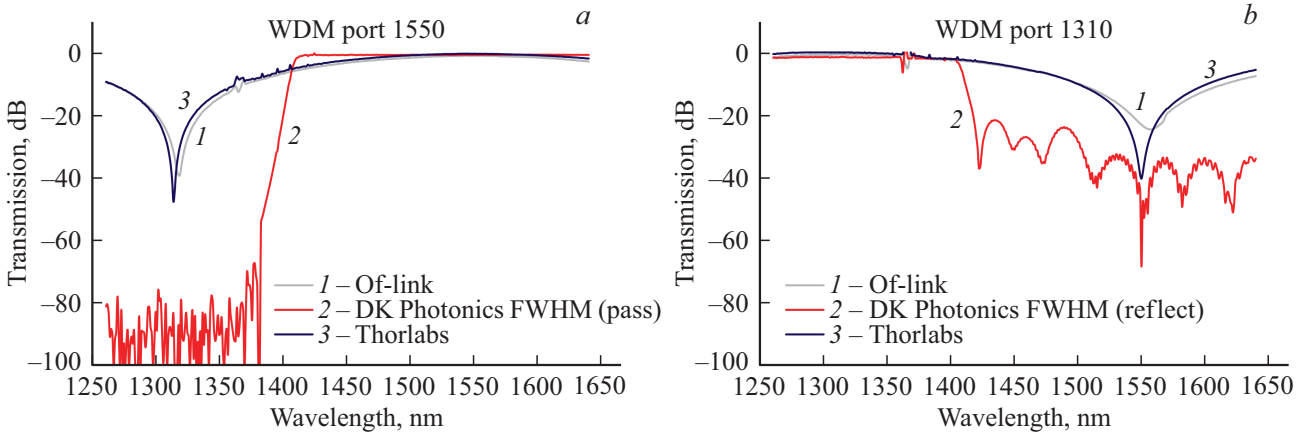

Рис. 9. Спектры пропускания WDM-компонентов от общего входа к выходу (*a*) 1550 nm (WDM port 1550) и (*b*) 1310 nm (WDM port 1310): Of-link WDM-1310/1550-SM-L-10-FA, DK Photonics FWDM-1X2-53-S-1-90 -10-FA, Thorlabs WD1350A.

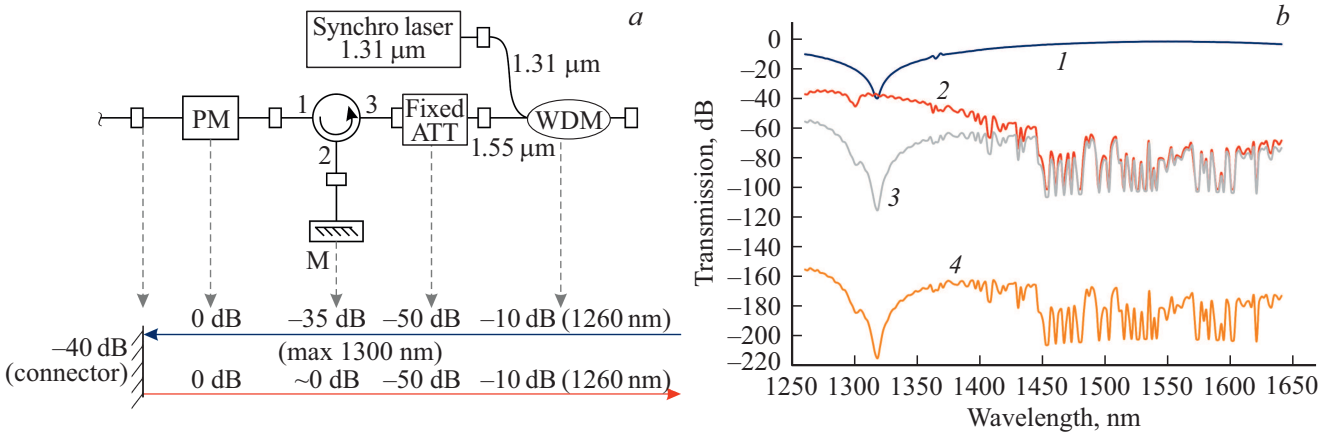

Рис. 10. Иллюстрация расчета степени изоляции PM (слева) и спектр пропускания схемы на проходе до PM и обратно (справа). Обозначения: PM — фазовый модулятор, M — зеркало, Fixed ATT — аттенюатор с фиксированным коэффициентом ослабления, WDM - спектральный мультиплексор 1310/1550.

обратном проходе подавляет его не менее чем на 30 dB. На рис. 8, *b* помимо измеренного спектра пропускания (синий график) представлена расчетная характеристика (красный график), представляющая собой сумму измеренных спектров пропускания 3-2 и 2-1 (рис. 8, *a*). Наличие „полочки“ ниже уровня 80 dB обусловлено достижением нижней границы динамического диапазона анализатора оптического спектра.

В рамках настоящей работы были исследованы CIRC производителей LightComm и DK Photonics. Результаты тестирования образцов DK Photonics PIOC-3-P-15-L-2-90-10-FA близки к измеренным спектрам для LightComm (представлены на рис. 8, *a* и рис. 8, *b*) с точностью до 1 dB, в связи с чем данные графики опущены. Таким образом, найдена и протестирована схема из двух оптических элементов (CIRC и зеркала), которая может использоваться для защиты от активного зондирования.

Несмотря на высокую изоляцию излучения в широком диапазоне длин волн вблизи 1550 nm, для CIRC, как и для OI, характерно „окно прозрачности“ на нерабочем участке — до 1350 nm. Очевидным решением данной проблемы является подключение отражательного спектрального фильтра (брэгговской решетки) к порту 2 CIRC, как сделано в работах [18,19].

Спектральные характеристики WDM-компонентов

Зачастую в системах КРК для объединения квантового канала и канала синхронизации используются WDM. Так как WDM-компоненты в схемах Алисы или Боба расположены непосредственно у выхода в волоконно-оптическую линию связи, то они также вносят свой вклад в защиту от зондирования мощными импульсами.

Очевидно, что спектр пропускания WDM-компонентов не является равномерным. При этом большинство производителей в спецификации на WDM не приводят спектральные характеристики, ограничиваясь для каждого порта лишь степенью изоляции (подавления)

излучения с длиной волны, соответствующей противоположному порту.

Широко используемое сочетание длин волн для импульсов синхронизации и информационных импульсов — 1310 nm и 1550 nm соответственно. Поэтому на рис. 9 приведены измеренные спектры пропускания компонента WDM 1310/1550. Стоит отметить, что спектр пропускания WDM инвариантен относительно направления распространения (мультиплексирование/демультиплексирование), поэтому показаны характеристики только для случая демультиплексирования.

Среди исследованных образцов наибольший интерес представляет Filter WDM производителя DK Photonics, блокирующий излучение ниже 1400 nm (для порта 1550 nm). Применение данного WDM совместно со стандартными OI позволяет эффективно блокировать зондирующие импульсы в широком спектральном диапазоне.

Пример расчета степени изоляции

Результаты исследований, представленные в данной статье, могут использоваться для оценки эффективности применения тех или иных мер защиты от атак активного зондирования. В качестве примера приведем расчет степени изоляции, обеспечиваемой схемой, показанной на рис. 10, в состав которой входят:

— PM;

— комбинация из CIRC с зеркалом, описанная выше;

— ATT для ослабления импульсов на 50 dB (для ослабления излучения стандартного телекоммуникационного лазера мощностью около 10 mW до квазиоднофотонного уровня со средним числом фотонов $\mu < 1$ требуется более 80 dB);

— классический WDM 1310/1550.

Под оптической схемой на рис. 10 показаны коэффициенты пропускания в прямом и обратном направлениях каждого компонента для диапазона длин волн, в котором зондирование наиболее эффективно для нарушителя (1200–1400 nm). Степень изоляции, т. е. величина, обратная суммарному пропусканию в прямом и обратном направлениях, для представленной системы составляет более 150 dB. Это также видно по итоговому графику спектра пропускания системы („CIRC + 2 WDM + 2 fixedATT“), который является суммой измеренных спектров WDM, CIRC с зеркалом и ATT.

Стоит отметить, что несмотря на то, что в работе рассматривается схема отправителя (Алисы), на приемной стороне (Бобе) также требуется защита от подобных атак. Так как в оптической схеме Боба отсутствует ATT, то для достижения такого же уровня изоляции (150 dB) потребуется дополнительный каскад изолирующих элементов. Например, для достижения уровня ослабления сигнала 100 dB в обратном направлении, что аналогично действию ATT в схеме Алисы, для рассматриваемого спектрального диапазона подойдёт комбинация из двух OI OZ Optics FOPI-21-11-1550-9/125-S-55-3U3U-1-1-55 и полосового фильтра Thorlabs FL051550-40.

Выводы

В настоящей работе представлены измеренные спектральные характеристики пропускания различных волоконно-оптических компонентов. Приведенные графики могут использоваться при выборе элементной базы для систем квантового распределения ключей, в частности при выборе мер защиты от атак на техническую реализацию. Также показан принцип расчета требуемого уровня изоляции системы КРК, обеспечивающего эффективную защиту от атаки Trojan-horse исходя из максимальных технических возможностей нарушителя: максимальной мощности зондирующих импульсов ($N = 10^{20}$ ph/s/50 μm^2) и минимального среднего числа фотонов ($\mu = 10^{-6}$), регистрируемого Евой. При наиболее жестких условиях для сторон КРК и наиболее благоприятных для нарушителя степень изоляции должна превышать 150 dB во всем спектральном диапазоне, разрешенном для распространения в ОВ. Приведенный пример подбора компонентов (CIRC, зеркало, ATT, WDM) показывает достижимость требуемого уровня в диапазоне от 1260 до 1650 nm.

Финансирование работы

Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований в рамках научного проекта № 19-37-80007.

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Список литературы

[1] *Балыгин К.А., Зайцев В.И., Климов А.Н., Климов А.И., Кулик С.П., Молотков С.Н.* // Письма в ЖЭТФ. 2017. Т. 105. В. 9. С. 570–576.

[2] *Молотков С.Н.* // ЖЭТФ. 2012. Т. 141. В. 5. С. 812–831.

[3] *Nielsen M.A., Chuang I.L.* Quantum Computation and Quantum Information. NY, USA: Cambridge University Press, 2000. P. 704; *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. М: Мир, 2006.

[4] *Jain N., Stiller B., Khan I., Elser D., Marquardt Ch., Leuchs G.* // Contemporary Physics. 2016. V. 57. N 3. C. 366–387.

[5] *Shi Y., Lim J., Poh H., Tan P., Tan P., Ling A., Kurtsiefer C.* // Opt. Express. 2017. V. 25. P. 30388–30394.

[6] *Jain N., Stiller B., Khan I., Makarov V.V., Marquardt Ch., Leuchs G.* // IEEE J. Selected Topics in Quantum Electronics. 2014. V. 21. N 3. C. 168–177.

[7] Deliverable D5-1. Best Practice Guide on Characterization of Counter-measures to Side-channel and Trojan-horse Attacks [Электронный ресурс] Режим доступа: http://projects.npl.co.uk/MIQC/documents/MIQC_BPG_v1.pdf

[8] *Божевольный С.И., Бурицкий К.С., Золотов Е.М., Похоров А.М., Черных В.А.* // Квант. электрон. 1981. Т. 8. № 11. С. 2486–2492.
[9] *Чапало И.Е.* // СПб гос. электротехн. ун-т (ЛЭТИ). 2017.
[10] *Paschotta R.* Tutorial on „Passive Fiber Optics". Part 3: Single-mode Fibers/RP Photonics Encyclopedia. [Электронный ресурс] Режим доступа: https://www.rp-photonics.com/passive_fiber_optics3.htm
[11] *Lucamarini M., Choi I., Ward M.B., Dynes J.F., Yuan Z.L., Shields A.J.* // Phys. Rev. X. 2015. V. 5. N. 3. C. 031030.
[12] *Du D., Liu X., Korn G., Squier J., Mourou G.* // Appl. Phys. Lett. 1994. V. 64. N 23. C. 3071–3073.
[13] *Huang A., Li R., Egorov V., Tchouragoulov S., Kumar K., Makarov V.* // Phys. Rev. Appl. 2020. V. 13. N 3. P. 034017.
[14] *Gisin N., Fasel S., Kraus B., Zbinden H., Ribordy G.* // Phys. Rev. A. 2006. V. 73. P. 022320.
[15] *Листвин В.Н., Трещиков В.Н.* // Фотон-экспресс. 2011. № 3(91). С. 38–39.
[16] EOSPACE. Phase Modulator. [Электронный ресурс] Режим доступа: https://www.eospace.com/phase-tmodulator/
[17] iXblue Photonics. Phase Modulator. MPX and MPZ series [Электронный ресурс] Режим доступа: https://photonics.ixblue.com/sites/default/files/2019-10/MPX%2BMPZ%20SERIES_1.pdf
[18] *Bloch M., Mc Laughlin S.W., Merolla J.-M., Patois F.* // Opt. Lett. 2007. V. 32. N 3. C. 301–303.
[19] *Gleim A.V., Egorov V.I., Nazarov Yu.V., Smirnov S.V., Chistyakov V.V., Bannik O.I., Anisimov A.A., Kynev S.M., Ivanova A.E., Collins R.J., Kozlov S.A., Buller G.S.* // Opt. Express. 2016. V. 24. N 3. C. 2619–2633.