ИЗВЕСТИЯ РАН. СЕРИЯ ФИЗИЧЕСКАЯ, 2022, том 86, № 10, с. 1406–1410

УДК 535.92

АНАЛИЗ СПЕКТРОВ ПРОПУСКАНИЯ ВОЛОКОННО-ОПТИЧЕСКИХ ЭЛЕМЕНТОВ В БЛИЖНЕМ ИК-ДИАПАЗОНЕ ДЛЯ УВЕЛИЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА

© 2022 г. Б. А. Наседкин[1, *], И. М. Филипов[1], А. О. Исмагилов[1], В. В. Чистяков[1], Ф. Д. Киселев[1], А. Н. Цыпкин[1], В. И. Егоров[1]

[1]*Федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский университет ИТМО", Санкт-Петербург, Россия*

******E-mail: banasedkin@itmo.ru*

Поступила в редакцию 01.06.2022 г.
После доработки 15.06.2022 г.
Принята к публикации 22.06.2022 г.

Измерены спектры пропускания волоконно-оптических изолятора и WDM-компонент на основе тонких пленок в диапазоне 700–850 нм. Продемонстрировано, что исследуемые элементы имеют окна пропускания в рассмотренном диапазоне, что может негативно отразиться на безопасности систем квантового распределения ключа.

DOI: 10.31857/S0367676522100143

ВВЕДЕНИЕ

Криптография является основой безопасности современной системы хранения и передачи информации, при этом широко используемые асимметричные алгоритмы шифрования находятся в зоне риска из-за возможности дешифрования при достаточном уровне развития квантовых вычислений, что обусловливает повышенный интерес к ним со стороны не только научного сообщества, но и частных компаний, и отдельных государств, заинтересованных в вопросах информационной безопасности. В данном контексте возникает необходимость не только в модификации существующих криптографических систем, но и в учете возможности дешифрования классов информации, предполагающих длительные сроки хранения. На данный момент можно выделить два основных подхода к решению поставленной проблемы: усовершенствование информационных систем с применением новых физических принципов при их построении, в частности, внедрение квантового распределения ключа (КРК) в аппаратно-программные комплексы средств криптографической защиты информации, и усовершенствование и разработка новых криптографических алгоритмов, называемых постквантовыми, а также объединение этих подходов [1].

КРК, в основе которого лежат законы квантовой механики, как уже было сказано выше, выступает в качестве возможной контрмеры от угрозы, исходящей от квантовых вычислений. Первый протокол КРК BB84 был предложен в 1984 году Беннетом и Брассардом [2], а в 1992 году был проведен первый эксперимент с демонстрацией КРК в рамках лаборатории [3]. К 2005 году развитие технологии позволило компании ID Quantique произвести первые коммерческие системы КРК. Развитие как в направлении создания [4, 5] и усовершенствования протоколов [6], так и улучшения технических реализаций систем КРК, позволило сформироваться КРК в качестве коммерческой технологии. Развитие аппаратных реализаций происходит не только за счет усовершенствования компонентной базы, используемой в волоконно-оптических линиях связи, но и за счет выявления и устранения недостатков, обусловленных наличием уязвимостей отдельных элементов, функциональных узлов или системы в целом из-за их физических и конструкторских несовершенств, которыми нарушитель может воспользоваться для осуществления атаки [7]. Одной из самых уязвимых частей систем КРК на дискретных переменных является детектор одиночных фотонов, доступ к которому является целью нарушителя в ряде атак [8, 9]. Данные атаки используются нарушителем, чтобы получить контроль над измерительным оборудованием получателя с последующим навязыванием ключевой информации. При реализации подобных атак, в общем случае, на детектор через волоконно-оптическую схему направляется интенсивное излучение, которое переводит детектор из режи-

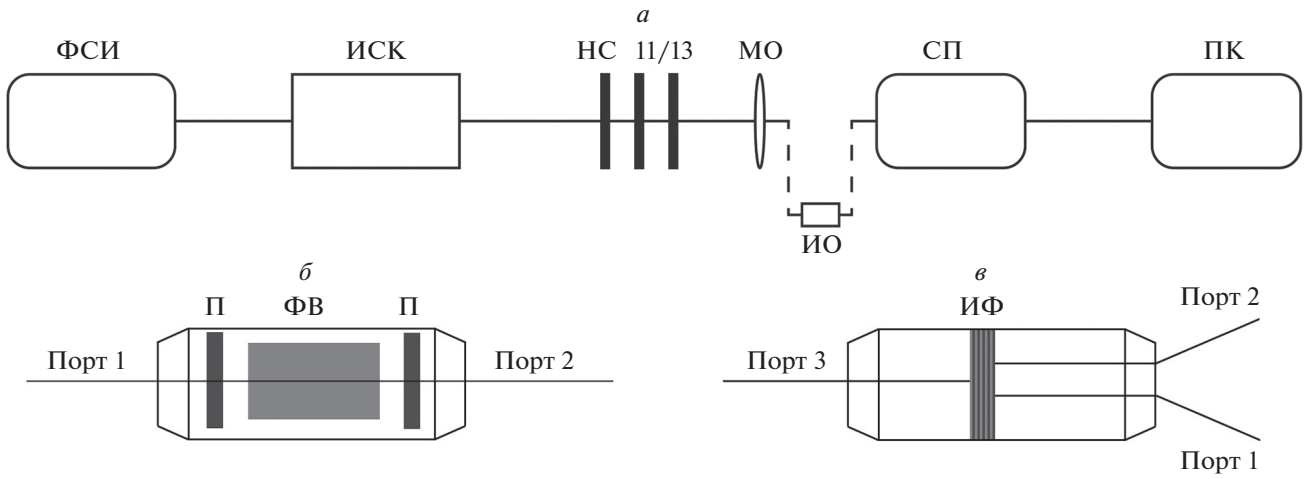

Рис. 1. Схематическое изображение оптической схемы экспериментальной установки (*а*), олоконного изолятора (П – поляризатор, ФВ – Фарадеевский вращатель) (*б*), тонкопленочного интерференционного фильтра (ИФ – тонкопленочный интерференционный фильтр) (*в*).

ма счета фотонов в линейный фотодиодный режим. В таком режиме нарушитель может контролировать срабатывания детектора. Важной особенностью данной атаки является ограничение возможности ее реализации диапазоном чувствительности используемых для регистрации передаваемых состояний детекторов одиночных фотонов, который обычно составляет 700–1700 нм для InGaAs-фотодиодов. Также возможно осуществление атаки Троянский конь (от англ. Trojan-horse), при которой нарушитель зондирует оптические компоненты в модулях КРК для получения информации об использованных состояниях в процессе генерации ключей [10]. Зондирующее излучение при осуществлении атаки отражается или претерпевает обратное рассеивание на электрооптических модуляторах света в момент их работы, при этом нарушитель может быть заинтересован в сканировании как фазового модулятора, так и амплитудного в случае применения протокола с обманными состояниями (от англ. Decoy states) [11]. Анализ возможности реализации перечисленных атак был проведен в ряде работ для диапазона длин волн 1000–1800 нм [12–15]. Также была продемонстрирована возможность реализации атаки Троянский конь для фиксированной длины волны 1924 нм [16].

Демонстрация возможности реализации атак вне телекоммуникационного диапазона (1250–1650 нм) ставит вопрос о необходимости исследования пропускания используемых в системах КРК волоконно-оптических элементов. В данной работе будут рассмотрены спектры пропускания изолятора и WDM-компонента (от англ. wavelength division multiplexing на основе тонкопленочного фильтра (от англ. thin-film filter), используемых в системах КРК для противодействия атакам в диапазоне 700–850 нм. Рассматриваемый диапазон интересен для измерений, поскольку в него может попадать один из пиков отражения брэгговских решеток второго типа [17] и, одновременно с этим, фотодиоды, используемые в системах КРК чувствительны к излучению в данном диапазоне.

ЭКСПЕРИМЕНТАЛЬНАЯ УСТАНОВКА И МЕТОДЫ

Для измерения спектров пропускания исследуемых волоконно-оптических элементов была собрана экспериментальная установка представленная на рис. 1*а*.

В качестве источника широкополосного оптического излучения использовалась кювета с дистиллированной водой 20 × 50 мм (ИСК), генерация в которой индуцировалась за счет фазовой самомодуляции импульсов излучения Ti:Sa фемтосекундной системы на основе регенеративного усилителя Regulus35f1k (Avesta Project) с центральной длиной волны 790 нм, длительностью импульсов 35 фс, частотой повторения 1 кГц и средней мощностью излучения 330 мВт (ФСИ) [18]. В результате генерировалось излучение в спектральном диапазоне 700–850 нм. Полученное излучение направлялось на нейтральные светофильтры НС10, НС11 и НС13 (НС11/НС13) с известным пропусканием. Далее излучение при помощи микрообъектива вводилось в одномодовое оптическое волокно. Спектры излучения, прошедшего оптическое волокно, измерялись при помощи спектрометра USB4000-UB-VIS-ES (Ocean Optics), спектральный диапазон измерений которого составлял 190–1100 нм, и имеющего разрешение 1.5 нм (СП). После прохождения од-

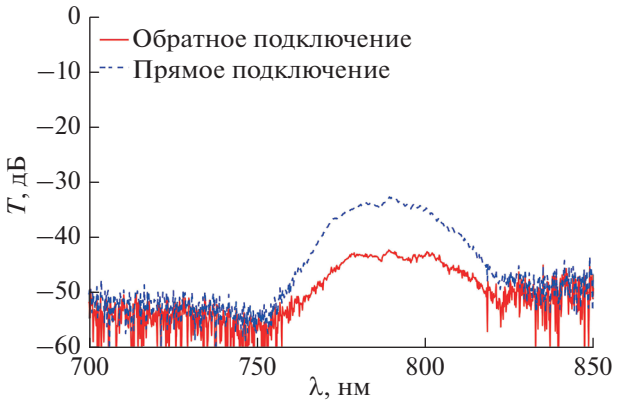

Рис. 2. Пропускание волоконно-оптического изолятора при прямом и обратном подключении.

номодового оптического волокна в отсутствии исследуемых волоконно-оптических элементов, регистрировался опорный спектр излучения, относительно которого рассчитывался коэффициент пропускания.

Далее в схему помещались исследуемые волоконно-оптические элементы (ИО). В случае отсутствия сигнала на приемнике из схемы вынимались нейтральные светофильтры до тех пор, пока сигнал не был обнаружен, либо не заканчивались фильтры. Это позволяло расширить динамический диапазон измерений. В качестве рассматриваемых волоконно-оптических элементов были использованы коммерчески доступные изолятор и тонкопленочный фильтр.

Пропускание волоконно-оптических элементов переводилось в децибелы и рассчитывалось по формуле:

$$T_{\text{dB}} = 10\lg\left(\frac{I_m\prod_i(T_i)}{I_{sc}}\right), \qquad (1)$$

где I_m – измеренный спектр пропускания исследуемого элемента; T_i – значение пропускания i-того нейтрального светофильтра для заданной длины волны (в случае, если фильтр не вынимался: $T_i = 1$); I_{sc} – измеренный спектр широкополосного излучения.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

Спектры пропускания изолятора

Волоконно-оптические изоляторы представляют из себя элементы, которые имеют высокий коэффициент пропускания при прямом подключении и низкий при обратном подключении. Это свойство изоляторов используется в системах КРК для защиты от атак. Основным требованием, предъявляемым к изоляторам, является высокая степень изоляции при обратном подключении. Устройство простейшего изолятора представлено на рис. 1*б*. Типичную зависимость пропускания изолятора в прямом и обратном направлениях можно найти в работах [14, 19].

На рис. 2 представлено пропускание волоконно-оптического изолятора, используемого для длин волн в диапазоне 700–850 нм. Значения пропускания рассчитывались согласно (1). Видно, что при прямом подключении пропускание составляет величину порядка минус 30 дБ для диапазона 780–800 нм. При обратном подключении, пропускание составляет величину, порядка –40 дБ.

Зная пропускание фильтра, можно оценить возможность реализации атаки с ослеплением детектора. Известно, что максимальное значение мощности оптического излучения, которое можно завести в оптическое волокно, не повредив его, составляет величину порядка 9 Вт для широкого диапазона длин волн. Для ослепления детектора одиночных фотонов, представленного в работе [20] требовалась мощность порядка 100 мкВт. Таким образом, можно оценить, что для уменьшения риска возможности реализации атаки необходима изоляция не менее, чем минус 50 дБ. В таком случае, можно заключить, что использование одного изолятора недостаточно, для защиты системы в целом. При этом пара идентичных изоляторов может позволить достичь достаточного уровня ослабления излучения, проходящего в обратном направлении.

Для оценки возможности реализации атаки Троянский конь, необходимо учесть несколько дополнительных факторов, а именно, пропускание изолятора как в прямом, так и обратном направлении, а также, потери при отражении излучения от дальней грани электрооптического модулятора, что ослабит отраженный сканирующий импульс не менее чем на 40 дБ. В таком случае суммарный коэффициент пропускания системы составит величину минус 110 дБ. Однако, в зависимости от используемой системы, может понадобиться коэффициент пропускания не более – 200 дБ. Соответственно, необходимо использование не менее двух изоляторов.

Спектр пропускания тонкопленочного фильтра

В системах КРК WDM-компоненты на основе тонкопленочных фильтров используются для выделения длины волны, на которой ведется распределение симметричной битовой последовательности. Наиболее распространены фильтры, соответствующие используемым для спектрального уплотнения по длинам волн. В волоконно-оптических исполнениях у подобных фильтров обычно присутствует три разъема (рис. 1*в*). В пер-

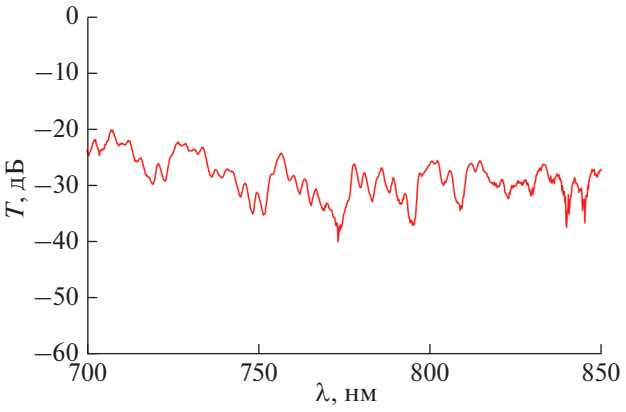

Рис. 3. Пропускание волоконно-оптического WDM-компонента на основе тонкопленочного фильтра при прямом подключении.

вый подается подвергаемое фильтрации излучение, во второй – отражается выделяемая в процессе фильтрации длина волны, и в третий проходит оставшееся излучение. Соответственно идеальный фильтр должен отражать только спектральный диапазон, для отражения которого он изготовлен. Однако, в зависимости от подхода к изготовлению фильтра, у него могут присутствовать дополнительные пики отражения [21].

На рис. 3 представлен измеренный спектр волоконно-оптического интерференционного фильтра на основе тонких пленок. При этом рассмотрено прямое подключение первого разъема относительно второго. Видно, что в отличии от спектра пропускания изолятора, фильтр не имеет ярко выраженного диапазона пропускания. Тем не менее, можно выделить отдельные пики, для которых пропускание выше. Изоляция для данных пиков лежит в диапазоне от –20 до –25 дБ.

Исходя из соображений, представленных ранее, и, пренебрегая потерями на остальных элементах и соединениях, можно заключить, что атака на детектор одиночных фотонов возможна для рассмотренного фильтра, поскольку его ослабления недостаточно для рассмотренных длин волн. Необходимый уровень ослабления может быть достигнут комбинацией из трех фильтров. Для противодействия реализации атаки Троянский конь потребуется наличие не менее четырех фильтров, что представляется нецелесообразным.

ЗАКЛЮЧЕНИЕ

Изучены спектры пропускания в прямом и обратном направлении волоконно-оптического изолятора и спектр пропускания для тонкопленочного интерференционного фильтра. Рассмотренные элементы имеют пропускание в диапазоне 760–820 нм.

Продемонстрировано, что при определенных условиях, использование одного фильтра или изолятора недостаточно для защиты от атак ослепление детектора и Троянский конь. При этом важно учитывать, что увеличение числа защитных элементов может привести к ухудшению характеристик системы КРК. Одной из возможных траекторий, позволяющей избежать возможности реализации атак без увеличения числа волоконно-оптических элементов в системе КРК, может являться проверка спектральных характеристик элементов до их использования в системе с целью подбора минимального числа элементов с максимально необходимыми коэффициентами пропускания на длинах волн, отличных от длины волны передачи информации.

Работа выполнена при финансовой поддержке Минобнауки РФ в рамках темы государственного задания (паспорт № 2019-0903).

СПИСОК ЛИТЕРАТУРЫ

1. *Wang L.J., Zhang K.Y., Wang J.Y. et al.* // Quantum Inform. 2021. V. 7. Art. No. 1.
2. *Bennett C.H., Brassard G.* // Proc. Int. Conf. Comp. Syst. Signal Process. (Bangalore, 1984) P. 175.
3. *Bennett C.H., Bessette F., Brassard G. et al.* // J. Cryptol. 1992. V. 5. No. 1. P. 3.
4. *Ralph T.C.* // Phys. Rev. A. 2000. V. 62. No. 6. Art. No. 062306.
5. *Merolla J.M., Mazurenko Y., Goedgebuer J.P. et al.* // Opt. Lett. 1999. V. 24. No. 2. P. 104.
6. *Lo H.K., Ma X., Chen K.* // Phys. Rev. Lett. 2005. V. 94. No. 23. Art. No. 230504.
7. *Xu F., Ma X., Zhang Q. et al.* // Rev. Modern Phys. 2020. V. 92. No. 2. P. 1.
8. *Lydersen L., Wiechers C., Wittmann C. et al.* // Nature Photon. 2010. V. 4. No. 10. P. 686.
9. *Wu Z., Huang A., Chen H. et al.* // Opt. Express. 2020. V. 28. No. 17. Art. No. 25574.
10. *Vakhitov A., Makarov V., Hjelme D.R.* // J. Modern Opt. 2001. V. 48. No. 13. P. 2023.
11. *Tamaki K., Curty M., Lucamarini M.* // New J. Phys. 2016. V. 18. No. 6. Art. No. 065008.
12. *Lucamarini M., Choi I., Ward M. B. et al.* // Phys. Rev. X. 2015. V. 5. No. 3. P. 1.
13. *Jain N., Stiller B., Khan I. et al.* // IEEE J. Sel. Top. Quantum Electron. 2015. V. 21. No. 3. P. 168.
14. *Борисова А.В., Гармаев Б.Д., Бобров И.Б. и др.* // Опт. и спектроск. 2020. Т. 128. № 11. С. 1758.
15. *Sushchev I.S., Guzairova D.M., Klimov A.N. et al.* // Proc. SPIE. 2021. V. 11868. P. 15.
16. *Sajeed S., Minshull C., Jain N., Makarov V.* // Sci. Rep. 2017. V. 7. No. 1. P. 1.
17. *Malo B., Johnson D.C., Bilodeau F. et al.* // Opt. Lett. 1993. V. 18. No. 15. P. 1277.

18. *Кандидов В.П., Голубцов И.С., Косарева О.Г.* // Квант. электрон. 2004. Т. 34. № 4. С. 348.
19. *Berent M., Rangelov A.A., Vitanov N.V.* // JOSA A. 2013. V. 30. No. 1. P. 149.
20. *Gu P., Zheng Z.* // J. Zhejiang Univ. Sci. A. 2006. V. 7. No. 6. P. 1037.
21. *Chistiakov V., Huang A., Egorov V., Makarov V.* // Opt. Express. 2019. V. 27. No. 22. Art. No. 32253.

Transmission spectra analysis of fiber-optic elements in the near IR range to increase the security of quantum key distribution systems

B. A. Nasedkin[a], *, I. M. Filipov[a], A. O. Ismagilov[a], V. V. Chistiakov[a], F. D. Kiselev[a], A. N. Tsypkin[a], V. I. Egorov[a]

[a]ITMO University, Saint-Petersburg, Russia
**e-mail: banasedkin@itmo.ru*

The transmission spectra of a fiber-optic insulator and a wavelength division multiplexing thin-film filter in the 700–860 nm range are measured. It was shown that investigated elements transmit light in these range which could negatively affected at quantum key distribution systems security.