

АППАРАТНО-ПРОГРАММНЫЙ ДЕМОНСТРАТОР СИСТЕМЫ РАСПРЕДЕЛЕНИЯ КВАНТОВЫХ КЛЮЧЕЙ ДЛЯ ЮНОШЕСКИХ ЧЕМПИОНАТОВ WORLDSKILLS

И.М. Габдулхаков, Е.А. Громов

(научные руководители: О.Г. Морозов, профессор КНИТУ-КАИ;

И.И. Нуреев, профессор КНИТУ-КАИ)

Казанский национальный исследовательский технический университет

им. А.Н. Туполева-КАИ

Российская Федерация, 420111, г. Казань, ул. К. Маркса, 10

Аннотация. В статье рассмотрен аппаратно-программный демонстратор для исследования характеристик системы квантового распределения ключей с частотным кодированием на основе тандемного амплитудно-фазового модуляционного преобразования оптической несущей и подготовки специалистов по их эксплуатации. Демонстратор является хорошим кандидатом для импортозамещения при использовании в ходе соревнований юношеских чемпионатов WorldSkills. Кроме того, предложенный демонстратор, встраиваемый в настольный компьютер, может выполнять функции устройств доступа, которые можно подключить к терминалу, совмещенному с узлом квантовой сети, для пополнения хранилища секретных ключей, которое затем можно использовать для шифрования повседневной деятельности на обычных платформах, таких как Интернет.

Ключевые слова: система квантового распределения ключей с частотным кодированием, тандемное амплитудно-фазовое модуляционное преобразование оптической несущей, аппаратно-программный демонстратор, импортозамещение, научно-исследовательская и образовательные платформы, юношеский чемпионат WorldSkills, устройство доступа в Интернет.

Введение

Требования массового потребительского и образовательного рынка накладывают большие ограничения на стоимость аппаратно-программных демонстраторов (АПД) при относительно низких требованиях к характеристикам процесса квантового распределения ключей (КРК). Это означает, что эти устройства не обязательно должны обладать передовыми характеристиками и, как таковые, могут обеспечить резкое снижение размера, веса и мощности (РВМ) по сравнению с другими системами КРК.

Концепция предлагаемого АПД также способствует сокращению РВМ потребительских устройств. В нашем случае имеет смысл поместить приемно-передающее оборудование Боба и Алисы в компьютер из-за относительной сложности обнаружения сигналов уровня одиночных фотонов по сравнению с их созданием. Большая часть постобработки данных также может выполняться на компьютере, поэтому требования к вычислительному оборудованию АПД минимальны.

Цель разработки АПД состоит в том, чтобы создать минимизированное, но функционально полное устройство, которое можно было бы сделать достаточно дешевым для широкого распространения в научно-образовательных организациях, на юношеских чемпионатах WorldSkills, а в дальнейшем для частных абонентов, для чего необходимо применение

достаточно простых и эффективных способов кодирования состояния фотона, а также элементной базы, удовлетворяющей условиям минимизации активных элементов и импортозамещения.

1. Структурная схема универсальной системы КРК для построения АПД с ремодуляцией в научно-образовательных целях

В основе работы универсальной системы (УС) КРК с частотным кодированием, предложенной для построения АПД, лежит тандемное амплитудно-фазовое (ТАФМ) модуляционное преобразование несущей фотона на основе метода Ильина-Морозова и его одно- и двухмодуляторных реализаций [1-8]. Для моделирования схемы и проведения проектных оценок были использованы принципы построения однопортового модуляционного радиофотонного звена последовательного типа и фотонного моделирования электрооптических модуляторов [9-10].

Выберем два базиса для частотного кодирования состояния фотонов при ТАФМ, поясним порядок их получения и покажем их реализацию на рис. 1.

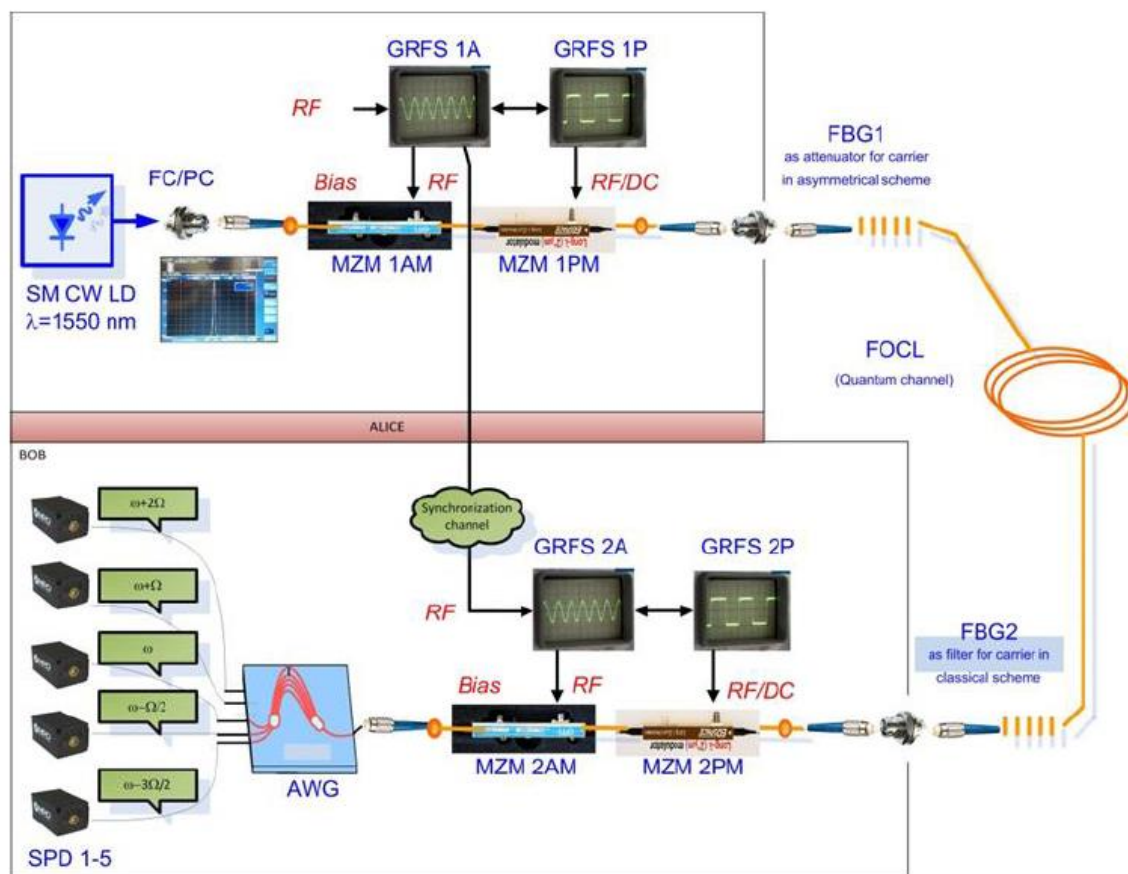


Рис. 1. Структурная схема АПД с ремодуляцией для практической реализации

Состояние $|+;1\rangle$ представляет собой немодулированный фотон, передаваемый от CW LD лазера, через открытые модуляторы MZM Алисы – амплитудный 1AM и фазовый 2AM; состояние $|-;1\rangle$ определяется при амплитудной модуляции на стороне Алисы напряжением с частотой Ω в «нулевой» рабочей точке и при отсутствии фазовой коммутации; состояние $|+;2\rangle$ кодируется при работе 1AM на линейном участке напряжением с частотой Ω и коэф-

фициентом амплитудной модуляции $m=0,55$ при дальнейшей фазовой коммутацией $0/\pi$ с частотой $\Omega/2$ в 1PM; состояние $|-,2\rangle$ описывается боковыми составляющими, полученными при параметрах фазовой коммутации с частотой $3\Omega/2$, либо с частотой $\Omega/2$, но при работе 1AM в максимальной точке модуляционной характеристики с аргументом функции Бесселя, равном 2,405.

Управление параметрами амплитудной модуляции выполняет генератор специальных функций GRFS 1A, фазовой коммутации – GRFS 1P с соответствующим изменением функций.

Как видно из пояснений к рис. 1 все четыре состояния фотонов могут быть пассивно выделены с помощью системы фильтров (показаны на стороне Боба), настроенных соответственно на частоты $\omega_0 \rightarrow |+,1\rangle$, $\omega_0 \pm \Omega/2 \rightarrow |+,2\rangle$, $\omega_0 \pm \Omega \rightarrow |-,1\rangle$, $\omega_0 \pm 3\Omega/2 \rightarrow |-,2\rangle$. Таким образом может быть построена и асимметричная система без ремодуляции ТАФМ-ВБР, где ВБР – система фильтров, подключенных к ОФП (SPD) на базе волоконных брэгговских структур. Полученные на экспериментальной установке сигналы для состояний $|+,1\rangle$, $|+,2\rangle$, $|-,2\rangle$ показаны на рис. 2, а-в.

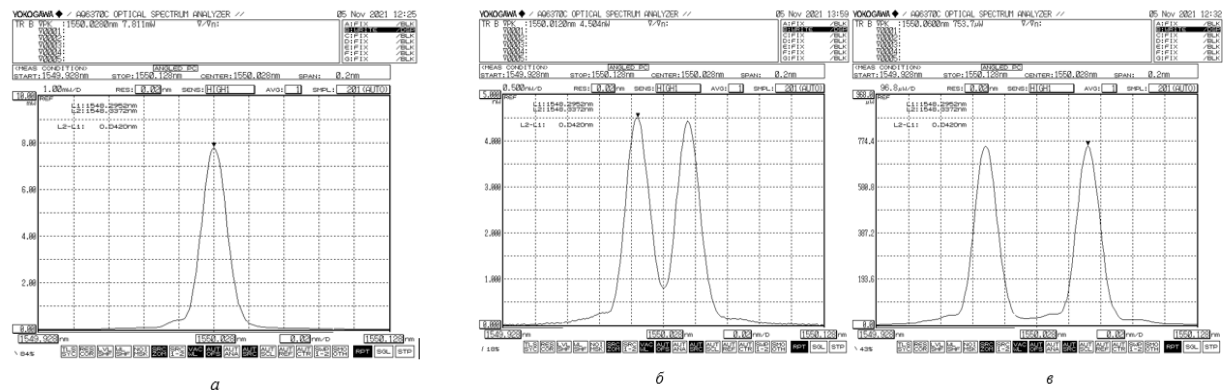


Рис. 2. Кодирование состояний фотонов $|+,1\rangle$ (а), $|+,2\rangle$ (б), $|-,2\rangle$ (в)

Вариант реализации симметричной структуры АМФК-ФКАМ в принципе может реализовать и базис (2) с пассивным выделением состояний $|\pm,2\rangle$, и активной рекоммутацией и ремодуляцией при определении состояний $|\pm,1\rangle$. Управление параметрами фазовой рекоммутации выполняет GRFS 2P с соответствующим изменением функций. Дополнительное введение стадий коммутации и рекоммутации позволит существенно повысить эффективность преобразования оптической несущей, повысить отношение сигнал/шум принимаемых сигналов и сократить полосу частот, занимаемую боковыми составляющими, на 25%, уже на стороне Боба, но не в квантовом канале. Данные утверждения сделаны на основе близких исследований по указанным параметрам, представленным по системам с АМ-АМ и ФМ-ФМ частотным кодированием [11-15].

2. Элементная база АПД УС РКК

Основой элементной базы каналов Алисы и Боба АПД выбраны:

- волоконно-оптическая линия связи, представляет собой одномодовое волокно SMF-28 с рабочей длиной волны 1550 нм различных производителей, например, ЗАО «Самарская оптическая кабельная компания»;

- источник монохроматического излучения, который может быть выполнен, как одностотный полупроводниковый лазер с волоконным выходом, с перестраиваемой длиной волны в диапазоне 1510-1560 нм и перестраиваемым значением выходной мощности от 3 до 10 мВт различных производителей, например, АО «НИИ «Полус» им. М.Ф. Стельмаха»;
- электрооптические амплитудный и фазовые модуляторы передающего устройства Алисы и приемного устройства Боба, может быть построен на кристалле ниобата лития (LiNbO₃) с потерями на пропускание 2.5-3 дБ различных производителей, например, ПАО «ПНППК»;
- радиочастотные генераторы, преобразователи, фазовые устройства сигнала передающего устройства могут быть выполнены, как устройства диапазона 2,0 - 8,0 ГГц различных производителей, например, АО «НПФ «Микран»;
- спектральные фильтры могут быть выполнены в виде одного многоканального с использованием ВБР, настроенных на несущую и боковые составляющие несущей фотона. Для его создания могут быть записаны ВБР с несколькими фазовыми π -сдвигами на волокне SMF-28, например, в НИИ ПРЭФЖС КНИТУ-КАИ;
- приемник классического излучения, может быть выполнен, как SFP транзиттер различных производителей, например, ООО «Модуль»;
- первый, второй, третий и четвертый приемники одиночных фотонов, могут быть выполнены, как детекторы одиночных фотонов на кремниевых лавинных диодах различных производителей, пока не российских, например: модели ID230, ID210, ID220, ID280 – фирмы ID Quantique (Швейцария).

Для макетирования АПД использовалась зарубежная база основной установки КРК на боковых частотах, установленная в Казанском квантовом центре КНИТУ-КАИ, и переносной установки на отечественной элементной базе, используемой в исследованиях и образовательном процессе НИИ ПРЭФЖС КНИТУ-КАИ.

Временно, в качестве источника монохроматического излучения применялся лазерный модуль TeraXion с блоком питания и оптическим изолятором (рис. 3-4). В реальном АПД он будет заменен на источники, комплектующие телекоммуникационные системы НИИ «Полус».



Рис. 3. Источник монохроматического излучения



Рис. 4. Источник питания для источника монохроматического излучения

На рис. 5-6 представлены используемые модуляторы в основной и переносной установках. На рис. 7 представлен макет АПД в разложенном виде для получения сигналов конструктивной и деструктивной интерференции на выходе канала ремодуляции.



Рис. 5. Амплитудный модулятор Torlabs

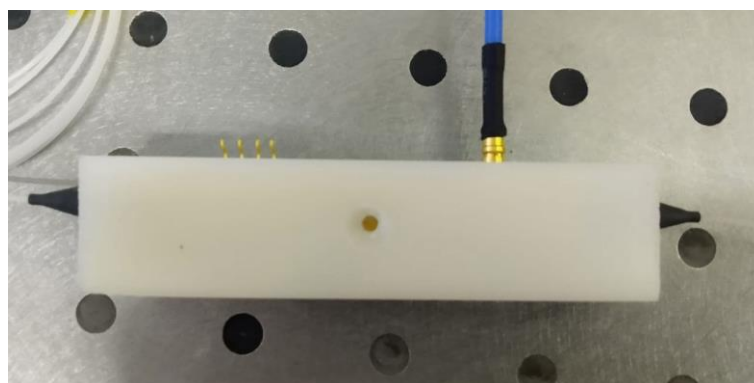


Рис. 6. Фазовый модулятор ПАО «ПНППК»

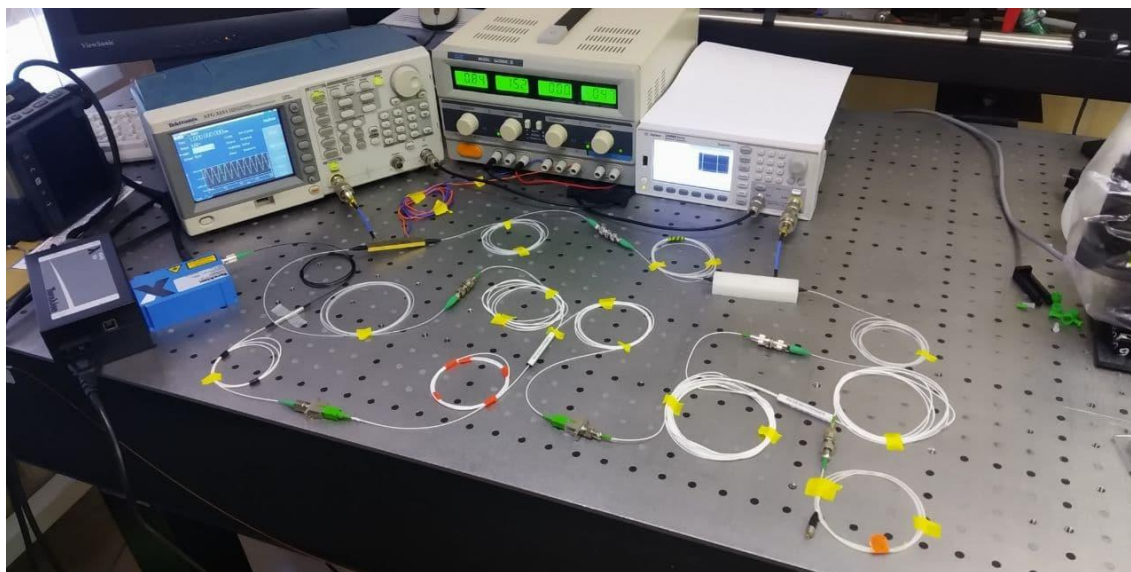


Рис. 7. Модуляторы в структуре макета АПД на рабочем столе

На рис. 8 представлены осциллограммы управляющих напряжений для амплитудного (верх) и фазового (низ) модуляторов.

На рис. 9 показаны полученные на выходе фотоприемника осциллограммы для случаев деструктивной (а) и конструктивной (б) ремодуляции, соответственно.

Таким образом, макетная реализации малофотонного варианта АПД УС РКК на основе ТАФМ подтвердила возможности его создания. Применение АПД позволит использовать несколько уровней криптографической защиты, в том числе с переключением схем модуляции и протоколов в варианте с ремодуляцией и без ремодуляции.

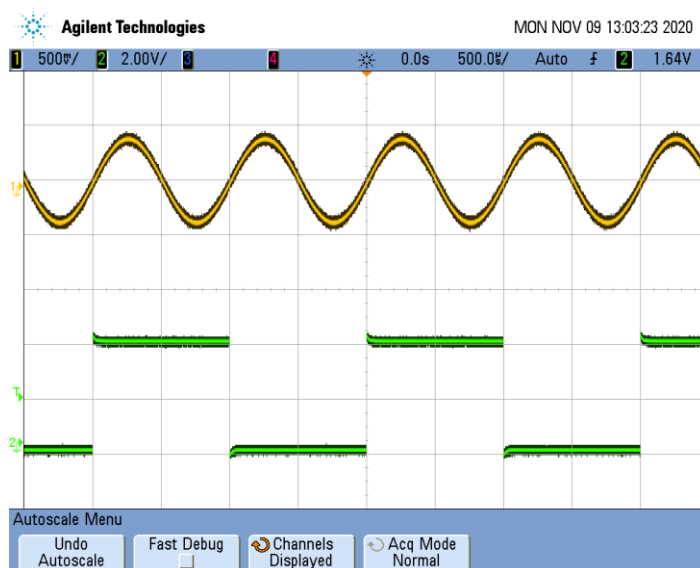


Рис. 8. Управляющие напряжения для модуляторов

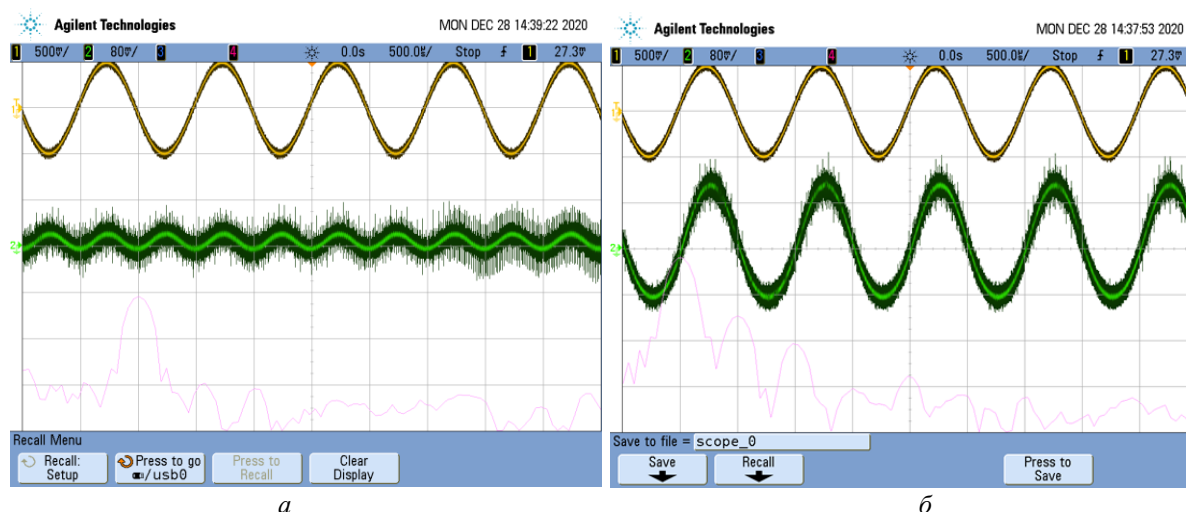


Рис. 9. Осциллограммы на выходе фотоприемника макета АПД для случая:
а) деструктивной ремодуляции, б) конструктивной ремодуляции

На разработанный АПД получен патент РФ на изобретение № 2692431 «Устройство квантовой рассылки криптографического ключа с частотным кодированием» [16].

3. Реализация АПД с пассивным приемником без ремодуляции

В собранном виде АПД применялся источник НИИ «Полус» и модуляторы ОАО «ПНППК». Дополнительно были установлены три сваренные катушки волокна SMF-28 производства Самарского завода для имитации линии связи (рис. 10).

АПД УС КРК ТАФМ с пассивным приемником был собран в корпусе системного блока настольного компьютера (рис. 11).

На рис. 12-14 показаны слои АПД, относящиеся к различным вариантам его реализации.

Основной целью эксперимента было подтверждение возможности формирования составляющих с дробной частотой от частоты модулирующего напряжения по амплитуде.

На рис. 15 и рис. 16 представлены полученные спектры, соответствующие $|+;2\rangle$ и $|-;2\rangle$ вариантам кодирования состояния фотона, которые соответствует теоретическим положениям (рис. 2,б и рис. 2,в).

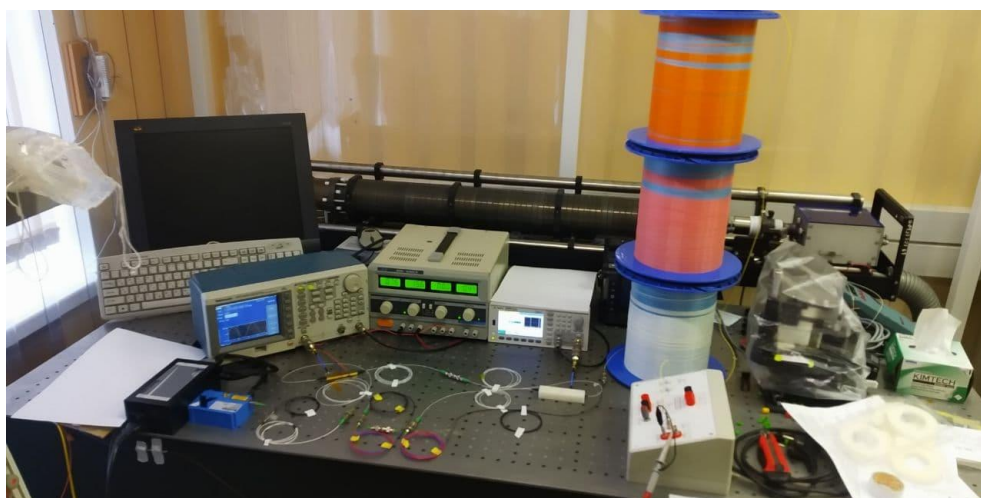


Рис. 10. Макет АПД с пассивным приемником в разложенном виде



Рис. 11. Макет АПД с пассивным приемником в собранном виде

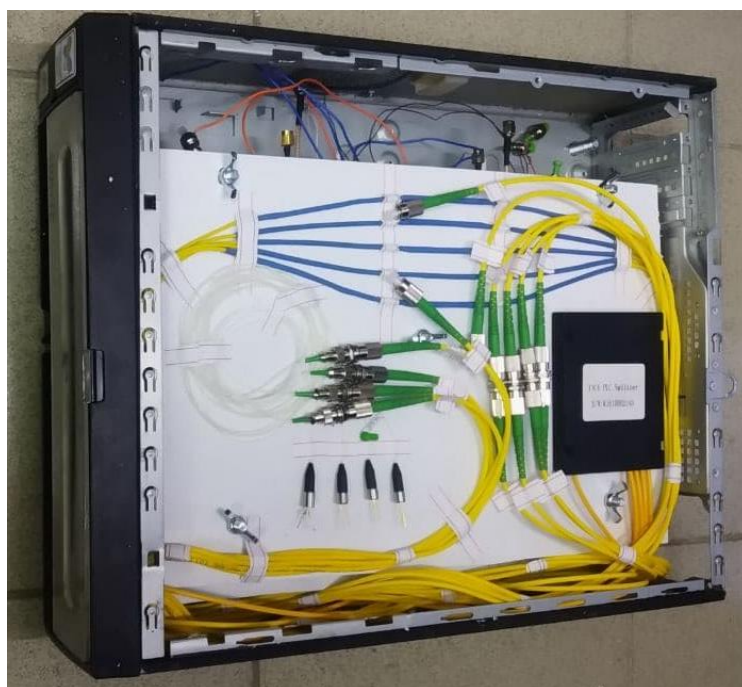


Рис. 12. Макет АПД. Блок фильтров на волоконных брэгговских структурах

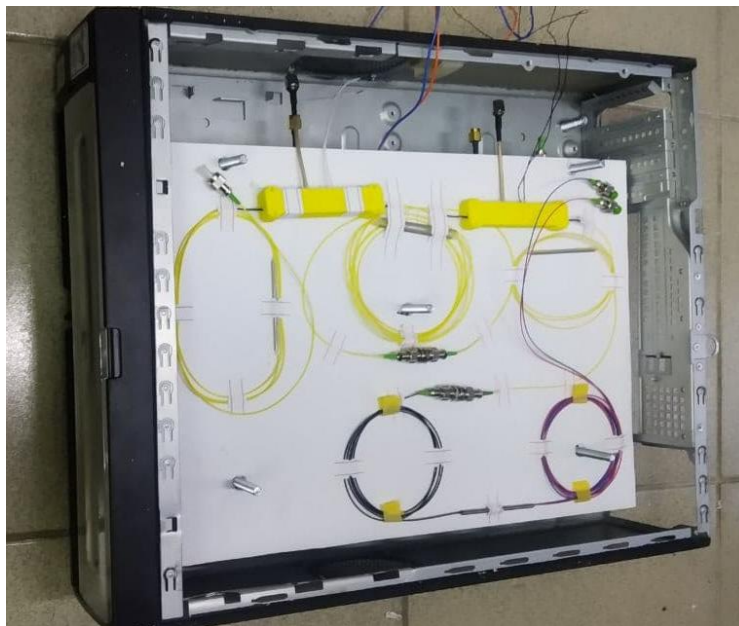


Рис. 13. Макет АПД. Блок Алисы на модуляторах ОАО «ПНППК»

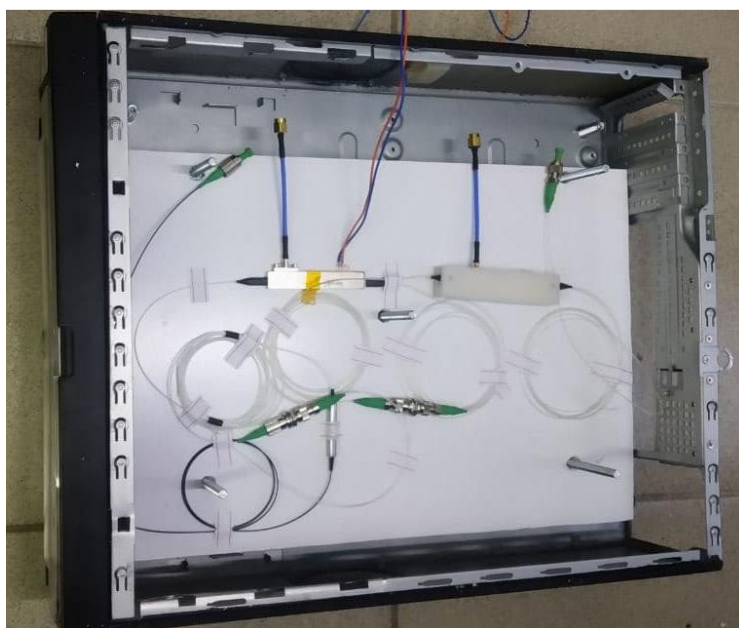


Рис. 14. Макет АПД. Блок Алисы и Боба на модуляторах Thorlabs

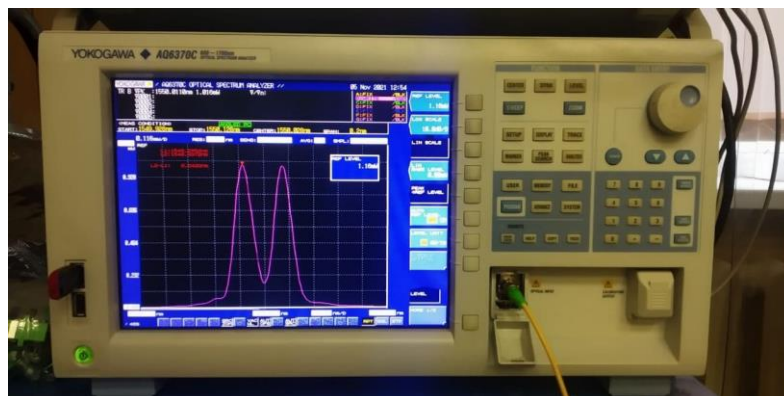


Рис. 15. Спектр, соответствующий состоянию фотона $|+;2\rangle$

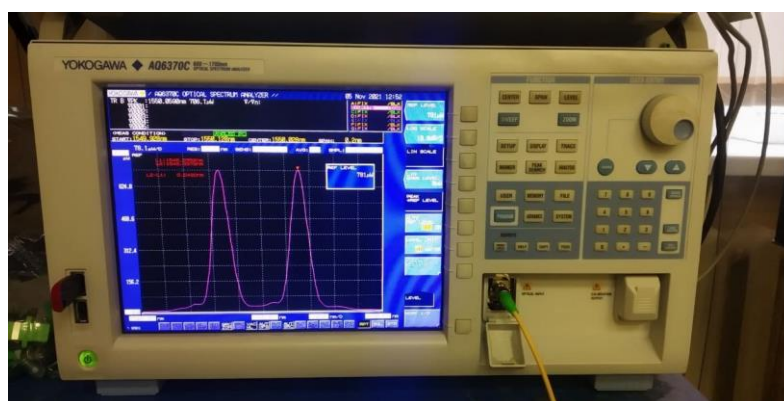


Рис. 16. Спектр, соответствующий состоянию фотона $|-;2\rangle$

Таким образом, разработанный вариант АПД УС КРК ТАФМ с пассивным приемником занимает свободное пространство, которое можно найти в системном блоке настольного компьютера, и позволяет снизить РВМ параметры при его изготовлении. Фактически АПД реализован на российской элементной базе, что отвечает функциям импортозамещения. Не отмеченные в данном разделе сведения об однофотонных фотоприемниках (показано в разд. 1) свидетельствуют о возможности их замены на российские в зависимости от принципиального назначения заказываемого АПД. Несомненно, при реализации в АПД 100%-но однофотонного режима, пока необходимо будет использовать импортные приемники.

Заключение

В статье представлены этапы разработки и создания экспериментального макета аппаратно-программного демонстратора универсальной системы квантового распределения ключей, реализующего существующие методы на основе амплитудной и фазовой модуляции, а также предложенный метод тандемной амплитудно-фазовой модуляции оптической несущей.

Проведена оценка технико-экономических и эксплуатационных характеристик аппаратно-программного демонстратора; сформулированы практические рекомендации по его разработке, созданию и эксплуатации, а также по выбору импортозамещающей элементной базы, что обеспечило его дешевизну и возможность широкого использования на

различных исследовательских и образовательных площадках, включая юношеские чемпионаты WorldSkills, а в дальнейшем и как устройства доступа в Интернет.

Работа выполнена в рамках гранта РФФИ «Конкурс на лучшие проекты фундаментальных научных исследований, выполняемые молодыми учеными, обучающимися в аспирантуре («Аспиранты»)» по теме «Универсальная система квантового распределения ключей с частотным кодированием на основе амплитудно-фазовой модуляции» (договор № 19-37-90057/19); работ по выполнению государственного задания КНИТУ-КАИ (программа «Фократ», соглашение № 075-03-2020-051, fzu-2020-0020) и работ по программе Приоритет-2030; в ходе инициативных исследований с организациями движения WorldSkills Республики Татарстан.

Список литературы

1. Пат. А 1338647 SU МПК4 G02F 1/03. Способ преобразования одночастотного когерентного излучения в двухчастотное / Ильин Г.И., Морозов О.Г.; заявитель КАИ им. А.Н. Туполева; заявл. 13.04.83; опубл. 20.07.2004. – Бюлл. № 20.
2. Пат. А1 1463010 SU МПК4 G02F 1/03. Двухчастотный лазерный излучатель / Ильин Г.И., Морозов О.Г., Польский Ю.Е., Терновсков В.Т.; заявитель КАИ им. А.Н. Туполева; заявл. 29.04.85; опубл. 20.07.2004. – Бюлл. № 20.
3. Пат. А1 1466494 SU МПК4 G02F 1/03. Двухчастотный лазерный излучатель / Ильин Г.И., Морозов О.Г., Польский Ю.Е.; заявитель КАИ им. А.Н. Туполева; заявл. 29.04.85; опубл. 20.07.2004. – Бюлл. № 20.
4. Пат. А1 1477130 SU МПК4 G02F 1/03. Двухчастотный лазерный излучатель / Ильин Г.И., Морозов О.Г., Польский Ю.Е.; заявитель КАИ им. А.Н. Туполева; заявл. 03.03.86; опубл. 20.07.2004. – Бюлл. № 20.
5. Морозов, О.Г. Амплитудно-фазовое преобразование частоты в системах временной и частотной рефлектометрии волоконно-оптических информационных и измерительных сетей / О.Г. Морозов // Физика волновых процессов и радиотехнические системы. - 2004. - Т. 7., № 1. - С. 63-71.
6. Морозов, О.Г. Амплитудно-фазовые методы формирования зондирующих излучений для систем анализа волоконно-оптических структур / О.Г. Морозов и др. // Физика волновых процессов и радиотехнические системы. - 2007. - Т. 10., № 3. - С. 119-124.
7. Морозов, О.Г. Синтез двухчастотного излучения и его применение в волоконно-оптических системах распределенных и мультиплексированных измерений / О.Г. Морозов, Д.Л. Айбатов, Т.С. Садеев // Физика волновых процессов и радиотехнические системы. - 2010. - Т. 13., № 3. - С. 84-91.
8. Morozov, O.G. Synthesis of two-frequency symmetrical radiation and its application in fiber optical structures monitoring / O.G. Morozov, G.A. Morozov, G.I. Il'in, T.S. Sadeev // Fiber optic sensors. - 2012. - P. 137-164.
9. Морозов, О.Г. Амплитудно-фазовая модуляция в системах радиофотоники / О.Г. Морозов, Г.И. Ильин // Вестник ПГТУ. - 2014. - №1(20).- С. 6-42.
10. Морозов, О.Г. Универсальная радиофотонная система квантового распределения ключей с частотным кодированием / О.Г. Морозов, И.М. Габдулхаков // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и информационные коммуникационные системы. – 2015. – № 2 (26). – С. 6-18.
11. Capmany, J. Quantum modelling of electro-optic modulators / J. Capmany, C.R. Fernandez-Pousa // Laser Photonics Rev. 5. – 2011. – № 6. P. 750–772.

12. Duraffourg, L. Compact transmission system using single-sideband modulation of light for quantum cryptography / L. Duraffourg, J.-M. Merolla, J.-P. Goedgebuer, Y. Mazurenko, W. T. Rhodes // Opt. Lett. – 2001. – V.26. – №18. – P. 1427-1429.
13. Bloch, M. Frequency-coded quantum key distribution / M. Bloch, S.W. McLaughlin, J.-M. Merolla, F. Patois // Opt. Lett. – 2007. – Vol. 32. – No 2. – P. 301-303.
14. Gleim, A.V. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference / A.V. Gleim, V.I. Egorov, Yu.V. Nazarov, et al. // Opt. Express. – 2016. – V.44. – №3. – P. 2619-2633.
15. Ruiz-Alba, A. Practical quantum key distribution based on BB84 protocol / A. Ruiz-Alba, D. Calvo, V. Garcia-Munoz, A. Martinez, W. Amaya, J.G. Roza, J. Mora, J. Capmany // Waves. – 2011. – No 3. – P. 4-14.
16. Патент 2692431 Российская Федерация, МКИ H04L 9/08 (2006.01), H04B 10/85 (2013.01). Устройство квантовой рассылки криптографического ключа с частотным кодированием / Морозов О.Г., Габдулхаков И.М., Нуреев И.И., Кузнецов А.А., Морозов Г.А., Сахабутдинов А.Ж.; заявитель и патентообладатель ФГБОУ ВО "Казанский национальный исследовательский технический университет им. А.Н. Туполева - КАИ" (RU). - № 2018124368; заявл. 03.07.2018., опублик.: 24.06.2019; Бюл. № 18.

HARDWARE AND SOFTWARE DEMONSTRATION QUANTUM KEY DISTRIBUTION SYSTEMS FOR YOUTH WORLDSKILLS CHAMPIONSHIPS

I.M. Gabdulkhakov, E.A. Gromov
(Supervisors: *O.G. Morozov, professor KNRTU-KAI;*
I.I. Nureev, professor KNRTU-KAI)

Kazan National Research Technical University named after A.N. Tupolev-KAI
10, K. Marx st., Russian Federation, 420111, Kazan

Annotation. The article discusses a hardware-software demonstrator for studying the characteristics of a quantum key distribution system with frequency coding based on tandem numerical-phase modulation conversion of an optical carrier and prepared by specialists in their operation. The demonstrator is a good candidate for import substitution during the WorldSkills Junior Championships. In addition, the proposed demonstrator, embedded in a desktop computer, can launch access to a terminal that can be connected to a terminal co-located with a quantum network node to store a secret key store that can be used to use the functions of daily activities on common platforms such as the Internet. .

Keywords: frequency-coded key distribution calculation system, tandem amplitude-phase modulation conversion of optical initiative, hardware-software demonstrator, import-substituting, research and educational platforms, WorldSkills youth championship, Internet access.

Статья представлена в редакцию 29 сентября 2022г.