УДК 621.383 *05.11.07*

УНИВЕРСАЛЬНАЯ СИСТЕМА КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА ОСНОВЕ АМПЛИТУДНО-ФАЗОВЫХ МОДУЛЯЦИОННЫХ ПРЕОБРАЗОВАНИЙ

И.М. Габдулхаков, О.Г. Морозов

Казанский национальный исследовательский
технический университет им. А.Н.Туполева-КАИ
Российская Федерация, 420111, г. Казань, ул. К. Маркса, 10.

Аннотация. Рассматривается возможность построения универсальной системы КРК, основанной на электрооптической схеме АМФМ-ФМАМ, позволяющей реализовать все ранее известные схемы ФМ-ФМ, АМ-АМ и АМ-ФМ (ФМ-АМ). Оцениваются характеристики схем, основанных на методе Ильина – Морозова – АМ и фазовой коммутации (ФК) – с возможностью реализации как симметричной структуры АМФК-ФКАМ с ремодуляцией и рекоммутацией, так и асимметричной – с пассивной фильтрацией АМФК-ВБР/УВР, а также перспективной многоканальной схемы АМФМ на основе гребенки поднесущих.

Ключевые слова: квантовая криптография, квантовое распределение ключей; частотное кодирование, электрооптическая модуляция фотона, амплитудно-фазовая тандемная модуляция.

Введение

Использование технологии квантового распределения ключей предоставляет уникальную возможность обмена случайной последовательностью битов между пользователями с гарантированной безопасностью, не достижимой в классических открытых или специальных системах с криптографической защитой [1].

1. Обзор

Технология частотного кодирования позволяет определить основное состояние фотонов через значение амплитуд его несущей частоты, модулированной по фазе или амплитуде радиочастотным сигналом, и полученных боковых составляющих [1]. За последние двадцать лет данная технология была существенно модифицирована и улучшена. Первоначально она использовалась для реализации КРК по модифицированному криптографическому протоколу B92. В этом случае уровень конструктивной или деструктивной интерференции обеих боковых составляющих, полученных с помощью фазовой модуляции (ФМ), определялся как функция типа косинус-квадрат от разности фаз между радиосигналами Алисы (легальный абонент – передатчик) и Боба (легальный абонент – приемник). При более детальном учете характеристик и применении амплитудной модуляции (АМ) вместо ФМ технология частотного кодирования была использована для реализации КРК по базовому криптографическому протоколу BB84. При этом в последних работах применяется расширенное понимание принципа

частотного кодирования, при котором каждому состоянию фотона ставится в соответствие не фаза модулирующего сигнала на некоторой частоте, а одна или несколько частот боковых составляющих либо сама оптическая несущая фотона.

2. Универсальная установка и ее структура

В схеме АМФМ-ФМАМ системы КРК с частотным кодированием (рис. 1) на стороне Алисы установлена передающая часть однопортового модуляционного радиофотонного звена последовательного типа, состоящая из маломощного импульсного лазера (далее МИЛ) – имитатора генератора одиночных фотонов, излучающего на несущей частоте ω_0; амплитудного модулятора Маха – Цендера (далее АММЦ) и фазового модулятора Маха – Цендера (далее ФММЦ) [2, 3]. На входе и выходе АММЦ установлены контроллеры поляризации (далее КП) скрещенного типа, позволяющие реализовать амплитудную модуляцию несущей при выборе различных рабочих точек на его модуляционной характеристике, а также управлять коэффициентом пропускания модулятора при отсутствии необходимости в модуляции.

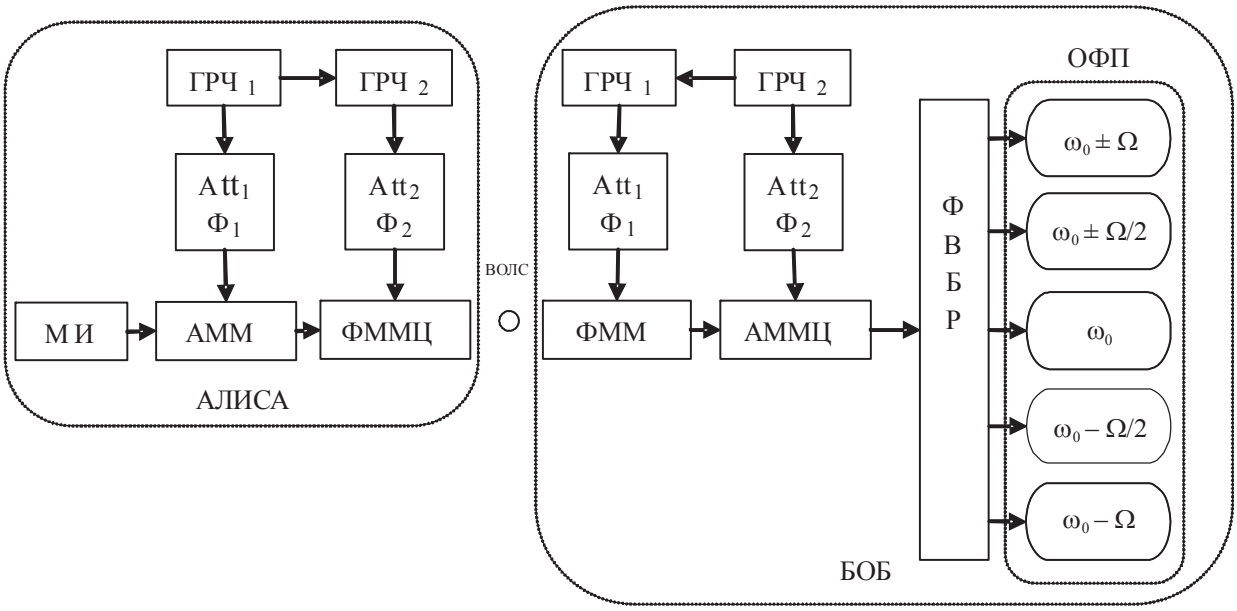

Рис. 1. Структурная схема АМФМ-ФМАМ системы КРК с частотным кодированием

Амплитудная и фазовая модуляции могут осуществляться с генератора радиочастотных колебаний (далее ГРЧ1) (А или Ф) с угловой частотой $\Omega << \omega_{00}$ и выбираемой фазой Φ_i из пары сопряженных базисов 0; π или $\pi/2$; 3 $\pi/2$. Для выбора рабочей точки модуляционной характеристики АММЦ служит источник постоянного смещения U_i, обеспечивающий работу модулятора в нулевой, четвертьволновой и полуволновой рабочих точках подачей на его вход соответствующего напряжения 0, $U_{\pi/2}$ или U_π, где U_π – полуволновое напряжение. Коэффициент модуляции как АММЦ, так и ФММЦ выбирается таким, чтобы обеспечить их рабо-

ту на линейном участке. При этом излучение на выходе однопортового модуляционного звена будет ограничено составляющими ω_0 и $\omega_0 \pm 2\Omega$, которые дополнительно выделяются фильтром на ВБР1. Установка такого звена обеспечивает возможность работы в режимах с амплитудной, фазовой, амплитудно-фазовой модуляциями и без модуляции.

На стороне Боба установлена приемная часть однопортового модуляционного радиофотонного звена последовательного типа, состоящая из ФММЦ, АММЦ, блока фильтров (далее ФВБР) и однофотонных фотоприемников (далее ОФП) для регистрации излучений на частотах ω_0 и $\omega_0 \pm \Omega$ и $\omega_0 \pm 2\Omega$.

Для передачи информации о модулирующем сигнале на частоте Ω от Алисы к Бобу служит специальный канал синхронизации, позволяющий использовать у Боба радиочастотный модулирующий сигнал той же частоты, что и у Алисы, с местного ГРЧ. Управление АММЦ и ФММЦ у Боба осуществляется аналогично вариантам, рассмотренным для модуляторов Алисы.

3. Анализ результатов, полученных известными электрооптическими схемами

Известные схемы электрооптической модуляции и ремодуляции описываются симметричными парами ФМ-ФМ, АМ-АМ и АМ-ФМ (ФМ-АМ), где первая составляющая определяет тип модуляции и модулятора на стороне Алисы, а вторая – на стороне Боба [3]. Известна схема с реализацией модуляции и ремодуляции на основе акустооптических технологий с пространственным разносом несущей и боковых составляющих. При этом отмечается, что наименьшее значение QBER достигается в схемах с пассивным определением одного или двух основных состояний фотона, т.е. без использования процессов ремодуляции, а формирование системы фильтров осуществляется с использованием волоконных брэгговских решеток (ВБР) или упорядоченных волноводных решеток (УВР), настроенных на несущую и боковые составляющие несущей фотона.

4. Возможность реализации модуляционного преобразования АМФМ-ФМАМ и ее преимущества

В основе работы АМФМ-ФМАМ системы КРК с частотным кодированием лежит модуляционное преобразование несущей фотона на основе метода Ильина – Морозова и его одно- и двухмодуляторная реализация [4, 5]. Для моделирования схемы и проведения проектных оценок были использованы принципы построения однопортового модуляционного радиофотонного звена последовательного типа и фотонного моделирования электрооптической модуляции. Использование метода Ильина – Морозова для перехода Р ($\omega_0 \rightarrow \omega_0 \pm n\Omega$), где n – номер гармоники, позволит получить:

– высокую эффективность перехода оптической несущей в боковые составляющие (до 0,6 – 0,8 по амплитуде для каждой из них);

– высокий уровень спектральной чистоты выходного излучения фотона на выходе АФМК модуля при оптимальных параметрах преобразования (при отклонении параметров от оптимальных до 10 %, коэффициент нелинейных искажений составит 0,01);

– возможность работы как с целыми компонентами боковых частот ($n \geq 1$), так и дробными ($n/2$, при $n \geq 1$), что позволит повысить уровень криптографической защиты системы связи

в случае обнаружения Евой канала синхронизации и получения ею доступа к данным, принятым Бобом;

– возможность формирования асимметричной системы с полностью пассивной фильтрацией данных, переданных Алисой, на стороне Боба без ремодуляции.

5. Перспективное решение системы АМФМ на основе гребенки поднесущих и исключения ремодуляции

Для повышения скорости передачи ключа используется схема на основе множества поднесущих (рис. 2).

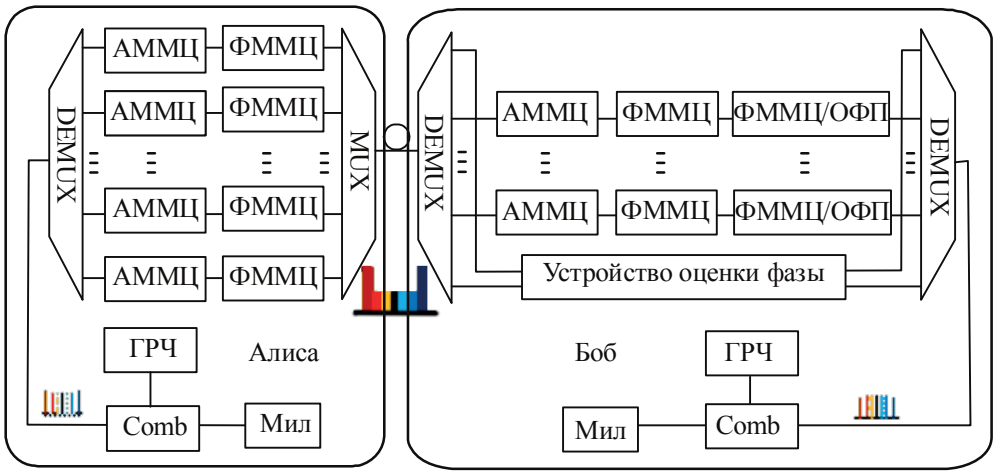

Рис. 2. Структурная схема многоканальной системы КРК

При многоканальной схеме [6] общая скорость передачи секретного ключа может быть выражена как сумма скорости каждого подканала:

$$V_{\text{общ}} = \sum_{k} V_k \,, \tag{1}$$

где k – количество квантовых подканалов.

Алиса генерирует оптические частотные гребенки с центральной частотой f_0 и частотой повторения f_s в качестве многоволнового источника, который может быть выражен как:

$$\hat{\mathrm{s}}(t) = \sum_{n=n_{\min}}^{n_{\max}} \hat{\mathrm{a}}_n \exp\left\{ j\left[-\varphi(t) + 2\pi f_n t \right] \right\}, \tag{2}$$

где $\hat{\mathrm{a}}_n$ – безразмерный комплексный оператор амплитуды, соответствующий режиму, представленному в n-х гребенчатых линиях с частотой $f_n = f_0 + nf_r$; случайная функция $\varphi(t)$ – фазовый шум в гребенке; $n_{\max}$ и $n_{\min}$ – две крайние внешние линии оптической частотной гребенки.

Оптические частотные гребенки сначала проходят через демультиплексор для формирования N подканалов, где количество подканалов равно количеству гребенчатых линий. Подканал k, который изменяется от $n_{\min}+1$ до $n_{\max}-1$, независимо модулируется по амплитуде

с помощью V_k и последующей фазовой коммутацией с помощью $Ф_k$. После этого все подканалы объединяются частотным мультиплексором и передаются Бобу.

Данный метод увеличивает безопасность передачи за счет исключения несущей из структуры сигнала, передаваемого по квантовому каналу распределения ключей, и разбиение информации о ключе на множество каналов.

Таким образом, можно выделить два основных преимущества: первое – увеличение скорости передачи ключа, второе – для получения положительного результата Еве необходимо получить информацию о передаваемом сигнале в каждом подканале одновременно, поскольку квадратурные информации каждого подканала не зависят друг от друга.

Заключение

Из приведенных результатов можно выделить основные преимущества разрабатываемой универсальной системы квантового распределения ключей на основе амплитудно-фазовых модуляционных преобразований: повышение скрытности канала КРК и скорости передачи ключа.Данную установку можно использовать при проведении мировых чемпионатов World Skills среди юниоров, школьников и студентов в компетенции «Квантовые технологии», так как с ее помощью можно удовлетворить требования к участникам: смонтировать и подготовить к работе оптоволоконную линию связи, настроить и установить устройства для квантовозащищенного распределения ключей, откалибровать линию и оборудование с минимальными затратами по сравнению с другими технологиями КРК.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90057.

СПИСОК ЛИТЕРАТУРЫ

1. *Морозов, О.Г., Габдулхаков, И.М.* Амплитудно-фазовая радиофотонная система квантового распределения ключей с частотным кодированием // Физика волновых процессов и радиотехнические системы. – 2015. – Т. 18. – № 3-2. – С. 62-69.

2. *Морозов, О.Г., Габдулхаков, И.М.* Универсальная радиофотонная система квантового распределения ключей с частотным кодированием // Вестник Поволжского государственного технологического университета. Серия: Радиотехнические и инфокоммуникационные системы. – 2015. – № 2 (26). – С. 6-18.

3. *Морозов, О.Г., Габдулхаков, И.М.* Многофункциональная система квантового распределения ключей с частотным кодированием // Фотон-экспресс. – 2015. – № 6 (126). – С. 208-209.

4. *Морозов, О.Г., Габдулхаков, И.М.* Радиофотонный канал квантового распределения ключей с частотным кодированием и амплитудно-фазовой модуляцией фотона // Физика волновых процессов и радиотехнические системы. – 2017. – Т. 20. – № 3-2. – С. 37-40.

5. *Габдулхаков, И.М., Морозов, О.Г.* Поляризационный модулятор на основе тандемной реализации амплитудно-фазовой модуляции // Системы синхронизации, формирования и обработки сигналов. – № 1. – 2018. – С. 42-49.

6. *Габдулхаков, И.М., Морозов, О.Г.* Построение многоканальной системы квантового распределения ключей с частотным кодированием // Инженерный вестник Дона. – № 5. 2020.URL: http://www.ivdon.ru/ru/magazine/archive/N5y2020/6438, ISSN 2073-8633. (Дата обращения: 11.05.2021).

UNIVERSAL SYSTEM OF QUANTUM KEY DISTRIBUTION, BASED ON AMPLITUDE-PHASE MODULATION TRANSFORMATIONS

I.M. Gabdulkhakov, O.G. Morozov

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

Abstract. The article considers the possibility of constructing a universal QKD system based on the electro-optical AMPM-PMAM scheme, which allows implementing all previously known PM-PM, AM-AM and AM-PM (PM-AM) schemes. The characteristics of the schemes based on the Ilyin – Morozov – AM method and phase switching (PC) – with the possibility of implementing both a symmetric AMPC-PCAM structure with remodulation and recommutation, and an assimitric one – with passive filtering of AMPC-FBG/AWG, as well as a promising multi-channel AMPM scheme based on a subcarrier comb.

Keywords: quantum cryptography, quantum key distribution; frequency coding, electro-optical photon modulation, amplitude-phase tandem modulation.

***Funding**: The reported study was funded by RFBR, project number 19-37-90057.*

Дата поступления статьи в редакцию 11.05.2021.