Chapter 6

Universal Microwave Photonics Approach to Frequency-Coded Quantum Key Distribution

Oleg G. Morozov, Airat J. Sakhabutdinov,
Gennady A. Morozov and Il'daris M. Gabdulkhakov

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.71974

Abstract

Design principles of universal microwave photonics system (MPS) for quantum key distribution (QKD) with frequency coding are concerned. Its main modulation concept lies in single photon generation on sidebands of optical carrier and determination of photons ground state through its registration and the amplitude value of its carrier frequency as reference channel. So, it is necessary to solve problems of signal-to-carrier ratio of single photon detector (SPD) and aspects of photon number splitting (PNS) attack, nonlinear phase modulation (NPM) between carrier and sidebands in fiber, and finally, spectral selection of carrier in receiver. The technologies, based on the modulation conversion of an optical carrier, are widely used in microwave photonics. Due to the natural symmetry of modulated signals and the highest achievable ratio of the modulation conversions, amplitude-phase modulation with complete or partial suppression of the optical carrier has found a particularly wide application in MPS. The characteristics of advanced MPS for QKD with frequency coding and carrier suppression based on tandem amplitude modulation and phase commutation are presented. New systems can have classical symmetric or non-classical asymmetric structure for QKD based only on spectral selection of carrier and subcarriers without re-modulation.

Keywords: quantum key distribution, frequency encoding and decoding, photon-modulated components, amplitude, phase and meshed amplitude/phase modulation, tandem amplitude modulation and phase modulation or commutation, re-modulation, passive spectral selection without re-modulation, microwave photonics decisions

1. Introduction

Quantum communication networks provide a unique opportunity of sharing a random sequence of bits between users with guaranteed security not achievable in classical open or special systems with cryptographic protection [1]. This is achieved by means of quantum key distribution (QKD) technology use.

Nowadays, there are at least four basic photonic QKD technologies: polarization [2], interferometric [3], differential phase shift [4] and frequency encoding [5]. The polarization technology is based on the features of four photons' fundamental states consideration and encoding, using one conjugate base of circular polarization and one of linear. The main disadvantage of this technology is the inability to maintain the polarization state of the photon along the entire length of fiber optic communication lines (FOCL). Interference technology relies on the use of optical delay lines and balanced interferometers in FOCL transmitter and receiver. The basic requirement for the implementation of this technology is to maintain the phase stroke difference of interferometers when exposed to temperature, vibration and other factors that are hard to realize. A phase technology is an approach based on the methods of differential phase shift, which allows implementing the QKD technology at FOCL lengths over 100 km, although with limited security [6].

The technology of frequency encoding allows determining the ground states of photons through the amplitude value of its carrier frequency, modulated in phase and/or amplitude by radiofrequency (RF) signal and the received high-order sidebands (subcarriers). This technology, based on the modulation conversion of multiphoton optical carrier, is widely used in microwave photonics, in its various classic applications [7–9].

Standard implementation of frequency encoding technology in quantum communication networks can be described as follows [10]. Alice (legal subscriber, transmitter) randomly changes the phase of the RF signal used to modulate the photons, among four discrete values $0;\pi,\ldots,\pi/2;3\pi/2$, which form a pair of conjugate bases, and sends it by FOCL quantum channel to Bob (legal subscriber, receiver). Bob modulates receiving photons again, using the same frequency RF signal as Alice, but with its own discrete phases, independent from Alice, from the same paired bases $0;\pi,\ldots,\pi/2;3\pi/2$. Along with this, the new order photon sidebands on the Bob's side will interfere with photons' sideband components received from the Alice's side. The interference result will determine the correctness of the adopted phase information and the encoded photon's state. For simplicity, quantum communication channel with sidebands only of first order is considered.

Over the last 20 years, this technology has been substantially modified and improved. Initially, it was used to implement the QKD in hardware, based on the modified cryptographic B92 protocol [11]. In this case, the level of constructive or destructive interference of the two lateral components, obtained by means of phase modulation (PM), was determined as a function of the cosine-squared type from the phase difference between the Alice and Bob signals. In more detailed characteristic consideration, the amplitude modulation (AM) application was used instead of phase technology to implement the QKD in hardware, based on the underlying cryptographic BB84 protocol [12], although the last one in theory was designed earlier than BB92 one. Thus, for the amplitude of the upper lateral components, the function of the sine square of the phases difference is characterized, and for the bottom—cosine-squared one. The optimal implementation of the QKD frequency encoding technology and the most clearly cryptography protocol BB84 can be obtained by using AM (Alice) and PM (Bob) (or PM-AM), which was shown in [13]. In the latter works, a broad understanding of frequency encoding principle is used, where to each state of the photons, instead of the phase of the modulating signal at a certain frequency, one or more lateral component frequencies either photon optical carrier [14] are put into line.

The symmetric pairs of the PM-PM, AM-AM and meshed AM-PM (PM-AM) are described by known electro-optical modulation and re-modulation schemes, where the first component determines the type of modulation and modulator on the side of Alice, and the other—on the side of Bob. The most important features of this type of QKD system are simplicity of schemes and phase shift matching decisions on both sides of quantum channel, efficient use of its bandwidth and capability to add quantity of subcarriers using one carrier source [15]. From another point of view [16], the smallest value of QBER is achieved in circuits with passive definition of photons states, without re-modulation and using only filter systems based on fiber Bragg gratings (FBG) or arrayed waveguide gratings (AWG) for subcarriers or carrier selection. Thus, we have to analyze as symmetrical systems with re-modulation, so and asymmetrical ones without re-modulation and only filter selection.

Disadvantages of above-described QKD systems are connected mainly with strong carrier and photon subcarrier levels' interaction along the optical fiber and its energy meshing. First, in [17], it was shown that effects of nonlinear phase modulation (NPM) are small on temporally separable sources utilizing symmetric group velocity matching but appreciably change the state of temporally entangled sources with the same group velocity-matching scheme. The largest changes to the state due to NPM occur in long FOCL with long pulse durations and low repetition rates (in limit, it is CW-technology of QKD with frequency coding). Second, in [18], it was shown that most quantum setups use simple attenuation of laser carrier as a source of quantum states. In such cases, average probability of single photon emission per time unit is equal to $\mu \approx 0.1$. The security condition in this case is no longer strict due to Poisson distribution of photons, so carrier or subcarriers may contain more than one photon. This fact can be easily used by Eve—illegal agent. She successfully can perform undetectable beam splitting or photon number splitting (PNS) attack without changing QBER and receive a part of the key, which can be significant at higher μ. Third, in [15], it was shown that quantum information transfer devices at subcarrier frequencies of modulated radiation required an exact separation of the quantum subcarrier signal and central wavelength. Inadequate extinction of the signal on the main frequency significantly reduces the signal-to-noise ratio of the system and leads to a significant increase in the number of errors in the quantum communication channel. Therefore, the QKD technology with frequency coding, based on the modulation conversion of an optical carrier with its complete or partial suppressing, is the actual problem to improve quantum channel characteristics.

Due to the natural symmetry of modulated signals and the highest achievable ratio of the modulation conversions, amplitude-phase modulation with complete or partial suppression of the optical carrier has found a particularly wide application in the systems of microwave photonics [19]. Let us apply microwave photonics principles to design of QKD systems with frequency encoding.

We present in this chapter the results of the universal QKD system design, based on a tandem electro-optic AMPM-PMAM scheme built on microwave photonics principles applied to photon carrier modulation. It allows us to implement all of the above-mentioned classical symmetrical schemes PM-PM, AM-AM and meshed AM-PM (PM-AM) and also to review the requirements for building a promising tandem AM and phase commutation (PC) scheme with the possibility of implementing a nonclassical asymmetric structure with passive filtering (FBG/AWG) on Bob's side and suppressed carrier.

The chapter in the main is based on the results of analytical review of [1–19], materials of Morozov et al. [20] and additional and new results of theoretical and experimental researches in QKD theme and miscellaneous applications. Next chapter sections are organized as follows. The second section shows the principles of design of QKD systems with frequency encoding based on the classical approaches; key nodes involved for the implementation of PM-PM, AM-AM and meshed AM-PM (PM-AM) schemes are described; the descriptions of protocol bases and some experimental results are given; the advantages and disadvantages of classical schemes are evaluated, and the ways of its development are discussed. The third section discusses the design of promising universal tandem AMPM-PMAM scheme and its microwave photonic (MWP) basis; version of QKD system with tandem amplitude modulation and phase commutation of photons is proposed; the capabilities of re-modulation and possibilities of re-commutation procedures, or their absent and using only passive filtering structure realizations. In conclusion, the received results are analyzed and the key development challenges for QKD systems with frequency encoding are highlighted.

2. Implementation of classical QKD schemes with frequency encoding

Let us consider implementation of various modulation schemes, relying on the chronology of QKD systems with frequency encoding. The protocols BB84 [12] and B92 [11] are two main protocols used for their construction. During the BB84 protocol realization, Alice prepares and sends to Bob a lot of random qubits, chosen from the four main states:

$$\begin{cases} |\psi_0\rangle = |0\rangle \\ |\psi_1\rangle = |1\rangle \end{cases}$$
$$\begin{cases} |\psi_+\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle] \\ |\psi_-\rangle = \frac{1}{\sqrt{2}}[|0\rangle - |1\rangle] \end{cases} \quad (1)$$

The first two states in (1) form one basis of two-dimensional quantum system, and the other two form second basis.

It is necessary to fulfill the terms $\langle\psi_0|\psi_1\rangle = 0$ and $\langle\psi_+|\psi_-\rangle = 0$, corresponding to the scalar production of their components. At the same time, the mentioned states of different bases are not orthogonal and maximum overlap [12]. Therefore, there is no measurement procedure, at which Eve can determine the state prepared by Alice and sent to Bob at 100% probability [21].

B92 protocol [11] is the modernization of BB84 protocol and is used to encode one of the two presented in (1) bases.

2.1. PM-PM schemes

One of the first PM-PM scheme variants is based on the B92 protocol [22]. Its OptiSystem model is presented in **Figure 1**.

Alice modulates photon $|\omega_0\rangle$ in left PM by RF signal from sine generator with frequency Ω and phase $\Phi = \Phi_A$, getting:

$$|A\rangle = \sum_{n=-\infty}^{n=+\infty} J_n\, exp^{jn\Phi_A} |\omega_n\rangle, \tag{2}$$

where, for simplicity of display, the argument of the Bessel's function J_n is not specified. On the receiving end, Bob modulates the input radiation synchronized with Alice RF signal from its sine generator (right) phase $\Phi = \Phi_B$. At Bob's PM output, one will receive:

$$|B\rangle = \sum_{n,k} J_n J_{k-n}\, exp^{jn\Phi_A}\, exp^{j(k-n)\Phi_B} |\omega_k\rangle \tag{3}$$

It should be noted that modulation effect is to transfer energy from carrier on the sidebands (subcarriers). Its effectiveness depends on modulation and corresponding phases Φ_A and Φ_B. Transfer efficiency $P(\omega_0 \rightarrow \omega_0 \pm \Omega)$ is proportional to the function $\cos^2(\Delta\Phi/2)$, where $\Delta\Phi = \Phi_B - \Phi_A$, and is at maximum when $\Delta\Phi = 0$, which indicates the same basis chosen by Alice and Bob (**Figure 2**).

Further exchange of information between Alice and Bob allows them to set a secure connection with the implementation of the B92 protocol. The definition of a key with probability equal to one for Eve is impossible.

Determination of phase's compliance level in the scheme is actually implemented by the amplitude of the subcarriers. That is also the evidence of these scheme drawbacks, taking into account the small power of optical subcarriers and the presence of noise in the communication channel and single photon detector (SPD).

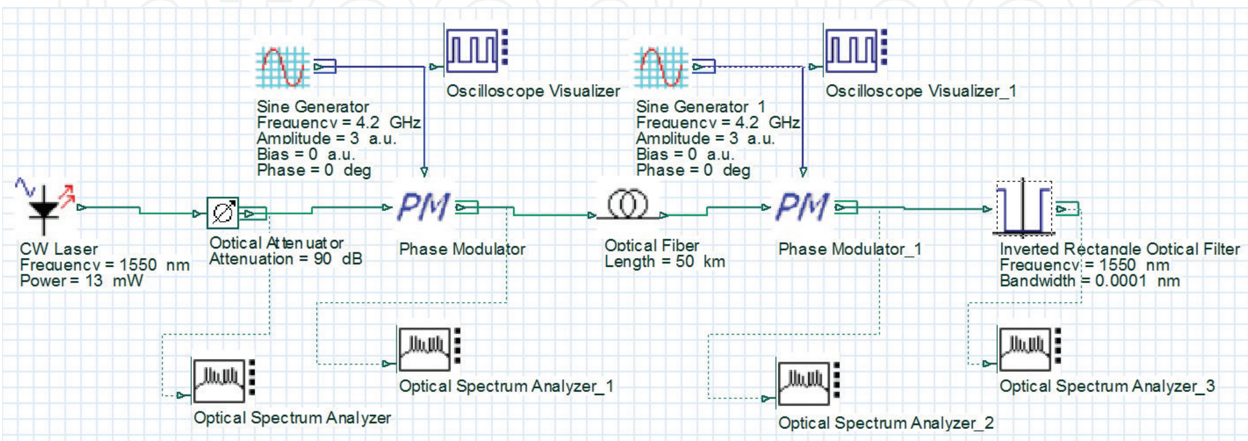

Figure 1. Modeling of PM-PM scheme for QKD system with frequency coding.

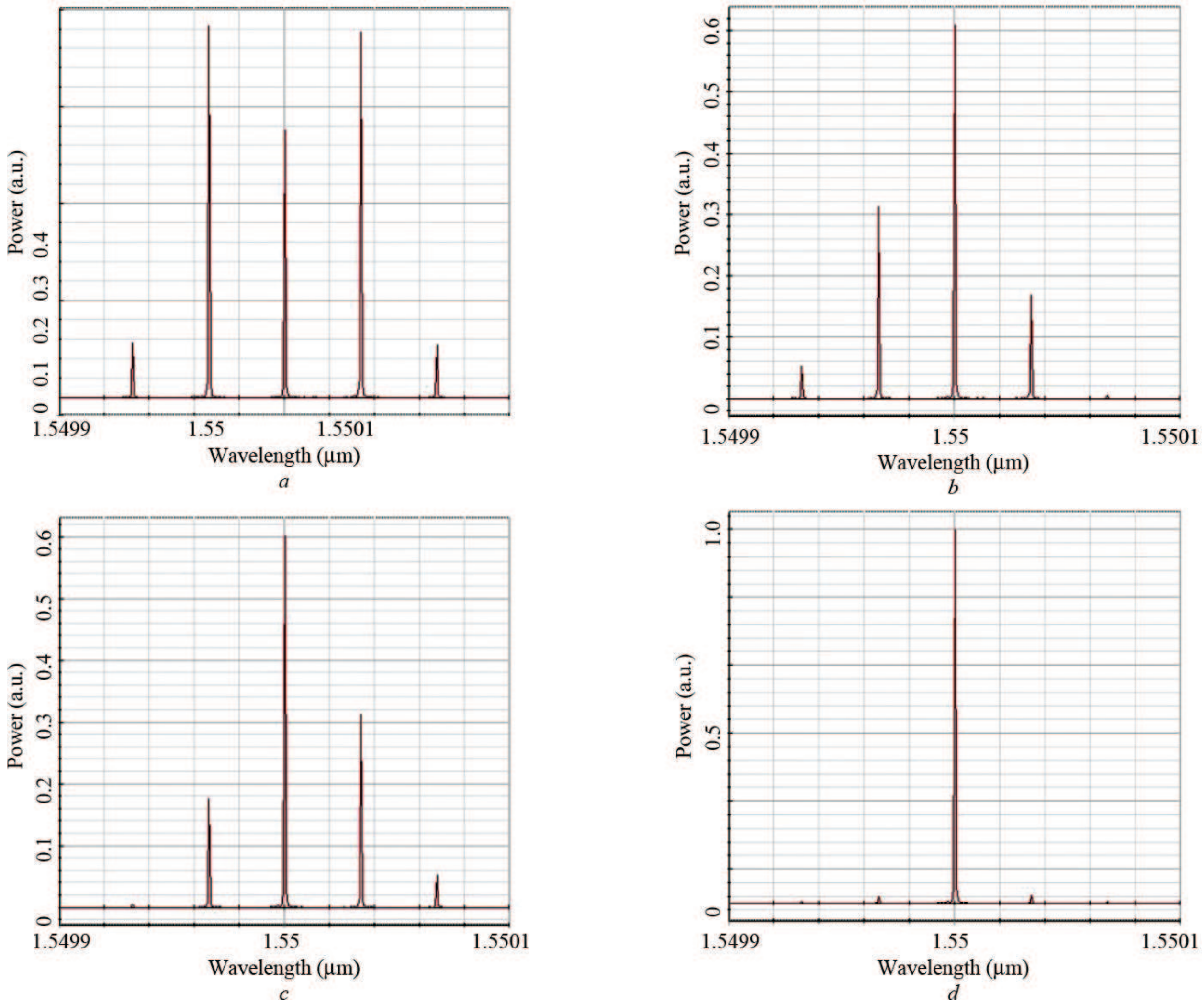

Figure 2. Constructive $\Delta\Phi = 0$ (a) and destructive $\Delta\Phi = \pi/2$ (b), $\Delta\Phi = 3\pi/2$ (c), $\Delta\Phi = \pi$ (d) interferences on the output of Bob's PM, when Alice's $\Phi_A = 0$.

A second version of the PM-PM scheme [14] was proposed for elimination of given drawbacks. It is based on nonlinear interaction of the RF signal and the photon in the electro-optic modulator and implements a more advanced BB84 protocol. Notch filter on ω_0 frequency is set prior to sideband SPD, which reflects the carrier at the corresponding receiver, transmitting all the remaining subcarriers on $\omega_0 \pm \Omega$ and $\omega_0 \pm 2\,\Omega$ frequencies.

For BB84 protocol realization, two bases are set as following:

$$\begin{cases} |+;\ 1\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0} + \frac{1}{2}|1\rangle_{\omega_0+\Omega} - \frac{1}{2}|1\rangle_{\omega_0-\Omega} \\ |-;\ 1\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0} - \frac{1}{2}|1\rangle_{\omega_0+\Omega} + \frac{1}{2}|1\rangle_{\omega_0-\Omega} \end{cases}. \quad \begin{cases} |+;\ 2\rangle = |1\rangle_{\omega_0} \\ |-;\ 2\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+\Omega} - \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-\Omega} \end{cases} \tag{4}$$

The |±;2⟩ states are determined without applying the re-modulation, by the use of filter sets based on FBG or AWG and logic conditions. Scheme decision shows the lowest QBER value. Only sideband SPD also works during the transfer of |±;1⟩ states, because at specified conditions of modulation and re-modulation the component at frequency ω_0 is equal to 0. The error level in transmission |±;1⟩ states is 4.7%.

AM-AM schemes use for elimination of PM-PM ones shortcomings. One of them was implemented only on the acousto-optic modulators [16].

2.2. AM-AM schemes

The first AM-AM scheme is based on BB84 protocol [23]. Its OptiSystem model is presented in **Figure 3**, and constructive and destructive interferences are shown in **Figure 4**.

It should be noted that the modulator on the of Alice's side is modulated according to the law $\cos(\Omega t + \Phi_A)$, and on the Bob's side according to $\sin(\Omega t + \Phi_B)$. Transfer efficiency $P(\omega_0 \rightarrow \omega_0 \pm \Omega)$ in this case is proportional to function $\cos^2(\Delta\Phi/2)$ and $\sin^2(\Delta\Phi/2)$ for the upper and lower side bands, respectively, at $\Phi_A = \pi/2$ and $\Phi_B = 3\pi/2$. Determination of phase's compliance level in the scheme is also implemented by the amplitude of the lateral components.

2.3. Meshed AM-PM (PM-AM) schemes

AM-PM or PM-AM scheme implementation intuitively appears to be based on the principles set out, respectively, for AM-AM and PM-PM schemes. One of its OptiSystem model is presented in **Figure 5**.

Determination of phase's compliance level in the scheme is also implemented by the amplitude of the lateral components (**Figure 6**).

It should be noted that we have some conflicting information about the possibility [13] and impossibility [23] of meshed AM-PM (PM-AM) scheme realization as for protocol BB84, so

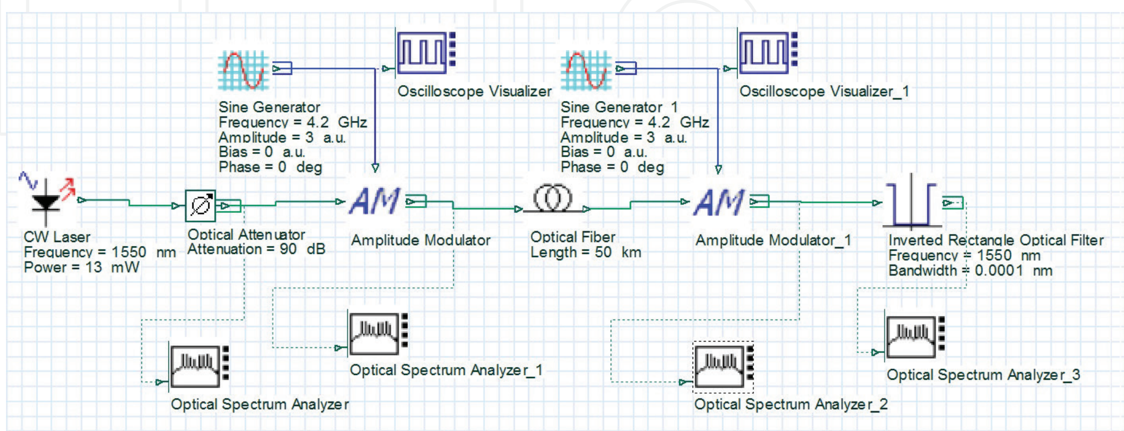

Figure 3. Modeling of AM-AM scheme for QKD system with frequency coding.

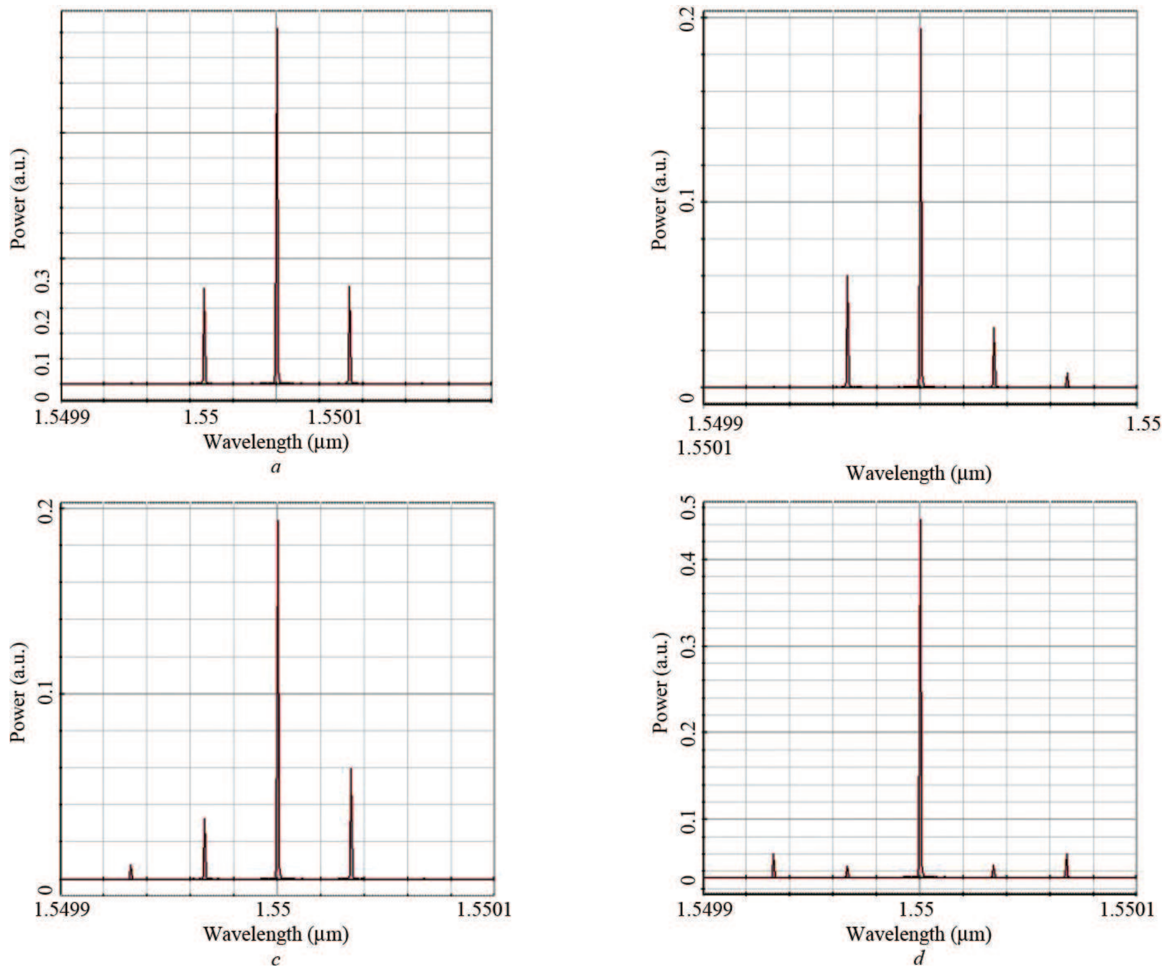

Figure 4. Constructive $\Delta\Phi = \pi$ (a) and destructive $\Delta\Phi = \pi/2$ (b), $\Delta\Phi = 3\pi/2$ (c); $\Delta\Phi = 0$ (d) interferences on the output of Bob's PM, when Alice's $\Phi_A = 3\pi/2$.

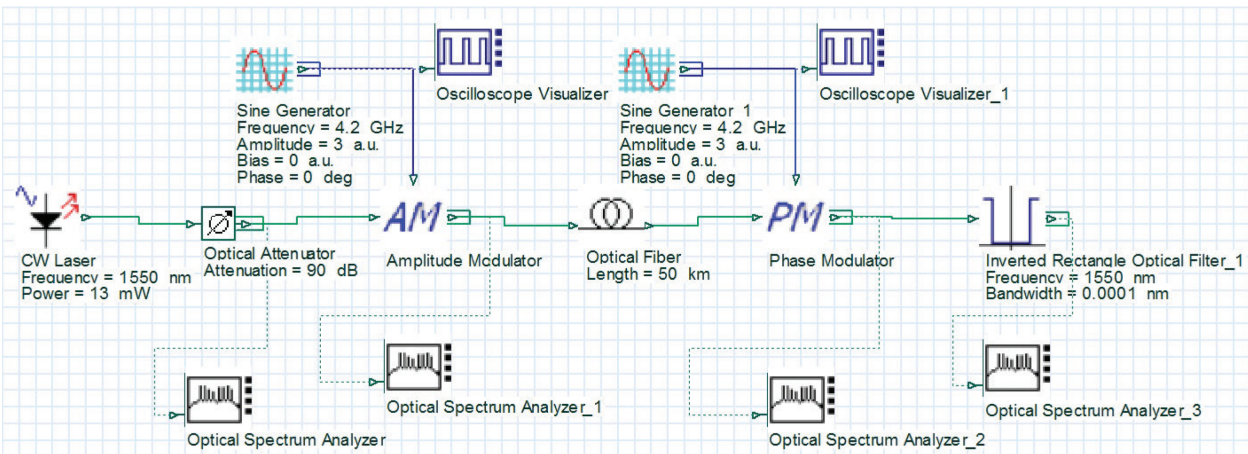

Figure 5. Modeling of AM-PM scheme for QKD system with frequency coding.

http://dx.doi.org/10.5772/intechopen.71974

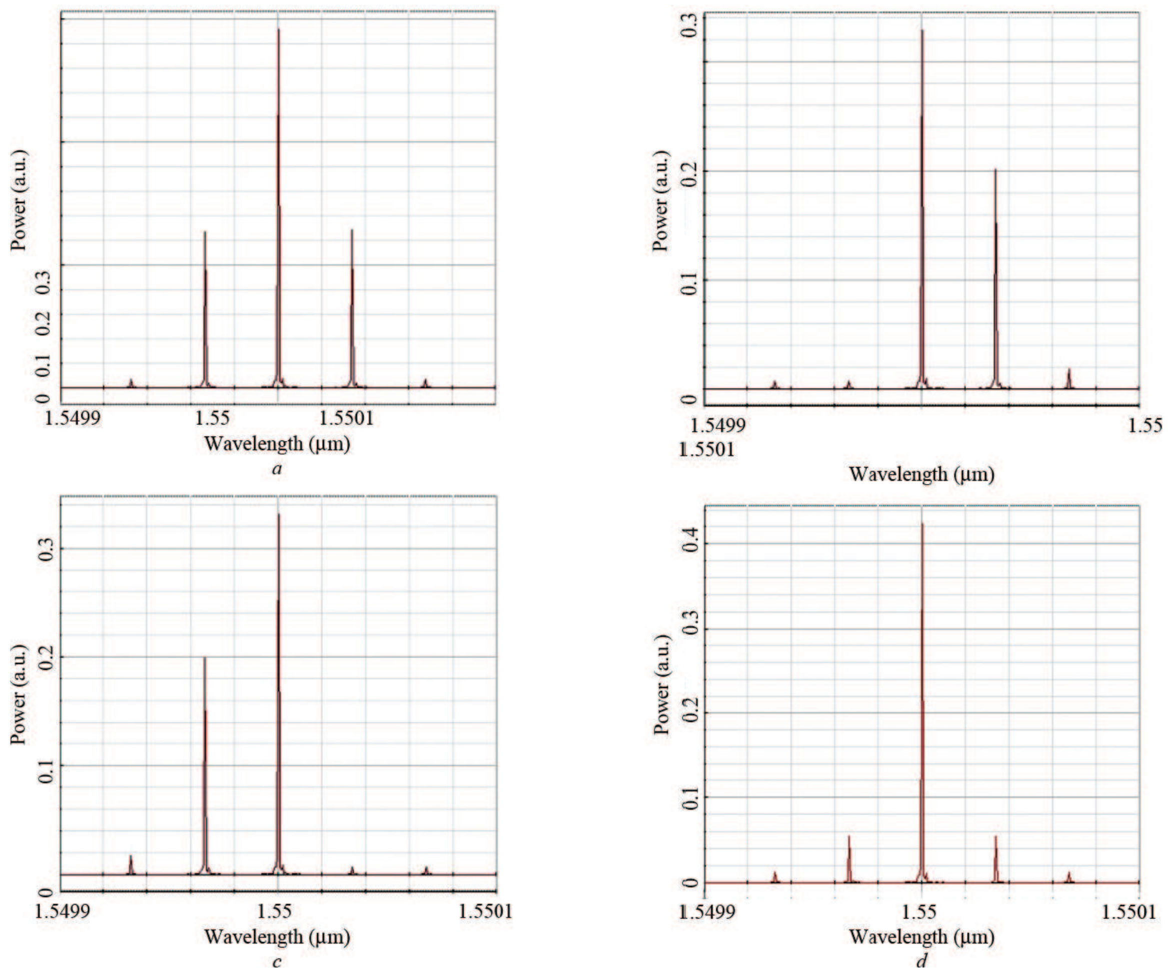

Figure 6. Constructive $\Delta\Phi = 0$ (a) and destructive $\Delta\Phi = \pi/2$ (b), $\Delta\Phi = 3\pi/2$ (c), $\Delta\Phi = \pi$ (d) interferences on the output of Bob's PM, when phase of Alice's AM $\Phi_A = 0$.

and B92 one. Taking into account that the definition of truth in these statements is not the aim of our chapter, let us consider some results of practical experiments for AM-AM schemes based on acoustic-optical modulators [16], which show us second attempt to implement QKD system without re-modulation.

2.4. Acousto-optic modulation for AM-AM schemes

There is a nonelectro-optical solution of AM-AM scheme based on acousto-optic modulation on Alice's side as well as on Bob's side [16].

In the case of Bragg diffraction, all orders of diffracted radiation except the first become negligibly small, and the frequency offset depends from the direction of laser radiation and sound wave propagation.

For BB84 protocol, two bases are set:

$$\begin{cases} |+;\ 1\rangle = |1\rangle_{\omega_0+\Omega} \\ |-;\ 1\rangle = |1\rangle_{\omega_0-\Omega} \end{cases}$$
$$\begin{cases} |+;\ 2\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+\Omega} + \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-\Omega} \\ |-;\ 2\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+\Omega} - \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-\Omega} \end{cases}. \quad (5)$$

The first pair of states $|+;1\rangle$ and $|-;1\rangle$ can be identified without re-modulation, using the filter block consisted from FBG or AWG, tuned on the frequencies $\omega_0 \pm \Omega$ or one of them, similar to the filtering implemented in the second variant of PM-PM scheme [14].

The second pair of states $|+;2\rangle$ and $|-;2\rangle$ is transmitted with the help of modulation on Alice's side. If we use filters without re-modulation on Bob's side, the error can occur, because both photosensors with $\omega_0 \pm \Omega$ filters will trigger. The given states are determined uniquely if re-modulation is used.

Replacing status $|+;1\rangle$ and $|+;2\rangle$ to '1' and $|+;1\rangle$ and $|-;1\rangle$ to '0', Alice and Bob will get an exact match of the sent qubits. This ensures an exact match of QKD protocol to BB84.

Certain difficulty, associated with spatial alignment of used devices as on Alice's so and Bob's sides, characterizes using of acousto-optic modulators in QKD system implementation with frequency encoding. Search for ways to implement bases, described in (5), with the help of electro-optic modulation, led us to use Il'in-Morozov's method [24, 25] for the photon carrier modulation transform.

Il'in-Morozov's method belongs to the methods with full or partial suppression of optical carrier. The theoretical justification for this application and synthesized conjugated bases is obtained by amplitude-phase modulation according to Il'in-Morozov's method we consider in the next section.

3. Tandem AMPM-PMAM structure of QKD system with frequency encoding

3.1. Serial and parallel microwave photonic AMPM one port units

The general model shown in **Figure 7** for a single-port parallel system, where either intensity or phase modulation (or both simultaneously in parallel) can be applied, can represent all the former examples from the point of view of traditional simple microwave photonic (MWP) links.

The impact of all intermediate optical components of quantum channel placed between the electro-optical (EO) and the optoelectronic (OE) conversion stages can be united into an optical transfer function $H(\omega)$ (in our case, its FBG as filter for carrier, fiber of channel with losses and so on). Authors of [26], in order to classify these systems, use the term 'filtered MWP links' (FMWPL).

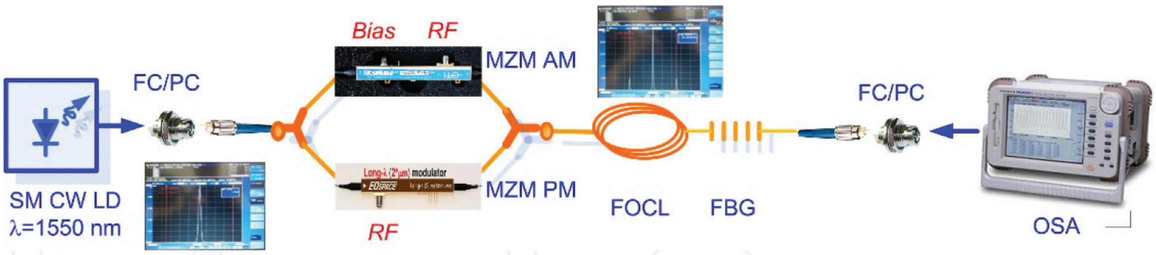

Figure 7. Schematic representation of a general parallel single-port filtered MWP link [25].

The features of FMWPL are evaluated in terms of figures of merit set: the radiofrequency link gain, the noise figure and the spurious free dynamic range [27]. These metrics have been computed for a wide variety of configurations in [26].

In principle, the interest was focused on intensity-modulated direct detection (IMDD) point-to-point links with direct or external modulation, and models were developed detailed description of the effects of the electronic biasing circuits and impedance matching networks [27]. Paper [28] reciprocally considers the inclusion of an arbitrary optical filter, acting as an FM discriminator, for the particular case of directly modulated FMDD links if synchronizing channel will change frequency.

For the AMPM feature analysis, classical generalized scheme of single-port FMWPL was converted from parallel to serial circuit type (**Figure 8**) in order to implement Il'in-Morozov's method.

On the basis of studies carried out in this section, the feasibility of AMPM scheme realized on the amplitude, and phase MZM was theoretically demonstrated. We carried out equations for the calculation of the AMPM scheme output spectrum [29]. The spectrum consists mainly from two components, if phase of PM triggered on π in the minimum of envelope of amplitude-modulated carrier. The difference frequency is equal to modulating one in synchronizing channel.

Figure 9 shows the spectrums of the original quasi-harmonic oscillations of the amplitude-modulated signals structure (**Figure 9a**) and the two frequency structure with partly suppressed carrier obtained by MZM AM in 'zero' point (**Figure 9b**) and fully suppressed carrier

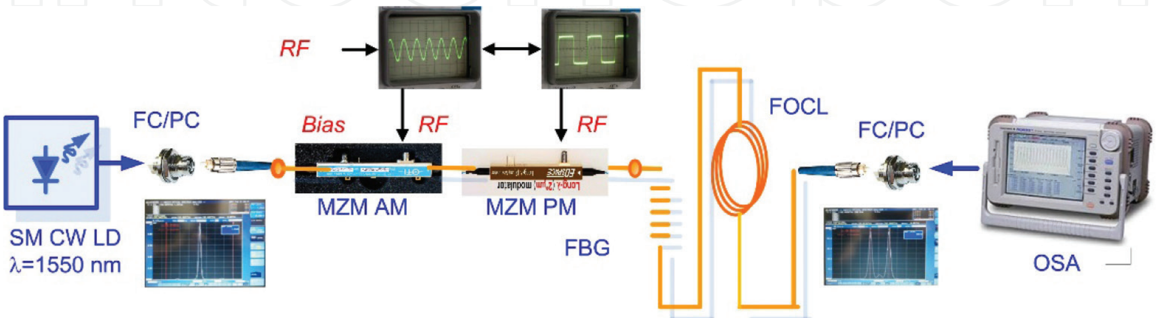

Figure 8. Schematic representation of a general serial single-port filtered MWP link [28].

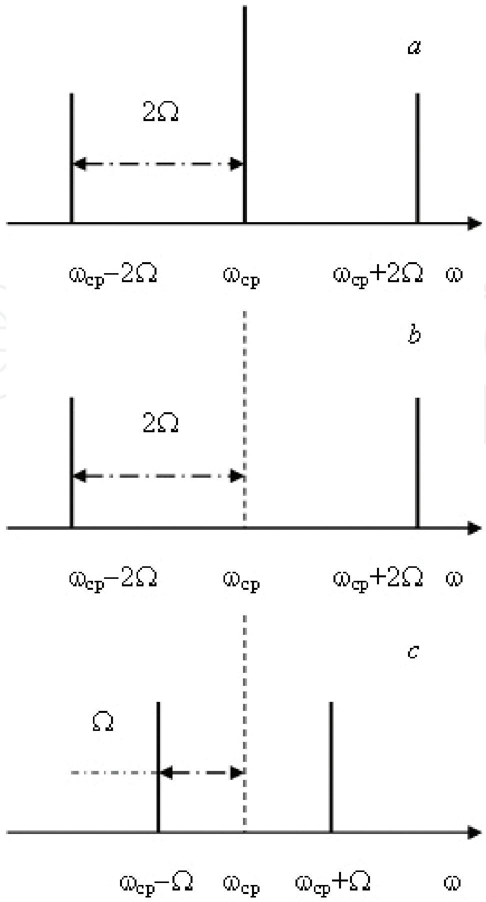

Figure 9. The spectrums of initial AM radiation (a) and output ones from amplitude MZM (b), operating in 'zero' point, and AMPM system based on tandem amplitude and phase MZM (c).

by AMPM method (**Figure 9c**). If these oscillations expose the amplitude detector, the frequency of their envelopes will be different in two times.

As seen from **Figure 9**, the difference frequency between two frequency components of radiation is equal to the frequency 2 Ω or modulating waveforms. Components of higher harmonics can be ignored because of the smallness of their amplitudes.

We obtained the doubled narrowing of the difference frequency if compared to classical schemes of modulation applicable in practice and using a single-amplitude MZM, operating in the 'zero' point of the modulation characteristics [29].

3.2. Tandem AMPM-PMAM scheme

Functional scheme of tandem AMPM-PMAM QKD system with frequency encoding is presented in **Figure 10**.

Alice's side—transmitter, based on a transmitting part of a single-port serial type FMWPL, consists of low-power single mode (frequency) continuous wave laser diode (SM CW LD)—simulator of single photons with carrier frequency ω, amplitude Mach-Zehnder modulator (MZM 1AM) and phase Mach-Zehnder modulator (MZM 1PM).

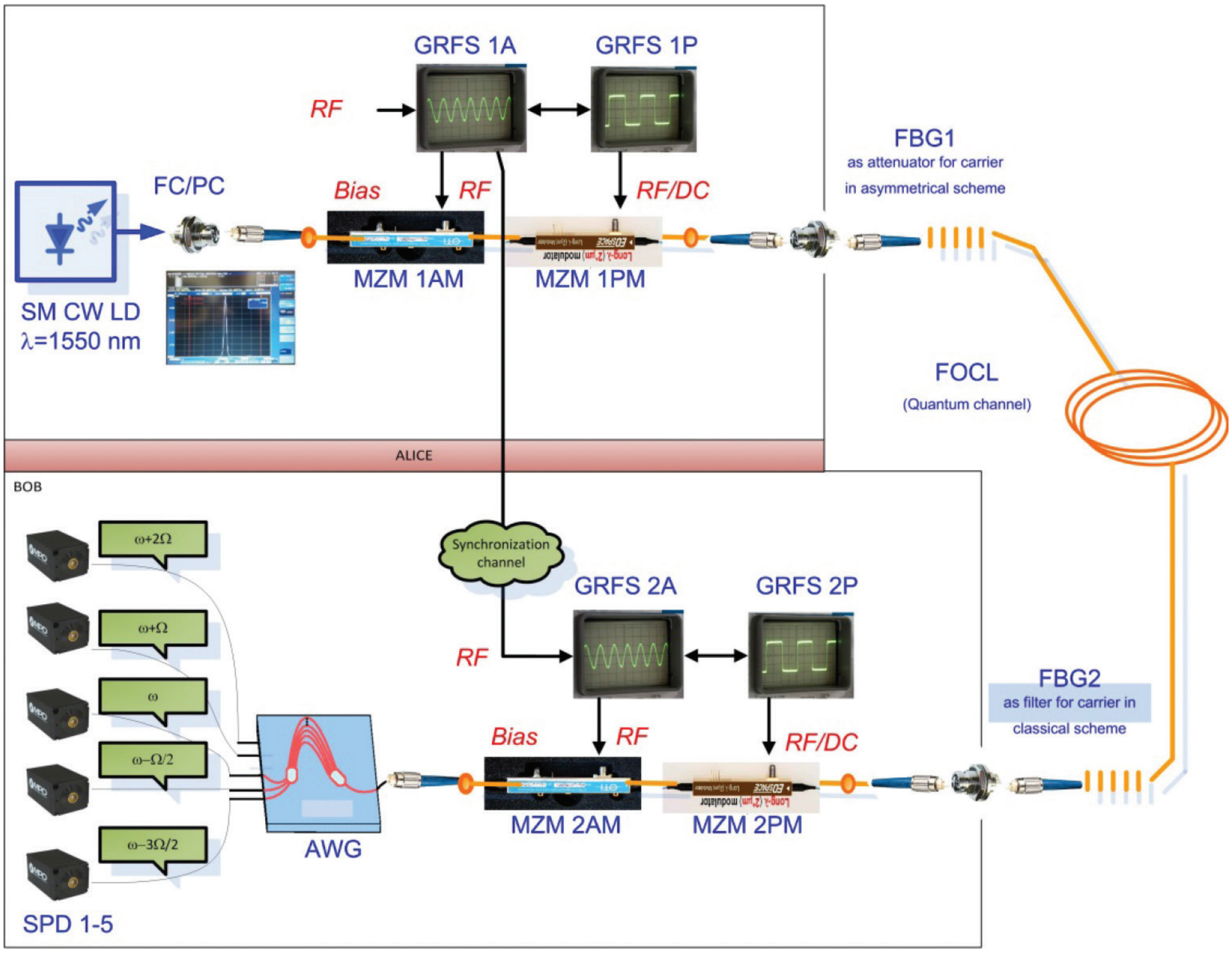

Figure 10. Functional scheme of AMPM-PMAM QKD system with frequency encoding.

Orthogonal polarization controllers, allowing carrier amplitude modulation and controlling the modulator transmission index, when no modulation is needed, can be installed at MZM 1AM input and output. Amplitude and phase modulation parameters are controlled by generator of radiofrequency signals GRFS 1 (A or P) with angular frequency $\Omega \ll \omega$ and selectable phase Φ of a pair of conjugate bases $0;\pi$ or $\pi/2;3\pi/2$. A source of DC bias serves to select the operating point of the MZM 1 AM modulation characteristics, providing amplitude modulation at zero, quarter-wave and half-wave operating points by submitting to its corresponding 0, $U\pi/2$ or $U\pi$ input voltage, where $U\pi$—half-wave voltage of modulator. The modulation factors of MZM 1AM and MZM 1PM are selected to ensure their operation in the linear range. Thus, the radiation at the output port in classical schemes will be limited by components in the range from ω to $\omega \pm 2\ \Omega$, and the filter on FBG2 additionally selects ω [15]. The setting of FMWPL provides the opportunity to work with and without amplitude and phase modulation of photons. In latter, the DC voltage put in MZM 1PM for its opening.

Bob's side—receiver, based on receiving part of single-port serial FMWPL, consists of MZM 2PM, MZM 2AM, filter units (FBG1/AWG) and the block of SPD for emission registration at frequencies ω, $\omega \pm \Omega$ and $\omega \pm 2\ \Omega$ (for classical schemes, half part of SPD is shown) and ω, $\omega \pm \Omega/2$, and $\omega \pm 3\ \Omega/2$ (for advanced schemes, half part of SPD is shown). A more detailed filter pack description will be given below when discussing the variants of QKD scheme implementation.

Special synchronization channel from Alice to Bob [15] serves to transmit information about a modulating signal at frequency Ω, which allows to use on Bob's side radiofrequency modulating signal with the same frequency as Alice and control it with local GRFS 2 (A or P). MZM 2AM and MZM 2PM Bob's modulators are controlled analogously to Alice's ones.

3.3. AMPM-PMAM system implementation for classical QKD schemes

General view of the AMPM-PMAM experimental setup is presented in **Figure 11**.

For amplitude modulation, an amplitude modulator JDSU APE microwave analog is used with operating frequencies band over 4.2 GHz and a half-wave voltage of 3.3 V. The size of the modulator reaches a length of 120 mm and a width of 15 mm. Irregularity of frequency response in the range of 0.13–20 GHz is 7 dB. For the phase modulation, the phase modulator JDSU APE with the working frequency band above 10 GHz was used. The sizes of phase modulator are close to the dimensions of the intensity modulator. It does not require the input (bias) of the operating point.

The range of wavelengths includes an operating wavelength of 1550 nm. Losses of both types of modulators are about 3 dB. Maximum input power is up to 200 mW. As far as the small signal approaches, we are interested in the power of 1 mW, the use of which does not result in nonlinear effects in an optical fiber such as stimulated Mandelstam-Brillouin or Raman scattering [20].

Let us consider the modeling implementation of PM-PM scheme. Laser radiation from the Alice's side, as the source of which the laser optical spectrum analyzer was used, allowing realization of low-power laser analogue, arrived on the MZM 1AM in an open state and a phase modulator MZM 1PM. Further on across the bay of optical fiber SMF-28 of 2 km length, the radiation was received on the Bob's side, where it was re-modulated within the MZM 2PM (MZM 2AM was open) and recorded in the optical spectrum analyzer and photodetector

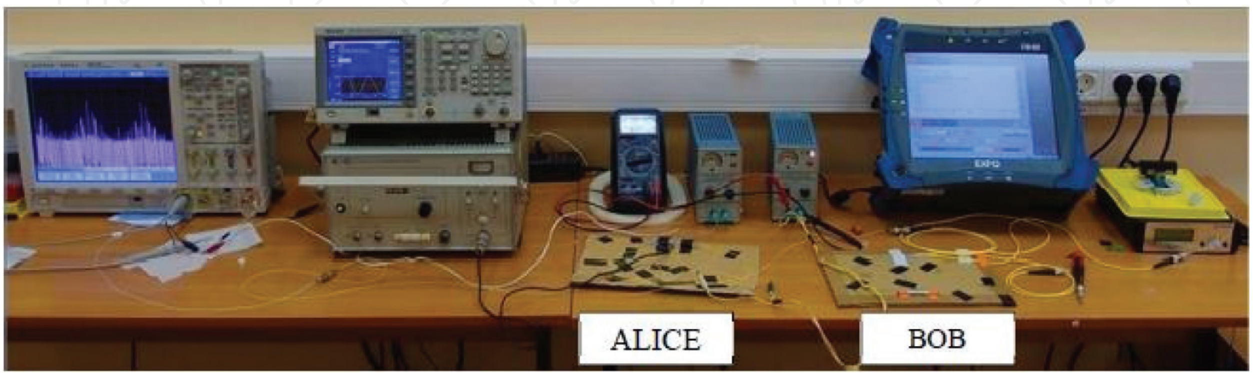

Figure 11. General view of the AMPM-PMAM experimental setup.

devices LSIPD-A75-FA, using filters based on FBG2. The modulation frequency was 4.2 GHz. **Figure 12** shows signal spectrograms in destructive and constructive interference on the lateral frequencies $\omega \pm \Omega$.

Thus, it was shown that AMPM-PMAM system could be implemented, for example, as PM-PM QKD scheme with frequency encoding based on classical approaches. It should be highlighted that in classical approaches transfer efficiency $P(\omega \rightarrow \omega \pm \Omega)$ at low modulation coefficients does not reach high values. The main energy is concentrated at the carrier frequency, and the proportion of energy of the side components is very small. Then, in order to compensate NPM, we have to extract carrier, so the efficiency of photon registration on subcarriers is very small also.

This factor gave us additional arguments to implement modulation transformation of photon carrier based on Il'in-Morozov's method [24, 25]. The procedures are concluded in amplitude modulation and phase commutation (PC) of optical carrier with its suppression and full energy transfer in subcarriers.

Let us evaluate the possibility of perspective AMPC-PCAM system implementation in two variants. First is symmetrical structure with amplitude modulation and phase commutation at the Alice's side and amplitude re-modulation and phase re-commutation on the Bob's side. Second is variant, in which the asymmetric structure of the QKD with amplitude modulation and phase commutation on the Alice's side and only passive filtering based on the FBG1/AWG on the side of Bob are implemented.

3.4. Estimation of possibility AMPC-PCAM scheme implementation

The operation of AMPC-PCAM QKD system with frequency encoding is based on amplitude-phase modulation conversion of the photon carrier realized with the procedures described by Il'in-Morozov's method and its implementations on one or two modulators [29, 30]. Variants of constructive AM interference are shown in **Figure 13** in the case of constructive PC on Alice and Bob sides.

a *b*

Figure 12. The spectrogram of the signal in destructive (a) and constructive (b) interference on the lateral frequencies $\omega \pm \Omega$ in PM-PM scheme implementation.

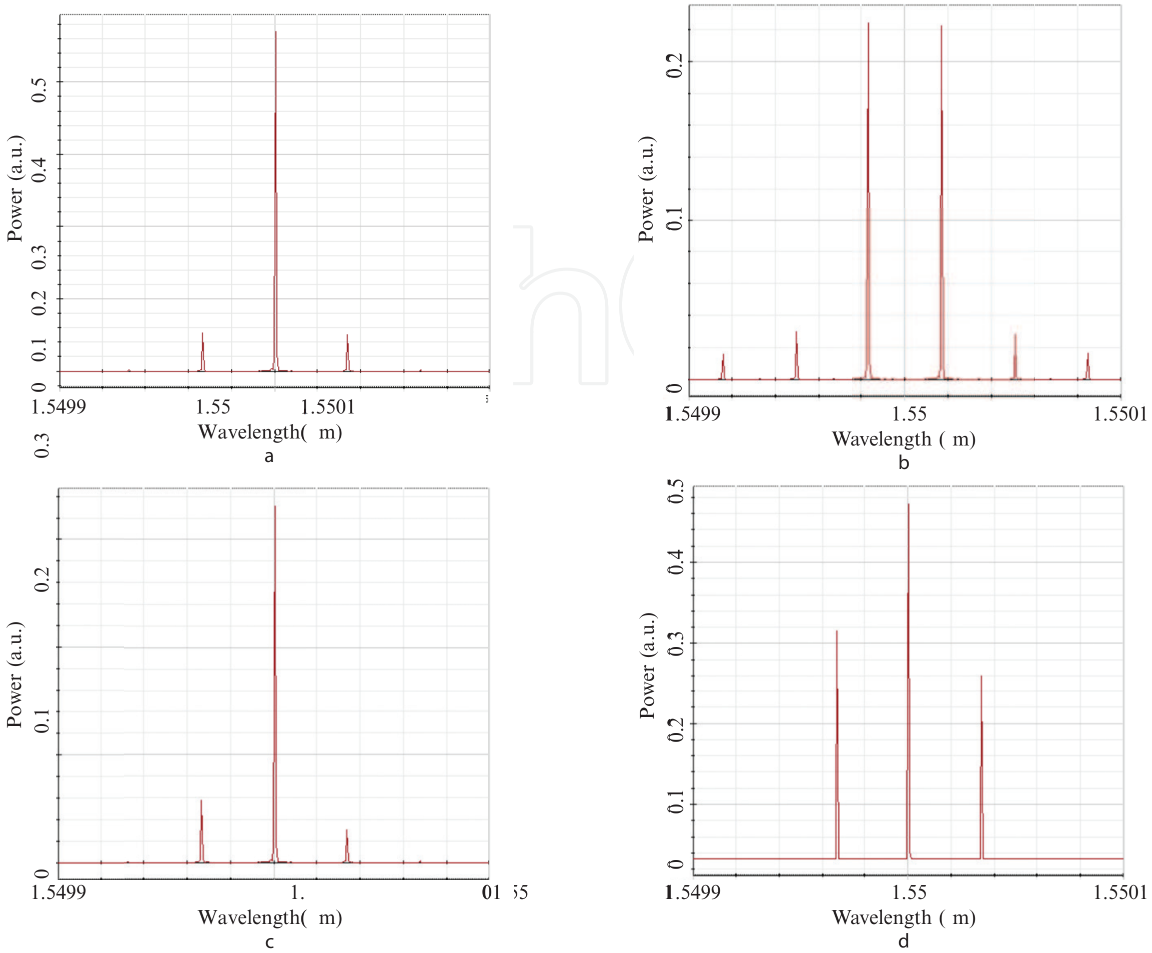

Figure 13. Variants of constructive interference with the coincidence of the parameters AM and PC on the side of Alice and Bob: the results of AM (a) and PC (b) at the output of modulators on the side of Alice; the results of PC (c) and AM (d) at the output of modulators on the side of Bob.

To simulate the scheme and carry out the project evaluations, the modeling principles of single-port modulation radio photon of serial link type proposed by us in [29, 31, 32] and photonic simulation of electro-optic modulators [33] were used.

The implementation of Il'in-Morozov's method for the modulation conversion $P(\omega \rightarrow \omega \pm n\Omega)$, where n is the number of subcarriers, will provide:

1. high-efficiency optical carrier transfer into subcarrier left and right components (up to 0.6–0.8 amplitude for each of them), high level of spectral purity under the optimal conversion parameters (only first or additionally third number subcarriers are existing);
2. NPM decreasing (carrier is absent), to exclude spectrum filter, which separates carrier and sidebands, to increase signal-to-noise ratio, because we can register photon by envelope amplitude on difference frequency Ω, which lies in SPD spectrum region with minimum level of noises;
3. synthesis of whole number subcarriers ($n \geq 1$) and fractional ones ($n/2$, for $n \geq 1$) that will improve the cryptographic protection level of the communication system, in case of Eve discoveries the frequency of synchronization channel;

4. implementation of an asymmetric system with a totally passive data filtering sent by Alice, on the of Bob's side without re-modulation or re-commutation.

Let us make the first three statements plain.

Figure 14 shows the output spectrum of AMPC procedure, which can be described as two-frequency symmetrical radiation with fully suppressed carrier and fractional harmonics nΩ/2 (here n = 1 for **Figure 14a** and n = 2 for **Figure 14b**).

In this case, we can decrease NPM (carrier is absent) in FOLC and increase signal-to-noise ratio, because we can register photon by envelope amplitude on difference frequency Ω, which lies in SPD spectrum region with minimum level of noises. The point about separation filter necessity is a question.

Thus, if we realize full re-modulation of Alice's phases in phases on Bob's side, we get spectrum, as shown in **Figure 12b**, after Bob's PM, and, as shown in **Figure 12a**, after Bob's AM. Therefore, the carrier is present, but only in receiver, not in quantum channel, and its influence on channel characteristics is minimized.

Let us clarify the last from above four statements.

Analysis shows that we can realize classical symmetrical QKD scheme with modulation and re-modulation. To do this, we are going to select the two bases for frequency-encoding the photon states in AMPC of asymmetrical type without re-modulation/re-commutation and explain the order they are received.

$$\begin{cases} |+;\ 1\rangle = |1\rangle_{\omega_0} \\ |-;\ 1\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+\Omega} - \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-\Omega} \end{cases}$$
$$\begin{cases} |+;\ 2\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+\Omega/2} - \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-\Omega/2} \\ |-;\ 2\rangle = \frac{1}{\sqrt{2}}|1\rangle_{\omega_0+3\Omega/2} - \frac{1}{\sqrt{2}}|1\rangle_{\omega_0-3\Omega/2} \end{cases} \tag{6}$$

The state $|+;1\rangle$ is the unmodulated photon transmitted from SM CW LD, through the open Alice's modulators. The state $|-;1\rangle$ is amplitude-modulated photon (frequency of modulation is Ω; 'zero' operating point of MZM 1 AM; absence of phase commutation). The state $|+;2\rangle$

a *b*

Figure 14. The output spectrum of AMPC procedure for propagation in FOLC: frequency encoding of second $|-;\ 1\rangle$ and third $|+;\ 2\rangle$ photon states is shown.

is full tandem amplitude-modulated and phase-commutated photon (quadrature operating point of MZM 1 AM; amplitude modulation coefficient m = 0.59; phase commutation 0/π with frequency Ω/2 in MZM 1 PM). The state |−;2⟩ is described by lateral components obtained at the same parameters of amplitude modulation, but MZM 1 PM had phase commutation 0/π with frequency 3 Ω/2. The parameter control of the amplitude modulation and phase commutation is performed by GRFS 1A and 1P with a corresponding change in functions.

Frequency encoding of second |−; 1⟩ and third |+; 2⟩ photon states is presented in **Figure 14b** and **a**, respectively. As can be seen from last paragraph and in **Figure 14**, all four photons states can be passively allocated through a system of filters tuned respectively to frequencies $\omega_0 \rightarrow |+;1\rangle$, $\omega_0 \pm \Omega/2 \rightarrow |+;2\rangle$, $\omega_0 \pm \Omega \rightarrow |-;1\rangle$, $\omega_0 \pm 3\,\Omega/2 \rightarrow |-;2\rangle$. Thus, AMPC-FBG/AWG asymmetric system can be constructed as shown in **Figure 10**, but without modulators on Bob's side.

4. Conclusion

The implementation of tandem AMPM(C)-PM(C)AM schemes of symmetric and asymmetric types and analysis of their advantages and disadvantages will be considered in subsequent publications and are the goal of future work. In this chapter, we demonstrate only the opportunity of its creation, the theoretical justification of their bases and preliminary evaluation of its characteristics. We show that tandem AMPM(C)-PM(C)AM QKD system, based on microwave photonic principles transferred to photon level, can be used as universal frequency encoding system.

The application of such type QKD system will allow us to use multiple levels of cryptographic security, including modulation, commutation schemes and protocol choices, so and choice from re-modulation (re-commutation) and passive detection procedures. The two-time increase of electro-optic modulator number will undoubtedly increase the cost of the system. However, this increasing can be minimized by its universality, and therefore, the expanded functionality, in comparison with each of the known and described by us earlier systems with frequency encoding.

In addition, the high spectral purity and stability of photon tandem modulation based on Il'in-Morozov's method should be highlighted. Qualitatively, we presented the advantages of carrier excluding from quantum communication channel. First, it was shown that effects of nonlinear phase modulation are decreased. Second, in this case, the security condition is stricter to a level of single photon transmission. Third, the signal-to-noise ratio of the system is increased and leads to a significant decrease in the number of errors in the given channel.

For the first time, it was shown the possibility of constructing a nonclassic asymmetric structure using modulators only on the Alice's side and passive filters based on fiber Bragg or arrayed waveguide gratings on the Bob's side.

Therefore, the QKD technology with frequency coding, based on the modulation conversion of an optical carrier with its complete or partial suppressing in the case of tandem amplitude modulation and phase modulation/commutation, is the promising tool for designing perspective quantum communication channels.

Acknowledgements

Ministry of Education and Science of Russian Federation supported this work: state R&D task to Kazan National Research Technical University n.a. A.N. Tupolev—Kazan Aviation Institute ("Asymmetry", base task no. 8.6872.2017/8.9).

Author details

Oleg G. Morozov[1]*, Airat J. Sakhabutdinov[1], Gennady A. Morozov[1] and Il'daris M. Gabdulkhakov[2]

*Address all correspondence to: microoil@mail.ru

1 Kazan National Research Technical University n.a. A.N. Tupolev-KAI, Kazan, Republic of Tatarstan, Russia

2 PJSC «Tattelecom», Kazan, Russia

References

[1] Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Reviews of Modern Physics. 2009;**81**:1301-1310. DOI: 10.1103/RevModPhys.81.1301

[2] Muller A, Breguet J, Gisin N. Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km. Europhysics Letters. 1993;**23**:383-388. DOI: 10.1209/0295-5075/23/6/001

[3] Zbinden H, Gautier JD, Gisin N, Huttner B, Muller A, Tittel W. Interferometry with Faraday mirrors for quantum cryptography. Electronics Letters. 1997;**33**:586-588. DOI: 10.1049/el:19970427

[4] Inoue K, Waks E, Yamamoto Y. Differential phase shift quantum key distribution. Physical Review Letters. 2002;**89**:037902. DOI: 10.1103/PhysRevLett.89.037902

[5] Duraffourg L, Merolla J-M, Goedgebuer J-P, Mazurenko Y, Rhodes WT. Compact transmission system using single-sideband modulation of light for quantum cryptography. Optics Letters. 2001;**26**(18):1427-1429. DOI: 10.1364/OL.26.001427

[6] Dixon AR, Yuan ZL, Dynes JF, Sharpe AW, Shields AJ. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. Optics Express. 2008;**16**:18790-18799. DOI: 10.1364/OE.16.018790

[7] Sadeev TS, Morozov OG. Investigation and analysis of electro-optical devices in implementation of microwave photonic filters. Proceedings of SPIE. 2012;**8410**:841007. DOI: 10.1117/12.923121

[8] Mora J, Ruiz-Alba A, Amaya W, Garcia- Muñoz V, Martinez A, Capmany J. Microwave photonic filtering scheme for BB84 subcarrier multiplexed quantum key distribution. IEEE Topical Meeting on Microwave Photonics. 2010:286-289. DOI: 10.1109/MWP.2010.5664176

[9] Aybatov DL, Morozov OG, Sadeev TS. Dual port MZM based optical comb generator for all optical microwave photonic devices. Proceedings of. SPIE. 2011;**7992**:799202. DOI: 10.1117/12.887273

[10] Merolla J-M, Mazurenko Y, Goedgebuer J-P, Duraffourg L, Porte H, Rhodes WT. Quantum cryptographic device using single-photon phase modulation. Physical Review. 1999;**A60**(3):1899-1905. DOI: 10.1103/PhysRevA.60.1899

[11] Bennett CH. Quantum cryptography using any two nonorthogonal states. Physical Review Letters. 1992;**68**:3121-3124. DOI: 10.1103/PhysRevLett.68.3121

[12] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing. 1984. pp. 175-179. DOI:10.1016/j.tcs.2014.05.025

[13] Xavier GB, Weid JP. Modulation schemes for frequency coded quantum key distribution. Electronics Letters. 2005;**41**(10):607-608. DOI: 10.1049/el:20050466

[14] Bloch M, McLaughin SW, Merolla J-M, Patois F. Frequency-coded quantum key distribution. Optics Letters. 2007;**32**(3):301-303. DOI: 10.1364/OL.32.000301

[15] Gleim AV, Egorov VI, Nazarov YV, Smirnov SV, Chistyakov VV, Bannik OI, et al. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. Optics Express. 2016;**24**(3):2619-2633. DOI: 10.1364/OE.24.002619

[16] Zang T, Yin Z-Q, Han Z-F, Guo G-C. A frequency-coded quantum key distribution scheme. Optics Communications. 2008;**281**:4800-4802. DOI: 10.1016/j.optcom.2008.06.009

[17] Smith RA, Reddy DV, Vitullo DL, Raymer MG. Verification of a heralded, two-photon fock state with a gang of detectors. Frontiers in Optics. 2015;**FTu3G**:FTu3G.2. DOI: 10.1364/FIO.2015.FTu3G.2

[18] Gaidash AA, Egorov VI, Gleim AV. Revealing of photon-number splitting attack on quantum key distribution system by photon-number resolving devices. Journal of Physics: Conference Series. 2016;**735**:012072. DOI: 10.1088/1742-6596/735/1/012072

[19] Morozov OG, Il'in GI, Morozov GA, Nureev II, Misbakhov RS. External amplitude-phase modulation of laser radiation for generation of microwave frequency carriers and optical poly-harmonic signals: An overview. Proceedings of SPIE. 2015;**9807**:980711. DOI: 10.1117/12.2231948

[20] Morozov OG, Gabdulkhakov IM, Morozov GA, Zagrieva AR, Sarvarova LM. Frequency-coded quantum key distribution using amplitude-phase modulation. Proceedings of SPIE. 2015;**9807**:98071F. DOI: 10.1117/12.2230665

[21] Ruiz-Alba A, Calvo D, Garcia-Munoz V, Martinez A, Amaya W, Rozo JG, Mora J, Capmany J. Practical quantum key distribution based on BB84 protocol. Waves. 2011;**3**:4-14. URL: https://riunet.upv.es/handle/10251/53967

[22] Mérolla J-M, Mazurenko Y, Goedgebuer J-P, Porte H, Rhodes WT. Phase-modulation transmission system for quantum cryptography. Optics Letters. 1999;**24**:104-106. DOI: 10. 1364/OL.24.000104

[23] Kumar KP. Optical modulation schemes for frequency-coded quantum key distribution. IEEE National Conference on Communications; Chennai, India; 29-31 Jan. 2010; 2010. pp. 1-5. DOI: 10.1109/NCC.2010.5430155

[24] Morozov OG, Aybatov DL. Spectrum conversion investigation in lithium niobate Mach-Zehnder modulator. Proceedings of SPIE. 2010;**7523**:75230D. DOI: 10.1117/12.854957

[25] Morozov OG. RZ, CS-RZ and soliton generation for access networks applications: Problems and variants of decisions. Proceedings of SPIE. 2012;**8410**:84100P. DOI: 10.1117/12. 923115

[26] Gasulla I, Capmany J. Analytical model and figures of merit for filtered microwave photonic links. Optics Express. 2011;**19**(20):19758-19774. DOI: 10.1364/OE.19.019758

[27] Cox CH III. Analog Photonic Links: Theory and Practice. Cambridge: Cambridge University Press; 2004. 289 pp

[28] Wyrwas JM, Wu MC. Dynamic range of frequency modulated direct-detection analog fiber optic links. Journal of Lightwave Technology. 2009;**27**(24):5552-5562. DOI: 10.1109/JLT.2009.2031986

[29] Il'In GI, Morozov OG, Il'In AG. Theory of symmetrical two-frequency signals and key aspects of its application. Proceedings of SPIE. 2014;**9156**:91560M. DOI: 10.1117/12.2054753

[30] Petoukhov VM, Akhtiamov RA, Morozov OG, Il'in GI, Pol'ski YE. Two-frequency IR CW LFM lidar for remote sensing of hydrocarbons and gas vapor. Proceedings of SPIE. 1997;**3122**:339-346. DOI: 10.1117/12.292705

[31] Morozov GA, Morozov GA, Il'in GI, Il'in AG. Instantaneous frequency measurements of microwave signal with serial amplitude-phase modulation conversion of optical carrier. Proceedings of SPIE. 2014;**9533**:95330Q. DOI: 10.1117/12.2181435

[32] Morozov OG, Talipov AA, Nurgazizov MR, Denisenko PE, Vasilets AA. Instantaneous frequency measurement of microwave signals in optical range using «frequency-amplitude» conversion in the π-phase shifted fibre Bragg grating. Proceedings of SPIE. 2014;**9136**:91361B. DOI: 10.1117/12.2051126

[33] Capmany J, Fernandez-Pousa CR. Quantum modelling of electro-optic modulators. Laser & Photonics Reviews. 2011;**5**(6):750-772. DOI: 10.1002/lpor.201000038