Chapter 15
Modeling of Quantum Key Distribution System for Secure Information Transfer

K. E. Rumyantsev
Taganrog Institute of Technology, Russia

D. M. Golubchikov
Southern Federal University, Russia

ABSTRACT

This chapter is an analysis of commercial quantum key distribution systems. Upon analysis, the generalized structure of QKDS with phase coding of a photon state is presented. The structure includes modules that immediately participate in the task of distribution and processing of quantum states. Phases of key sequence productions are studied. Expressions that allow the estimation of physical characteristics of optoelectronic components, as well as information processing algorithms impact to rate of key sequence production, are formed. Information security infrastructure can be utilized, for instance, to formulate requirements to maximize tolerable error level in quantum channel with a given rate of key sequence production.

1. QUANTUM KEY DISTRIBUTION

Quantum Cryptography (QC) is a part of quantum computing that examines the methods of information security by using a quantum carrier (Kilin, Nizovtsev, & Horoshko, 2007; Scarani, 2006; Bouwmeester, Ekert, & Zeilinger, 2000; Gisin, Ribordy, Tittel, & Zbinden, 2002; Rumyantsev, 2010). QC proposes a new method of generating random private keys for quantum communication line users. Its privacy and eavesdropping protection is based upon quantum principles instead of Classical Cryptography (CC) methods (Kotenko, & Rumiantsev, 2009; Mao, 2003; Smart, 2004; Singh, 2000; Brassard, 2007) used now and based upon mathematical law, which can be cracked.

Quantum key distribution (QKD) is a technology based upon quantum principles for generation random bit strings, which could be used as privacy keys, between two remote users.

The hardware is the realization of the process of sending and receiving data, for example, a single photon used in a fiber link. An eavesdropping changes the influential parameters of the physical objects, which used as data carrier.

DOI: 10.4018/978-1-4666-2208-1.ch015

QC is permitted to generate random keys for two users, which has no shared confidential data initially, and that key will be unknown for eavesdroppers.

The quantum physics law starts influence when data transmission uses signals containing average photon number less than 0.1 instead of the signals containing many thousands of photon. The nature of QC privacy is based on this law in conjunction with CC procedures. One of these laws is Heisenberg's uncertainty principle, and in accordance with it, a trial measurement of a quantum state changes to an initial state

The main gain of QC is that eavesdropping will be known to legal users, besides of absolute privacy.

Indivisible quantum and entanglement are very specific features of quantum physics (Kilin, Nizovtsev, & Horoshko, 2007; Scarani, 2006; Bouwmeester, Ekert, & Zeilinger, 2000; Gisin, Ribordy, Tittel, & Zbinden, 2002). QC uses both of these features.

The necessity in symmetric encryption systems arises in process of data transmission for reducing economic and social risks.

1.1. Symmetric Ciphers Require a Single Key to Encrypt and Decrypt

The quantum channel and open data link for checking of eavesdropping are the main components of QKD. The quantum channel and open data link connect legal users. The term of quantum channel mean that data carrier is a quantum in it.

QKD starts from transmission quantum between legal users. A matching of keys is realized through open data link. The eavesdropper has access to open data link, but it could not change information in it.

The sender encode the message into bit string (a_m is binary number) by using a random key a_k in symmetric encryption systems. Each bit of message add to same bit of key to make ciphertext as $a_t = a_m \oplus a_k$. Here $\oplus$ is congruence addition by 2 without carry (XOR). A receiver decode ciphertext by subtract key from it as $a_t\text{-}a_k = a_m \oplus a_k - a_k = a_m$. The bits of the ciphertext are random as the bits of the keys, so they are not contain any information. That cryptosystems are secure in accordance with information theory.

The system is secure absolutely on condition that the sender Alice and receiver Bob have shared private key, which has the same length as the message, and the key is used only once for encode.

The eavesdropper Eva can record all ciphertexts in order to create an image of plaintexts and the key if the key is used more than once.

If Eva has two ciphertexts a_{t1} and a_{t2} which encoded by single key a_k then she could add both ciphertexts and get a sum of plaintexts:

$$a_{t1} \oplus a_{t2} = a_{m1} \oplus a_k \oplus a_{m2} \oplus a_k$$
$$= a_{m1} \oplus a_{m2} \oplus a_k \oplus a_k = a_{m1} \oplus a_{m2}.$$

The symmetric encryption systems *require for all users shared private key which* has the same length as the message and can be used only once.

The main idea of QC is trusted key distribution between users never met each other.

QC proposes a perspective way based on physical principles to solve the key distribution problem.

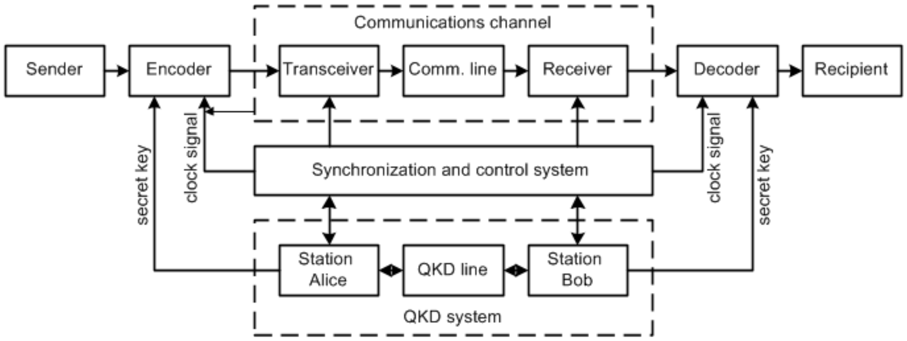
Statement 1: An unknown quantum state could not be cloned.

Statement 2: Information from the nonorthogonal quantum states could not be obtained without distortion it.

Statement 3: Any measurement performed by an eavesdropper leads to changes quantum state of data carrier.

Hardware-software solution for confidential data transmission with QKD system and synchronizing system is shown of Figure 1.

Figure 1. The structure of hardware-software complex for confidential data transmission



On Figure 1 data source generate digital signals correspond to specified type of telecommunication data. The encoder realizes the signal characteristics encode process for protection against eavesdropping. The communications channel consists of transceiver, receiver and communication link, which used for transmission encrypted data. The communications channel creates the route of data transfer from sender to recipient (Kotenko, & Rumiantsev, 2009).

In a symmetric cryptosystem sender and recipient of data using the same secret key, which requires periodic updating. The complex (Figure 1) uses the QKD system, which consists of two stations, called Alice and Bob, to perform the function of key updating.

Stations have control inputs and outputs for synchronizing its operation, monitoring QKD system parameters and control the communication channel.

Generation of secret keys is implemented through the communication line, where the single photons transmitted. QKD systems use three types of coding of quantum states: the polarization encoding, phase encoding, and encoding by time shifts. QKD line can be a free space or an Optical Fiber (OF). Commercial QKD systems using fiber-optic communication lines (FOL).

Each station generates shared secret keys and distributes it between the legitimate users. These keys use for encryption data of sender and decryption data for the recipient.

Synchronization system provides synchronization of spatially separated transmitter and receiver in the communication channel, Alice and Bob stations in the QKD (Quantum Key Distribution). system, as well as the encoder and decoder. The accuracy of the arrival of the synchronization signals is lie within the range of tens of picoseconds, and strongly influences the overall system performance. The control system and synchronization software generates control commands.

2. COMMERCIAL QKD SYSTEMS WITH THE PHASE CODING OF STATES OF PHOTONS

The first commercial system of quantum cryptography was presented at the CeBIT-2002 exhibition, where engineers of GAP-Optique from the University of Geneva presented a system of QKD Scientists create a compact and reliable system, which was located in two cases, and could work without any setup immediately after connecting to a PC. It was used for key distribution through atmospheric and fiber-optic link between the cities of Geneva and Lausanne, the distance between which is 67 km (Stucki, Gisin, Guinnard, Ribordy, & Zbinden, 2002). The infrared laser with a wavelength of 1550 nm was source photons in it. Data transfer rate was low, because the high speed is not required for transmission keys with length from 27.9 up to 117.6 kilobits.

There are only three companies that enter the market with commercial QKD systems.

One of the earliest systems named id 500 Clavis (later version named id 3000 Clavis) began offering Swiss company id Quantique (Id Quantique SA, 2005). The system consists of two stations, operated by one or two external computer. The id 3000 Clavis software ensures quantum key distribution in automatic mode. The system supports two quantum cryptographic protocols BB84 and SARG04. The system generates the secret keys through the quantum line extending some 100 km. The system uses a built-in protocol sifting key and encryption protocol and file transfer. Generation rate of keys is up to 1500 bps.

Later, the id Quantique company released improved system id 3100 Clavis2 (Id Quantique SA, 2008) and the id 5000 Vectis (Id Quantique SA, 2005).

Manufacturers seek to develop integrated systems. For example, the system Vectis (2005) from the id Quantique company encrypts the data on the link layer using a cipher AES (Advanced Encryption Standard, 2001). The key can have a length of 128, 196 or 256 bits, and change with frequency up to 100 Hz. The maximum range of key transmission is 100 km (Id Quantique SA, 2005).

Company MagiQ Technologies (USA) offers a system QPN 5505 (2003), QPN 7505 (2005), and the QPN 8505 (2009).

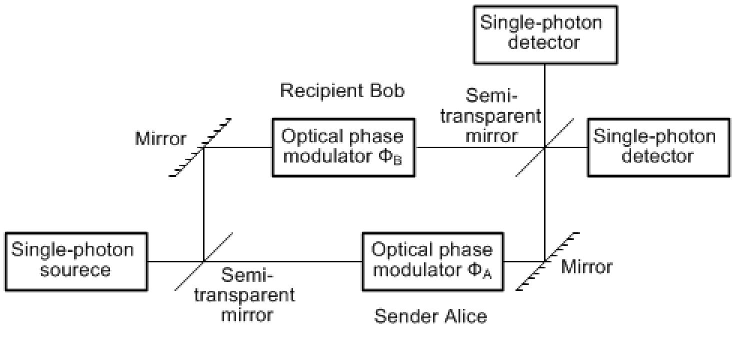
The Quintessence Labs Pty Ltd (Australia) company enters the market in 2009 and joins to two other companies. It also offers QKD systems for fiber-optic lines (Pauli, 2009). This system is housed in a rack-mounted case which is generally used in the network infrastructure.

Now government organizations and corporations with high security requirements use the commercial QKD system. Id Quantique reports of the implementation of QKD system into the banking sector (Id Quantique, 2011). Reducing the price of QKD systems can make quantum cryptography accessible to a large number of organizations. It is expected that quantum cryptography could become the de facto standard for inter-bank communications in a few years.

Commercial QKD systems transmit data through fiber-optic communication lines and encode information about the key bits in the phase states of photons. This is due to the fact that the instability of the polarization state greatly complicates the use of a polarization coding of states of the photon.

The idea of phase coding of states of photons was first mentioned C. Bennett (1992). Figure 2 illustrates the principle of phase coding of states of a photon using the interferometer.

Figure 2. Implementation of BB84 protocol with phase coding of states of a photon



Rumiantsev, 2008). Key bits are encoded using the phase states of photons of two pulses that propagate from one station to another and backward.

The first system based on this principle, called id 500 Clavis, has been produced by id Quantique since 2003. The system consists of two stations located in two cases and a software package for their control (Id Quantique SA, 2005). The first station is a transceiver, codenamed QKDS-B or Bob. The second station QKDS-A, or Alice, is the coding and does not contain transceiver equipment.

Let the Bob station to Alice station propagate optical pulses, and from Alice station to Bob station propagate photonic pulses. The term of optical pulse means a laser pulse with the average number of photons μ>> 1. The term of photonic pulse is a pulse containing a countable number of photons (in the QKD systems, as a rule, μ<1).

Let's perform an analysis of the structure of QKD system (Golubchikov, 2008) on a commercial system id 3000 Clavis manufactured by id Quantique company (Switzerland).

A Diagram of transceiving station Bob of id 3000 Clavis system is shown on Figure 6. It is purposed to generate optical pulses, receiving and processing the encoded quantum state of photons.

The station includes OTM, fiber optic circulator (FOC), two receiving optical module (ROM), FC X-type, FOL, PM and fiber-optic polarization coupler (FPC). Polarization-maintaining optical fiber (PMOF) connects these functional elements.

Station Alice of id 3000 Clavis system is shown in Figure 7. It is purposed to encode the phase states of photons. The coding station includes FC Y-type with a division factor of 1:9 from the port 1 to ports 2 and 3, respectively, two variable fiber-optic attenuators (VOA), FODL, PM, Faraday mirror and OF connecting all these elements.

A laser pulse with a wavelength of 1550 nm is emitted at the Bob station. It goes through FOC to FC X-type with a 50/50 division factor from port 1 to ports 2 and 3, respectively (see Figure 6). Thus. In the FC X-type laser pulse is split into two pulses.

The polarization of the optical pulse from port 3 FC X-type (first pulse) in the OF change its state to the orthogonal on the way to port 1 FPC.

Figure 6. Diagram of the transceiving station of id 3000 Clavis system

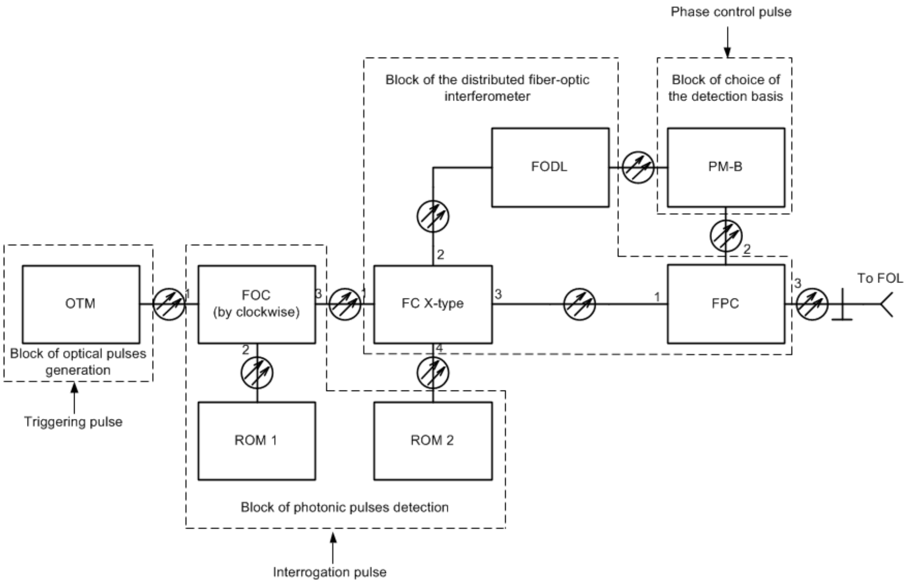

Phase control pulse
Block of the distributed fiber-optic interferometer
Block of choice of the detection basis
FODL
PM-B
2
OTM
1
FOC
(by clockwise)
3
1
FC X-type
3
1
FPC
3
To FOL
2
2
4
Block of optical pulses generation
Triggering pulse
ROM 1
ROM 2
Block of photonic pulses detection
Interrogation pulse

Table 1. BB84 protocol with phase coding of states of photons

Alice Station		Bob Station		
Bit Value	**Phase Shift Φ_A**	**Phase Shift Φ_B**	**Phase Difference $\Phi_A - \Phi_B$**	**Bit Value**
0	0	0	0	0
0	0	π/2	3π/2	underdeterminable
1	π	0	π	1
1	π	π/2	π/2	underdeterminable
0	π/2	0	π/2	underdeterminable
0	π/2	π/2	0	0
1	3π/2	0	3π/2	underdeterminable
1	3π/2	π/2	π	1

in practice not possible to maintain the lengths of the arms when users are separated from each other by more than a few meters.

In (Bennett, 1992) showed how to solve this problem by using two unbalanced Mach-Zehnder interferometer connecting by FOL (Figure 5).

In this scenario, the sender and recipient have identical unbalanced Mach-Zehnder interferometers. The phase difference between long and short arms should be much longer than the coherence length of the light source. For this reason, the interference in unbalanced interferometer does not occur. But it occurs at the interferometer output of receiver. The probability that the amplitude of the photonic pulses will interfere is equal $P_D = 0{,}25 \times \left[1 + \cos\left(\Phi_A - \Phi_Б\right)\right]$

It should be noted that the signal amplitude is two times less than in the case shown in Figure 2.

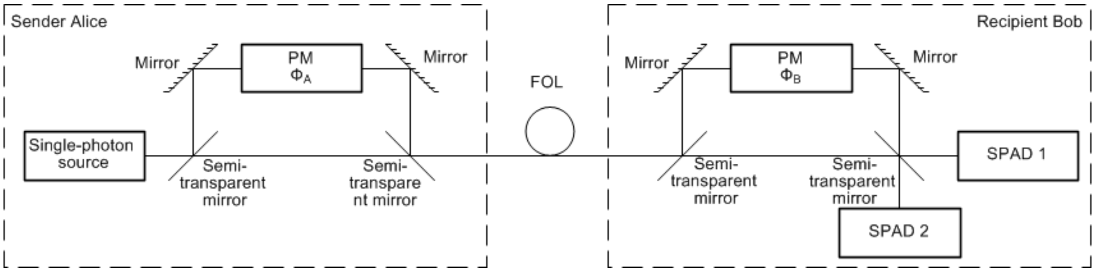
Signal splitter can be implemented in fiber-optic link as FC. Experimental measurements for 14 km FOL shown the effectiveness of the key bits generation at the level of 0,22% with bit error probability (BER) of about 1.2%.

The commercial QKD systems use more complicated coding scheme of the phase states of photons, which includes distributed interferometer with passive mode automatic compensation of polarization distortions (Ribordy, Gautier, Gisin, Guinnard, & Zbinden, 2000). Distortion compensation is required to observe a clear interference pattern of single photons on the SPAD input.

3. STRUCTURE OF COMMERCIAL QKD SYSTEMS

QKD system with automatic compensation of polarization distortions, which works on the principle of plug & play, is the only technology that is presented on the QKD market (Golubchikov, &

Figure 5. Implementation of the protocol on the B92 two unbalanced interferometers



When the phase difference is $\pi + 2n\pi$, the situation is opposite. The destructive interference is at the input of the second SPAD, while the average number of photons at the input of the first SPAD reaches a maximum. The optical radiation can be detected at the inputs of both SPAD in case of errors of SPAD.

Mach-Zehnder interferometer with single-photon source and the two SPAD can be used in quantum cryptography (see Figure 4). Station Alice in this case should consist the optical transmitting module (OTM) based on laser diode, fiber optic attenuator (VOA), FC Y-type and the first PM. Optical pulse of OTM through the VOA send to the port 1 FC Y-type as an single photons (Golubchikov, & Rumiantsev, 2008).

It should be noted that it is extremely important is to maintain a constant and small difference between the lengths of the interferometer arms to get a stable interference.

Bob station consists of the second PM, FC X-type and two photon counters based on SPAD.

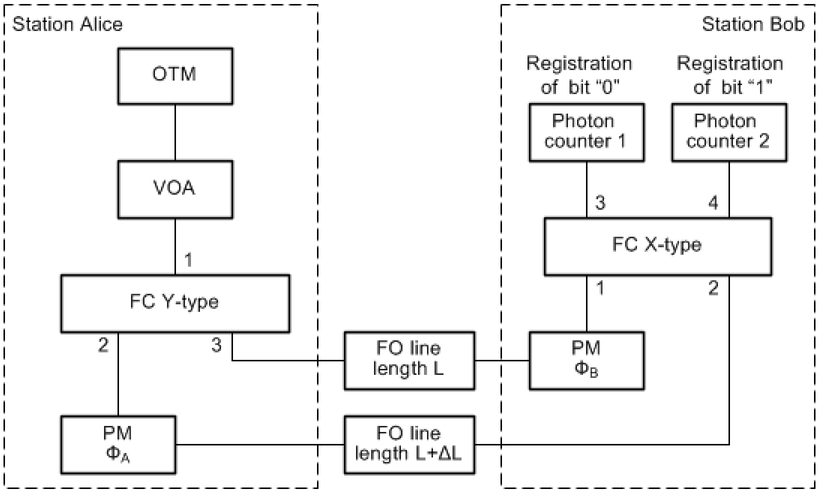
We consider the using BB84 protocol with four states in such scheme. Station Alice through the first PM implement one of the four phase shifts (0, π/2, π, 3π/2). The bit value 0 corresponds to the phase shift of 0 and π/2, the bit value 1 corresponds shift of π and 3π/2. The Bob station through the second PM makes the choice of basis in random order, by shifting the phase by 0 or π/2. The photon which came to the first photon counter is assigned the 0 value of bit., & the photon which came to the second counter corresponds to 1 value of bit

When the phase difference equal to 0 or π, then the stations Alice and Bob use compatible bases and obtain definite results. In such cases, the station Alice can determine which of the SPAD of the Bob stations gets a photon, and hence, it can determine the value of the bit. For its part, the Bob station can determine which phase shift is selected by Alice station. In the case where the phase difference takes values π/2 or 3π/2, the stations use incompatible bases, so the photon will be detected on random SPAD of Bob station.

All possible combinations of phase shifts in BB84 protocol with four states listed in Table 1.

Note that the system is extremely important to maintain a stable difference in the lengths of the interferometer arms pending the all key distribution session. This difference shouldn`t change more than a fraction of the emission wavelength. Changes in the one arm length may lead to a phase drift and to the errors in the key in the result. This scheme works well in laboratory conditions, but

Figure 4. Quantum system with a Mach-Zehnder interferometer



Transmitter and receiver create a system based on Mach-Zehnder interferometer to realize the BB84 protocol. The sender sets the angles of phase shift corresponding to the logical zero ($\Phi_A = 0$ or $\Phi_A = \pi/2$) and to the logical one ($\Phi_A = \pi$ or $\Phi_A = 3\pi/2$). The receiver sets its phase shifts for the equivalent vertical basis ($\Phi_B = 0$) and equivalent to the diagonal basis ($\Phi_B = \pi/2$).

In this context, *the phase shift of 2π using an optical phase modulator corresponds to the change in path length for one step of wavelength.*

The photons behave as particles in to photodetection process, but they propagate as waves. The probability that a photon sent by the sender will be detection by the recipient, is

$$P_D = \cos^2\left(\frac{\Phi_A - \Phi_{\text{Б}}}{2}\right)$$

and determined by the interference of waves propagating along the two arms of Mach-Zehnder interferometer.

Detection probability will vary from 1 (for zero phase difference) to zero. Here it is assumed that the optical phase modulators sender Alice and receiver Bob use the phase shifts (Φ_A, Φ_B) = (0, $3\pi/2$) for zero bits and (Φ_A, Φ_B) = ($\pi/2$, π) for a single bit.

Preparing the quantum states and their analysis is realized in the interferometer, which can be implemented on single-mode fiber optic elements. Figure 3 shows a fiber-optic implementation of the Mach-Zehnder interferometer.

The interferometer consists of a fiber coupler (FC) Y-type, two fiber-optic phase modulators (PM) and FC X-type. In each arm of the interferometer includes one PM. Single-photon optical radiation can introduced into the interferometer and it will registered at the outputs of 3 and 4 FC X-type.

If the coherence length of single-photon source (SS) is greater than the difference between the lengths of the interferometer arms, then you can get an interference pattern.

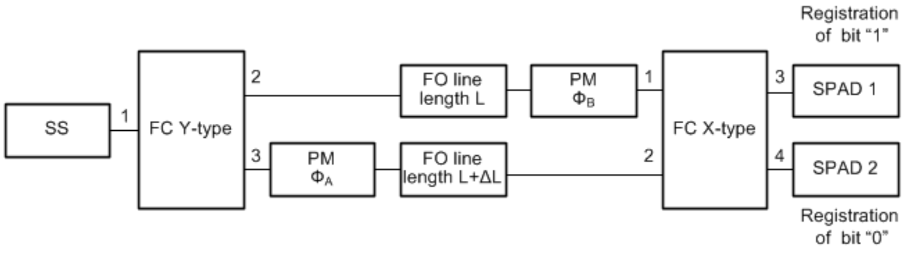
In FC Y-type and FC X-type phase shift is *π/2 in each.* Because of the PM actions (Φ_A and Φ_B) and the difference between the lengths of arms in *ΔL*, the average number of photons during the observation period τ_{observ} at the input of the first single-photon avalanche detector (SPAD) is defined by

$$\overline{N}_{SPAD} = \overline{N}_{LS} \cdot \cos^2\left(\frac{\Phi_A - \Phi_B + k\Delta L}{2}\right)$$

where k is a wave number, and $\overline{N}_{LS}$ is the average number of photons SS during the observation period. Note that the first SPAD detects photons corresponding to the zero bits.

If the phase difference is $2n\pi$ (n is an integer), then destructive interference is on the input of the first SPAD which registering zero bits. Therefore, the number of photons detected by the first SPAD reaches a minimum value. Ideally, the second SPAD register all photons.

Figure 3. Mach-Zehnder interferometer



OTM includes a laser and is designed to generate coherent optical radiation with a wavelength of 1550 nm and a spectral width not exceeding 0.6 nm (optical output 2). The light source based on the principle of distributed feedback due to which it is possible to achieve a narrow spectral width. The small width of the spectrum permits to emit a signal with high temporal coherence, which can increase the transmission distance and reduce the effects of dispersion distortions. In the OTM can also be integrated photodiode for direct measurement of the laser power (output 1). Electronic control module can adjust the power of the source and the duration of the emitted laser pulses.

Electronically controlled VOA-B has a wide range of attenuation from 1.5 to 50 dB. Change the voltage onto the control input 2 of VOA-B may prevent interception of optical pulses and reduce the reflected from the Faraday mirror emission to the level of the photonic pulse.

FOC has three ports, each of which can be input and output. The principle of operation is based on the transfer of energy from port 1, which is in the circuit is connected to the OTM, to the nearest clockwise port 2 connected to the FC X-type. Transmission in the opposite direction from port 2 to port 1 is excluded due to the large attenuation of the radiation. However, the energy is transferred from port 2 to port 3. Fiber-optic circulator is a passive optical element and has no electrical control inputs.

ROM-B1 and ROM-B2 are designed to detect photonic pulses. The structure of the modules is complex and has many control inputs, which used for adjustment of the bias, dead time period, wait time period and others. The module includes SPAD, cooling device, gain controller and control device.

When working SPAD possibly causing an avalanche of electrons in the absence of a photon at the input. Such a process is defined as the dark current SPAD. The frequency of a dark count is characterized by the number of false count SPAD per time unit and has the dimension of hertz.

One of the important factors that influence the dark count rate is temperature of SPAD. In ROM photodiode temperature set by the user and continuously monitored using a thermistor. Peltier cooler is used for cooling SPAD. The drift of the temperature does not exceed 0.1°C. The temperature difference of 1°C has a significant impact on the frequency of dark count.

Gain controller designed to amplify the response of the detection of single-photon pulse by SPAD.

The control device is designed for analyzing the signals from the SPAD, temperature control, regulating the amplitude, duration and the filing of bias. In most schemes, the method of bias booster is used. This method keeps up the permanent bias voltage on the control input of SPAD, but at a level not enough to generate an avalanche. This scheme allows to reducing the time of transients at the moment of applying bias voltage required for the registration of single-photon pulse.

FC X-type is a passive element with 4 ports. With direct distribution of an optical pulse generated by OTM only pass to port 1 of FC X-type, where the energy is distributed equally on the two ports 2 and 3.

With the passage of the photonic signal from the Alice station was in the FC X-type came two waves and interfere with each other. Then the result of interference sent to one of two ports 1 and 4, respectively, leading to ROM-B1 or ROM-B2.

FODL-B is the segment PMIF and is intended to introduce a time delay between the signals coming from different optical interferometer arms.

PM-B is based on electro-optical crystal of lithium niobate. The principle of operation based on the Kerr effect. Modulator allows you to make a phase shift in the signal passing through the long arm in the reverse signal propagation. The range of phase shifts is from 0 to 2π.

Photonic signal from the Alice station at port 3 FPC, will be redirected to the opposite interferometer arm. This is because after the passage of

Figure 9. Diagram of the coding station of the QPN 5505 system

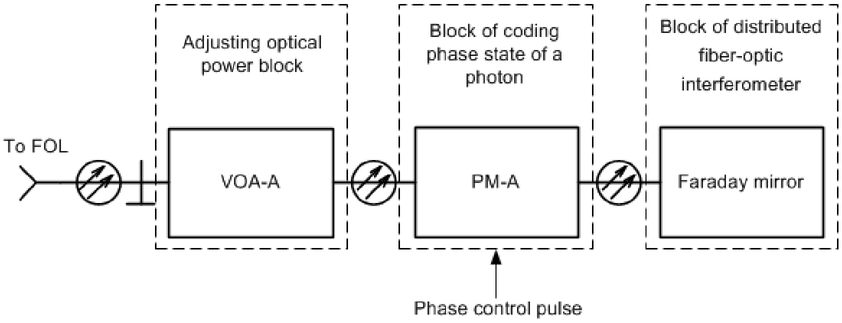

Adjusting optical power block
Block of coding phase state of a photon
Block of distributed fiber-optic interferometer
To FOL
VOA-A
PM-A
Faraday mirror
Phase control pulse

Figure 10. Generalized structure of QKD systems

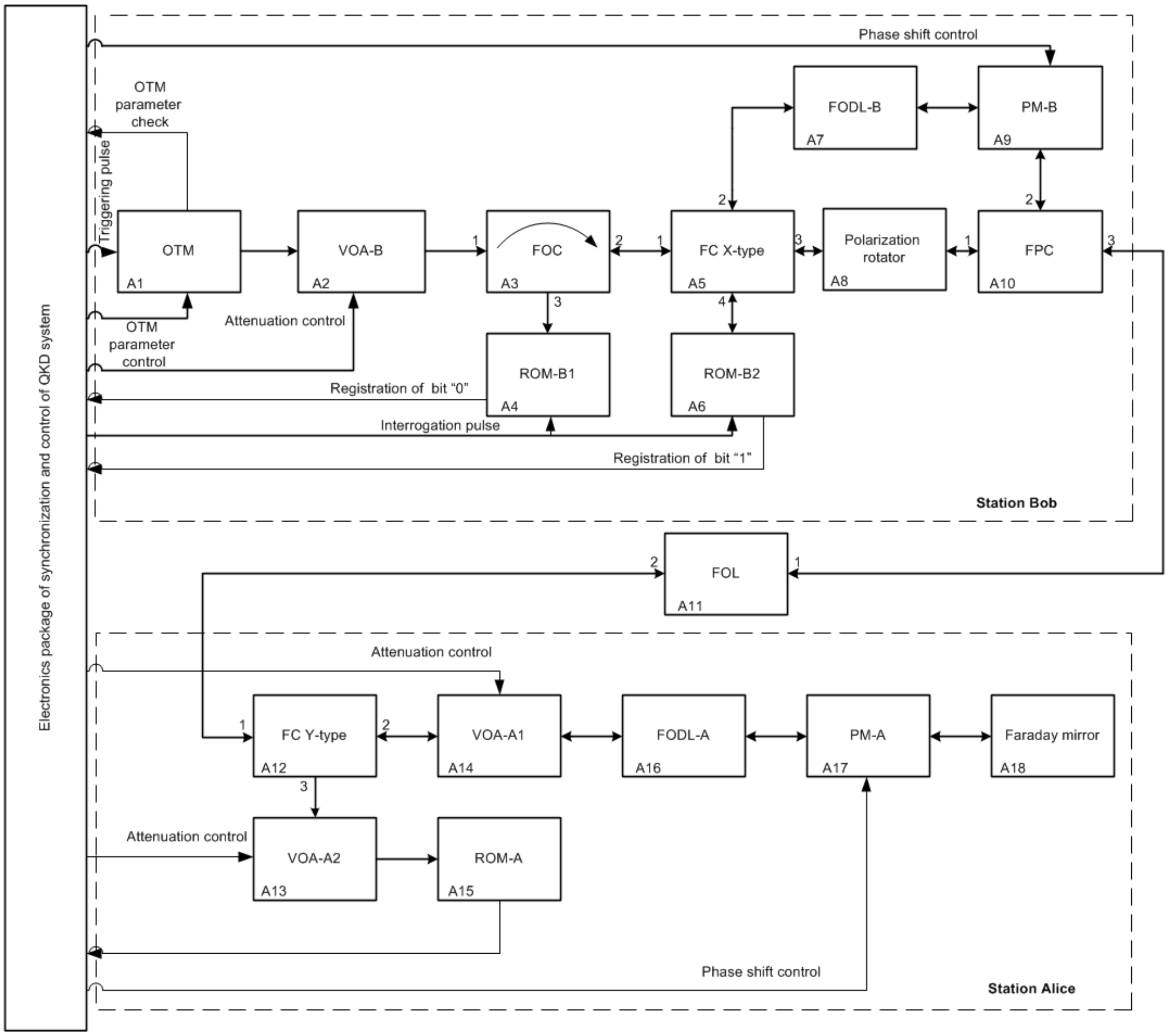
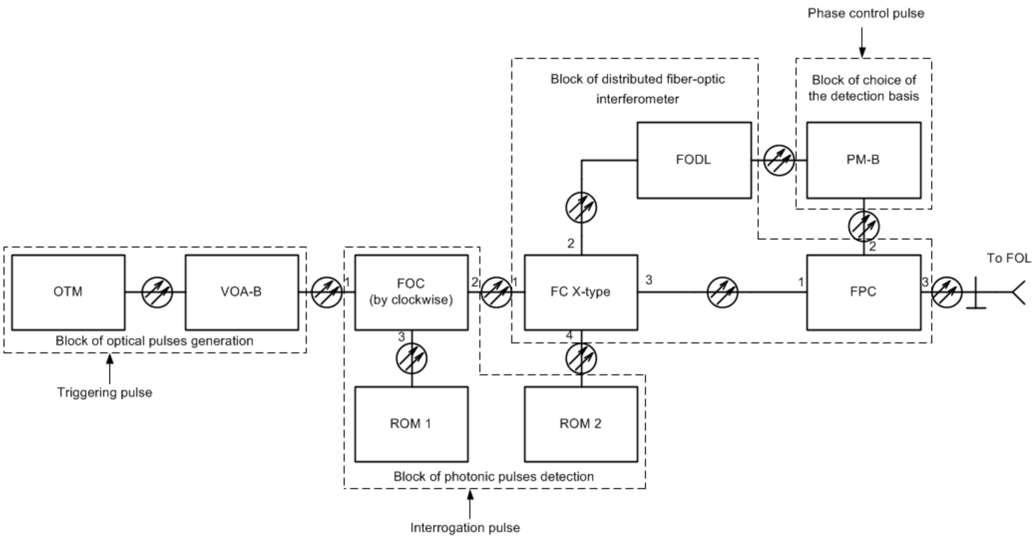


Figure 8. Diagram of optical transmitter-receiver station system QPN 5505


Phase control pulse
Block of distributed fiber-optic interferometer
Block of choice of the detection basis
FODL
PM-B
2
OTM
VOA-B
1
FOC
(by clockwise)
2
1
FC X-type
3
1
FPC
3
To FOL
Block of optical pulses generation
Triggering pulse
3
4
ROM 1
ROM 2
Block of photonic pulses detection
Interrogation pulse

3000 Clavis, has VOA through which the OTM is connected to port 1 on FC. All blocks, as in the system id 3000 Clavis, connected by PMOF.

There are significant differences in the structure of the coding station of the QPN 5505 system (Figure 9) from the id 3100 Clavis system (Figure 7).

The coding station consists of an adjusting optical power block, block of coding phase state of a photon, and a block of distributed fiber-optic interferometer. All the blocks are interconnected by OF.

Due to the presence of features implemented in the coding station QPN 5505 system has not synchronization block. The system id 3100 Clavis used to synchronize optical pulses passing through FOL from Bob station to Alice station. In the QPN 5505 synchronization is ensured by an additional communication line and an additional transceiver module.

For the system id 3100 Clavis is necessary and sufficient one FOL, since clock line and the QKD link combined, but for the system QPN 5505 requires additional FOL for synchronization and data transfer.

4. GENERALIZED STRUCTURE OF QUANTUM KEY DISTRIBUTION SYSTEM WITH PHASE CODING OF PHOTONS STATES

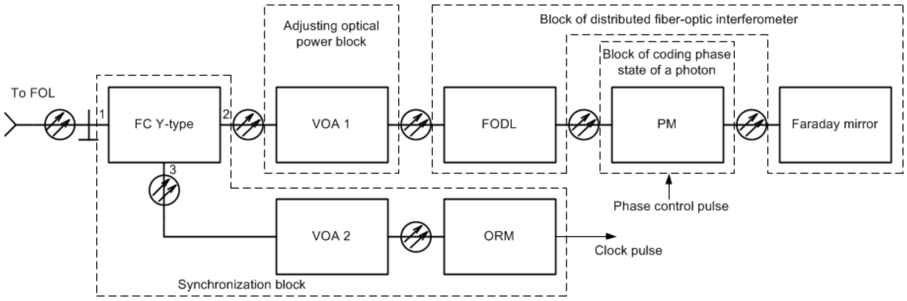
The analysis of commercial systems id 3100 Clavis and QPN 5505 allowed to identify common structural similarity solutions: the block of optical pulses generation, the block of the distributed fiber-optic interferometer, the block of choice of the detection basis, the block of photonic pulses detection, the block of power control, the block of coding states of the photon, and synchronization block.

We propose a generalized structure of the QKD system with phase coding of photons, which shown on Figure 10 and based on the analysis above.

Transceiving Bob station is designed to generate optical pulses, receiving and processing the encoded quantum states of photons.

The structure of transceiving stations consist OTM, VOA (VOA-B), FOC, two ROM (ROM-B1 and ROM-B2), FC X-type, FODL (FODL-B), the polarization rotator by 90°, PM (PM-B), fiber-optic polarizing multiplexer/demultiplexer (FPC). All blocks are interconnected by PMOF.

Figure 7. Diagram of the coding station of id 3000 Clavis system


Adjusting optical power block
Block of distributed fiber-optic interferometer
Block of coding phase state of a photon
To FOL
1
2
3
FC Y-type
VOA 1
FODL
PM
Faraday mirror
Phase control pulse
VOA 2
ORM
Clock pulse
Synchronization block

A laser pulse from port 2 FC X-type (second pulse) goes through FODL and PM to port 2 FPC. The second pulse is delayed on 50 ns relative to the first as a result of the propagation through two different optical paths.

Note that signals propagated in different arms of the interferometer are orthogonally polarized, which is due to the fact that the fast axis of PMOF in two arms are rotated by an angle of 90° to each other.

Fiber-optic polarization coupler is a passive element. Since the orthogonally polarized pulses from ports 1 and 2 FPC out to the port 3, then FPC represents the polarization multiplexer, which output is the output of transceiving station Bob.

Impulses are going to the station Alice via FOL and are reflected by Faraday mirror (see Figure 7). Faraday mirror is a rotator with a fixed angle of rotation of the polarization by 90°. The consequence is that the reflected pulses are not only orthogonally polarized with respect to each other, but also orthogonally polarized with respect to the primary pulse state at the input of the Faraday mirror.

Reflected by the Faraday mirror pulses are weakened by VOA and follow back to the station Bob.

Both photonic pulses pass by turn through FPC into transceiver stations (see Figure 6). These pulses are orthogonally polarized relative to the primary state. The pulses pass into the arms in which there are no the direct propagation. Here FPC works as a polarization demultiplexer.

Photonic pulses pass to FC X-type at the same time and interfere. Then the interference is detected on the first or second ROM.

Since both pulses pass the same optical path, such an interferometer automatically compensate of the polarization distortion.

To implement the BB84 protocol at the Alice station the second pulse is phase shifted by one of the randomly selected values of the series 0, $\pi/2$, π, $3\pi/2$. At the Bob station chooses a basis of measurement by the phase shift of the first pulse at 0 or $\pi/2$ at the backward pulse propagation.

Note that in the station Bob combines the functions of the transmitter and receiver. However, the function of phase coding the quantum state of photon assigned to the PM of the Alice station. Thus, the diagram shown on Figure 7 is a scheme of Alice station in the classical interpretation of the BB84 protocol.

Commercial system QPN 5505 presented in 2003. It based on QKD plug & play technology with automatic compensation of polarization distortion.

Let analyze the functional scheme of transceiver stations of QPN 5505 (Figure 8). The station is designed to generate optical pulses, receiving and processing the encoded quantum states.

The structure of transceiving station QPN 5505 system showing on Figure 8, unlike the system id

FOL the pulse changes its polarization orthogonal in the Faraday mirror of Alice station.

Signals that propagate in different arms of the interferometer are polarized orthogonally because the polarization rotator by 90° is used.

Optical pulses arriving at the two ports 1 and 2 of FPC are sent to port 3, which is the output of transceiving Bob station.

Alice encoding station in Figure 10 is designed to encode the phase states of photons. It consists of FC Y-type, two VOA (VOA-A1 and VOA-A2), FODL (FODL-A), PM (PM-A), ROM (ROM-A), Faraday mirror and OF linking all of the elements.

FC Y-type is intended to separate the energy of the optical signal. Pulse passing FOL, get to port 1 of FC Y-type, which is divided into two pulses with the energy ratio of 1:9.Two ports 2 and 3, respectively, pulses are sent to VOA-A1 and VOA-A2.

To ROM-A is sent 90% of the energy of the optical pulse receiving by the Alice station. The remaining 10% of the energy of input pulses is sent to the FODL-A input through the VOA-A1.

Electronically controlled VOA-A1 and VOA-A2 have attenuation band up to 50 dB. Changing the level of voltage onto the control input of VOA helps to prevent damage an optical components in case of trying to introduce high-power optical pulses (wide pulse attack), or in case if the attenuation of the pulse energy is too small because the FOL is too short, and as well as to reduce the reflected emission from the Faraday mirror to the level of the photonic signal.

At the Alice station ROM-A has two functions:

1. Synchronize the stations clock and mark the moment of arrival of the pulse for the subsequent issuance of electronic control signal to PM-A,
2. Monitoring of incoming signals level to detect an attacker in the channel.

FODL-A is OF line segment with length about 10...12 km and is intended to prevent false alarms of SPAD in ROM in consideration of Rayleigh backscattered radiation from the elements of encoding station established between port 2 FC Y-type and Faraday mirror.

PM-A apply a phase shift only for photons of the second pulse, which delayed to the first in the reverse signal propagation. Structurally PM-A is identical to the modulator used in the station Bob.

To implement the BB84 protocol the PM-A uses the following values of the phase shift:

1. Zero bit 0 is encoded in a linear basis, zero phase shift,
2. Single bit 1 in the linear basis is encoded by a phase shift of π,
3. Zero bit 0 is encoded in the diagonal basis of a phase shift of π/2,
4. Single bit 1 in diagonal basis is encoded phase shift of 3π/2.

Faraday mirror is a rotator of polarization angle by 90^o. Thus, the photon pulses in backward propagation will have orthogonal polarization relative to the pulses at the input Faraday mirror.

After reflection from the Faraday mirror the photon pulses via port 2 of FC Y-type coming in the opposite direction to the station Bob through the FOL.

Synchronization in a QPN 5505 is provided with an additional synchronization and monitoring block. That block in comparison with the QKD system is external, while mounted on a same case. In id 3000 Clavis id used to synchronize the optical pulses by direct spread from station to station, Bob Alice.

Designed the generalized structure of the QKD system with phase coding of photons includes all the blocks that have a direct influence on the propagation and processing of quantum states and are available in 4 commercial systems.

Excluding of the generalized structure QKD systems the FC Y-type, FODL-A, VOA-A2 and ROM-A, we get the structure of MagiQ QPN 5505. To obtain the structure of the system id 3100 Clavis enough to exclude from the generalized structure VOA-B.

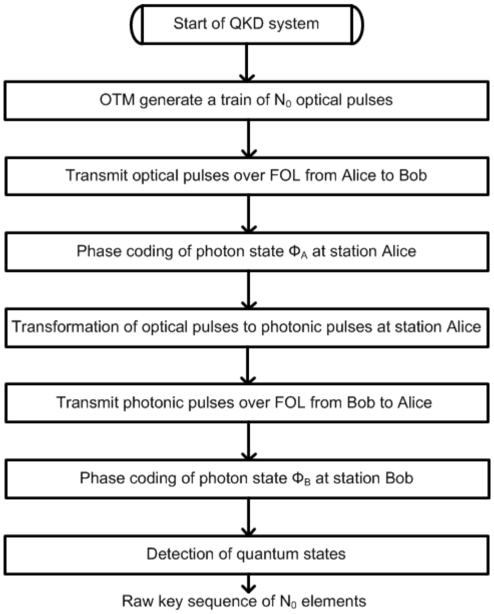
Generalized structure used to estimate the influence of component parameters on the process of signal propagation in commercial QKD.

5. MODEL OF INFORMATION SECURITY INFRASTRUCTURE WITH QUANTUM KEY DISTRIBUTION

The pulses of the transmitter can be multi-photon. In addition, single-photon detectors have a spontaneous emission noise. Therefore, the data Alice and Bob share will be different even in the absence of eavesdropping. Consequently, the generation of the secret key is preceded a number of intermediate processing steps to correct the difference in key sequences of Alice and Bob.

Step 1: Generation of raw key sequence (Figure 11). At the first stage the OTM generates a train of optical pulses. The next operations are performed sequentially: transmission the train of pulses through FOL from Bob to Alice, the PM encode a phase state inside the Alice station, the shaping of photonic pulse for transmission through FOL from Alice to Bob and, finally, the measurement of quantum states of photons in receiver modules ROM-B1 and ROM-B2 (Figure 10). After that Alice and Bob have the *raw key sequence*.

Figure 11. Block-diagram of the raw key sequence generaion

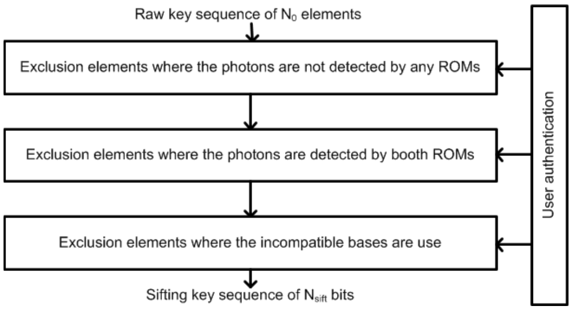

Start of QKD system
OTM generate a train of N_0 optical pulses
Transmit optical pulses over FOL from Alice to Bob
Phase coding of photon state Φ_A at station Alice
Transformation of optical pulses to photonic pulses at station Alice
Transmit photonic pulses over FOL from Bob to Alice
Phase coding of photon state Φ_B at station Bob
Detection of quantum states
Raw key sequence of N_0 elements

In this sequence of N_0 elements (number of ROMs gating) contains the results of measurements, where the two receiver modules ROM-B1 and ROM-B2 at the Bob station don`t detected any single photon. In addition, this sequence has the results of measurements in which the two modules ROM-B1 and ROM-B2 detected photons at the same time. Finally. In the sequence are the results of measurements in which users are using different bases.

During subsequent refinement through the exchange of data by open channel Alice and Bob can get a version of a key sequence, suitable for the shaping and sharing of the secret key, or discard the raw key sequence and repeat the process of generation and transmission of quantum state. Refinement may include the following four steps (Center for KvanteInformatik).

Step 2: Generation of the sifted key sequence (Figure 12). Users Alice and Bob reveal the strobe pulse intervals in which the receiving module ROM-B1 and ROM-B2 don`t detect any photons. In addition, Bob show the positions of strobe pulse intervals in which the

Figure 12. Block-diagram of the sifted key sequence generaion


Raw key sequence of N_0 elements
Exclusion elements where the photons are not detected by any ROMs
Exclusion elements where the photons are detected by booth ROMs
Exclusion elements where the incompatible bases are use
Sifting key sequence of N_{sift} bits
User authentication

two modules time ROM-B1 and ROM-B2 detected photons at the same. The positions of raw key sequence, which revealed abnormalities in photon detection, are excluded.

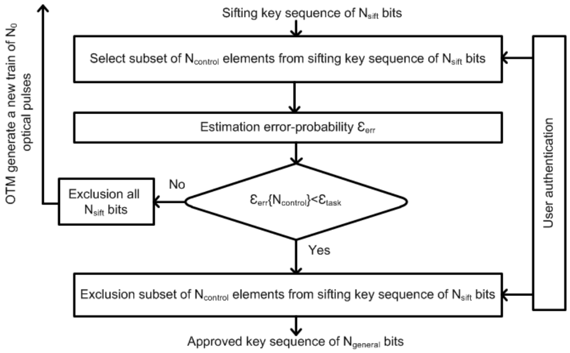
User Bob publicly on the open channel inform Alice which bases are chosen in each position of the remaining sequence. Alice confirms or not confirms chosen bases. Any communication channel in which is implemented a standard protocol RSA with public key or the Internet may use as open channel.

From raw key sequence excludes also the results of measurements in which users are using different bases.

As a result of these three operations generated *sifted key sequence* which contains only the bits corresponding to the same basis. Note that the length N_{sift} of the sifted key sequence of bits does not exceed the size of the train of optical pulses.

Step 3: Generation of approved key sequence (Figure 13). As the ideal communication channels do not exist then sifted key sequence may contain errors. Therefore, the formation of identical user key sequence is necessary to estimate the probability of bit errors in the sifted key sequence of bits.

Figure 13. Block-diagram of the approved key sequence generaion


Sifting key sequence of N_{sift} bits
Select subset of $N_{control}$ elements from sifting key sequence of N_{sift} bits
Estimation error-probability ε_{err}
$\varepsilon_{err}\{N_{control}\}<\varepsilon_{task}$
No
Yes
Exclusion all N_{sift} bits
Exclusion subset of $N_{control}$ elements from sifting key sequence of N_{sift} bits
Approved key sequence of $N_{general}$ bits
OTM generate a new train of N_0 optical pulses
User authentication

To estimate the error probability Alice announces by open channel the subset of N_{control} positions in the sifted key sequence N_{sift} length and the corresponding values of the bits. Recipient Bob also sends to Alice the value of bits detected in the same positions. Alice and Bob compute the error probability of his observations $\varepsilon_{err}\left\{N_{control}\right\}$ on the N_{control} length of the subset. The result of the transfer of key sequences is considered positive if the measured error probability is $\varepsilon_{err}\left\{N_{control}\right\}$ less than the permissible level ε_{task}, i.e. $\varepsilon_{err}\left\{N_{control}\right\} < \varepsilon_{task}$. In this case announced subset of bits N_{control} is removed from the sifted key sequences. The *approved key sequence* length is $N_{\text{general}} = N_{\text{sift}} - N_{\text{control}}$. In the case of $\varepsilon_{err}\left\{N_{control}\right\} \geq \varepsilon_{task}$ the generation of the train of optical pulses N_0 is repeated.

Note that in a perfect quantum channel without a noise reveal the mismatch in the one open position is enough for the detection of an eavesdropper. In a real situation it is impossible to recognize errors that occurred due to noise and errors that occurred the attacker.

In (Shor, & Preskill, 2000) showed that if the error rate $\varepsilon_{\text{err}}\left\{N_{\text{control}}\right\}$ does not exceed 11% then the legitimate users can extract the secret key from approved key sequence after the stages of errors correction and privacy amplification. In addition, the key will not be known to the attacker.

Step 4: Generation consistent key sequence (error correction). The minimum number of *m* bits that Alice and Bob must share openly to correct errors in its bit sequences is determined by the Shannon's coding theorem. In our case, when the error probability of any bit sequence is constant and equal to p_{bit}, Shannon's theorem states that

$$m = N_{\text{general}}\left[-p_{\text{bit}}\log\left(p_{\text{bit}}\right)-\left(1-p_{\text{bit}}\right)\log\left(1-p_{\text{bit}}\right)\right]$$

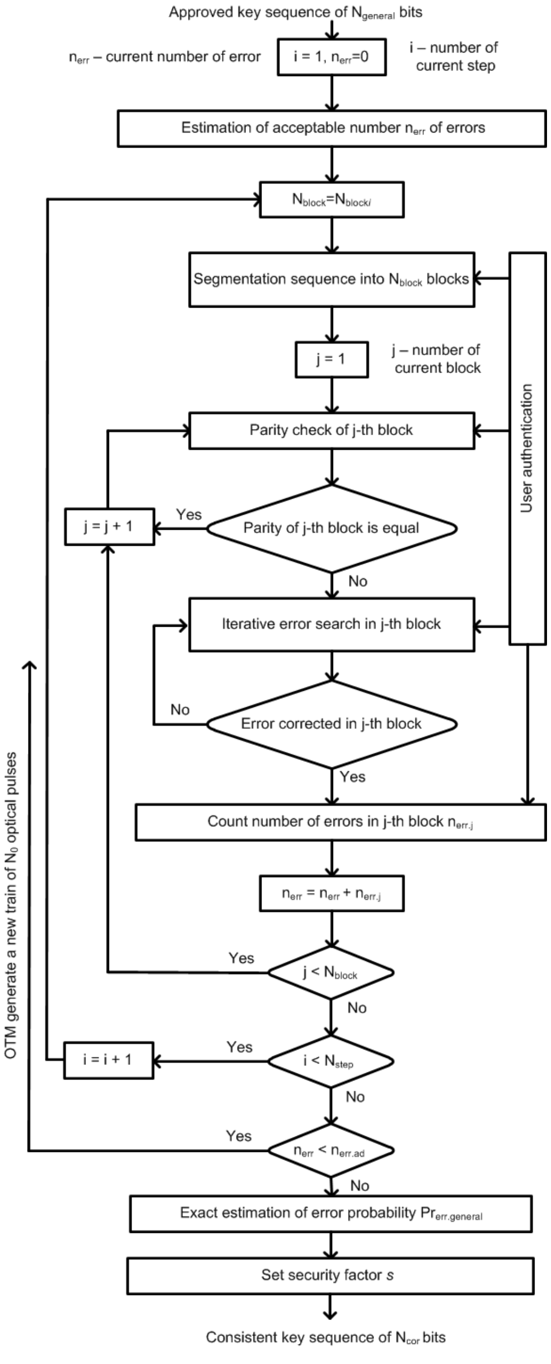
Shannon's theorem suggests the possibility of error correction at the opening of m bits of the key sequence of N_{general} elements. However, the theorem does not give explicit error correction procedure. Conventional linear error-correcting codes in this respect rather inefficient.

In QKD systems Alice and Bob perform the matching procedure on approved key sequence using an iterative error correction algorithm based on the parity check (Brassard, & Salvail, 1993).

In the first step, users Alice and Bob group their bits in the N_{block1} blocks of a certain size (Figure 14). They share information about the parity of each j-th block of N_{block1} by open channel.

If the parity of the j-th block is equal then Alice and Bob proceed to the next $(j + 1)$-th block. If the parity of the j-th block is not equal then Alice and Bob conclude that within the bock imply odd number of errors. In this case users are search for an error in the j-th block recursively. To do this they divide the j-th block into two sub-blocks and compare the parity of the sub-blocks. If the parity in the first sub-block is the same of Alice and Bob, then the second sub-block must contain an odd number of errors. If the parity of the first sub-blocks is different so the odd number of errors is disposed in the first sub-block. Error correction procedure recursively continues in the sub-block with an odd number of errors.

Figure 14. Block-diagram of the consistent key sequence generation


Approved key sequence of N_{general} bits
n_{err} – current number of error
$i = 1$, $n_{\text{err}}=0$
i – number of current step
Estimation of acceptable number n_{err} of errors
$N_{\text{block}}=N_{\text{block}i}$
Segmentation sequence into N_{block} blocks
User authentication
$j = 1$
j – number of current block
Parity check of j-th block
$j = j + 1$
Yes
Parity of j-th block is equal
No
Iterative error search in j-th block
No
Error corrected in j-th block
Yes
Count number of errors in j-th block $n_{\text{err},j}$
$n_{\text{err}} = n_{\text{err}} + n_{\text{err},j}$
Yes
$j < N_{\text{block}}$
No
$i = i + 1$
Yes
$i < N_{\text{step}}$
No
Yes
$n_{\text{err}} < n_{\text{err.ad}}$
No
OTM generate a new train of N_0 optical pulses
Exact estimation of error probability $\text{Pr}_{\text{err.general}}$
Set security factor s
Consistent key sequence of N_{cor} bits

After a first step each block contains either an even number of errors or none. Therefore, the second step ($j = 2$) Alice and Bob change the position of their bits and repeat the same procedure with N_{block2} blocksoflargersize $(N_{\text{block1}} > N_{\text{block2}})$. However, if the error is corrected then Alice and Bob can conclude that in some previously examined blocks now contain an odd number of errors.

They choose the least of these blocks and recursively, as before, correct the error.

Users realize the error correction as long as each block contains an even number of errors or none.

Iterative correction of errors will stop after a certain number of steps N_{step}. The number of steps should minimize the probability of errors.

However, there is a nonzero probability that a key sequence length $N_{general}$ has more than $\Pr_{err.general.ad} = 11\%$ of errors. This value is the critical limit of the probability of errors in a consistent key sequence, beyond which it is impossible to guarantee the secrecy of the key (Shor, & Preskill, 2000; Mayers, 2001; Biham, Boyer, Boykin, Mor, & Roychowdhury,). In this case excluded all approved key sequence length $N_{general}$ and OTM generates a new train of optical pulses N_0.

Step 5: Privacy amplification. After error correction Alice and Bob have a high probability identical consistent key sequence of bit and know exactly what the error rate is. They assume that all errors are caused by eavesdropper Eve. In addition, they allow a leakage of information during the error correction by setting the compression options *s*.

Alice announces to Bob a description of a randomly chosen hash function, which is used to the consistent key sequence to get the full secret key sequence.

In most QKD protocols the Alice on privacy amplification stage applies one-way function or Universal 2 HASH Function based on any Toeplitz matrix

$$\left\|rnd_{ij}\right\|_{(N_{\text{hash}}\times N_{\text{cor}})} = \left\|\begin{matrix} rnd_{11} & rnd_{12} & \dots & rnd_{1N_{\text{cor}}} \\ rnd_{21} & rnd_{11} & \dots & \dots \\ \dots & \dots & rnd_{11} & rnd_{12} \\ rnd_{N_{\text{hash}}1} & \dots & rnd_{21} & rnd_{11} \end{matrix}\right\|$$

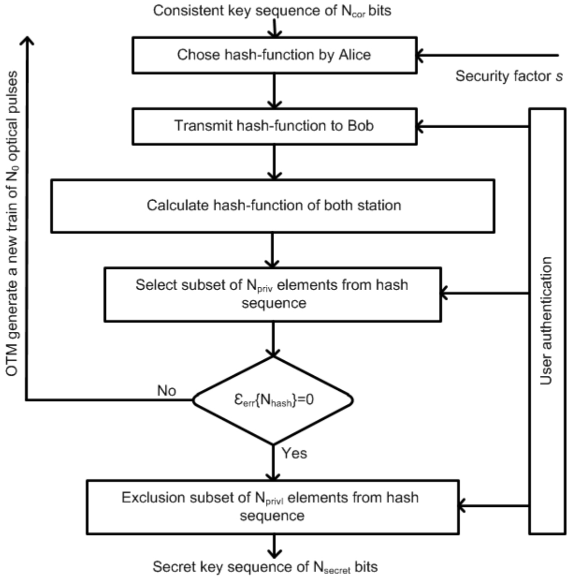
Matrix size is $N_{\text{hash}} \times N_{cor}$, where $N_{\text{hash}} = N_{\text{cor}} - s$, rnd_{ij} are random numbers takes the value 0 or 1. This matrix Alice sends to Bob by open channel (Figure 15).

Let the values of bits of the consistent key sequence given as elements of the column matrix X_i with $N_{cor} \times 1$ size. Transformed key sequence Y_j will be determined by the elements of the row matrix $1 \times N_{\text{hash}}$ size. So (Bouwmeester, Ekert, & Zeilinger, 2000)

$$\begin{gathered} {}_1 \quad Y_2 \quad \dots \quad Y_{N_{\text{hash}}} \Big) = \left\|Y_{ij}\right\|_{(1\times N_{\text{hash}})} \\ \left\|rnd_{ij}\right\|_{(N_{\text{hash}}\times N_{\text{cor}})} \times \left\|X_{ij}\right\|_{(N_{\text{cor}}\times 1)} \\ \begin{pmatrix} rnd_{11} & rnd_{12} & \dots & rnd_{1N_{cor\pi}} \\ rnd_{21} & rnd_{11} & \dots & \dots \\ \dots & \dots & rnd_{11} & rnd_{12} \\ rnd_{N_{\text{hash}}1} & \dots & rnd_{21} & rnd_{11} \end{pmatrix} \times \begin{pmatrix} X_1 \\ X_2 \\ \dots \\ X_{N_{cor}} \end{pmatrix} \pmod 2. \end{gathered} \tag{1}$$

Alice and Bob randomly selected N_{priv} control bits of the transformed sequence N_{hash} length.

Figure 15. Block-diagram of the secret key sequence generation


Consistent key sequence of N$_{cor}$ bits
Chose hash-function by Alice
Security factor s
Transmit hash-function to Bob
Calculate hash-function of both station
Select subset of N$_{priv}$ elements from hash sequence
ε$_{err}${N$_{hash}$}=0
No
Yes
Exclusion subset of N$_{privi}$ elements from hash sequence
Secret key sequence of N$_{secret}$ bits
OTM generate a new train of N$_0$ optical pulses
User authentication

No errors $\varepsilon_{err}\left\{N_{\text{priv}}\right\}$ in the selected bits ensure that the sequence N_{hash} of the users Alice and Bob are identical with probability close to 1. The remaining bits $N_{\sec ret} = N_{hash} - N_{\text{priv}}$ form the secret key sequence.

In the case of $\varepsilon_{err}\left\{N_{\text{priv}}\right\} \neq 0$ all consistent key sequence is excluded, OTM generates a new stack of N_0 optical pulses.

As the result of these actions, illustrated in Figures 11-15, the legitimate users Alice and Bob have the identical sequence of bits. These bits are the secret key sequence. The secret key of a required length is taken from the secret key sequence. Users with the secret key are able to encode and decode private information and transmit information over the insecure data line.

The authentication should use in the stages of key generation to prevent an attack the man in the middle. The authentication allows users to make sure that message comes from a legitimate user. Only after approval and authentication key can be used for encryption or other cryptographic purposes.

The combination of public key cryptography for authentication and quantum key distribution leads to high levels of long-term security.

6. ESTIMATION OF THE REDUCING OF KEY RATE GENERATION AT THE PHYSICAL LEVEL

Efforts of developer of quantum cryptography systems are concentrated on increase the key rate, increase the communication range, exclusion the probability of hack the system through quantum channel.

One of the main limitations of commercial systems produced by id Quantque, MagiQ Technologies and Quintessence Labs companies are a low rate of the secret key generation (Golubchikov, & Rumiantsev, 2008). So for the system id 3100 Clavis2 rate of raw key sequence is 500 bps at the length of the quantum channel 25 km (Dixon, Yuan, Dynes, Sharpe, & Shields, 2010).

Using the generalized structure of QKD systems (Figure 10) and the model of information security infrastructure (Figures 11-15) we estimate the influence of each stage on a rate of key generation.

Infrastructure of information security for quantum key distribution provides the physical and logical levels of the key generation. The physical layer includes the optical pulse generation by OTM, optical pulse transmission from Alice station to station Bob, the weakening of the power of optical pulse to the level of the photonic pulse, the phase coding of states of photons, the photonic pulse transmission from station Alice to station Bob, the choice of measurement basis of the photon states, the detection of photons in the receiver modules ROM-B1 and PROM-B2 in Bob stations (Figure 10).

Let the OTM in the generalized structure of QKD systems in Figure 10 generates optical pulses with energy E_{OTM}, repetition rate of f_{OTM} and duration of τ_{OTM}. This is equivalent to generating an average duration of an optical pulse of photons:

$$\mu_{OTM} = \frac{\mathrm{E}_{OTM}}{\mathrm{E}_{ph}} = \frac{\mathrm{E}_{OTM}}{hc_{opt} \big/ \lambda_{opt}}. \tag{2}$$

The photon energy $\mathrm{E}_{ph} = hc_{opt} \big/ \lambda_{opt}$ is determined by Planck constant $h = 6,628 \times 10^{-34} J \cdot s$, wavelength λ_{opt} and the velocity of propagation c_{opt} of optical radiation.

The optical pulse is attenuated while pass through component of QKD system. The average number of photons per pulse absorbed at the photocathode of one of the two-SPAD

$$\mu_{APD} = K_{\text{B}} \cdot K_{\text{A}} \cdot K_{\text{link}} \cdot \mu_{OTM} \tag{3}$$

In accordance to Figure 10 μ_{APD} is determined by the losses of FOL K_{link}, the attenuation K_{B} of the fiber-optical structures of Bob station (VOA-B, FOC, FC X-type, FODL-B, PM-B, the polarization rotator, PFC) and K_{A} of Alice station (FC Y-type, VOA-1, FODL-A, PM-A, Faraday mirror). When the FOL uses optical fiber with length of L_{FOL} and linear attenuation of the radiation, so losses can be calculated by

$$K_{\text{link}} = \exp\left(-\alpha_{\text{OF}} \cdot L_{\text{link}}\right). \tag{4}$$

The security condition of the QKD system is re-emission in the direction of the Bob station photonic pulse. Quantum key distribution system is configured so that each photonic pulse consists on average no more than one photon. In such conditions, the probability of receiving n_{ph} photons per pulse while strobe duration $\tau_{strobe} > \tau_{\text{OTM}}$ in receiving optical modules ROM-B1 and ROM-B2 of Bob station and the average of number of photon μ_{ROM} has the Poisson distribution (Bychkov, & Rumiantsev, 2000)

$$\Pr\left\{n_{ph} \middle| \mu_{\text{ROM}}\right\} = \frac{\mu_{\text{ROM}}^{n_{ph}}}{n_{ph}!} \exp\left(-\mu_{\text{ROM}}\right). \tag{5}$$

In quantum cryptography photonic pulse mean that $\mu_{\text{ROM}} = 0.1..\ 0.2$. Then, for $\mu_{\text{ROM}} = 0.1$ the proportion of pulses at the input of ROM with two photons is 0.45%, and three photons is 0.015%. Almost 9 out of 10 gated intervals will not contain any photons.

The average number of click of SPAD is

$$\mu_{APD} = \eta_{APD} \cdot \mu_{\Pi POM} + \nu_{\text{dark}} \cdot \tau_{strobe} \tag{6}$$

determined by the quantum efficiency of SPAD η_{APD}. The second summand in (6) is associated with the pulses of the dark current and afterpulsing effect. We assume that it frequency is ν_{dark}.

It is known that the quantum efficiency of existing SPAD at 1550 nm does not exceed 10% (Gisin, Ribordy, Tittel, & Zbinden, 2002; Dusek, Lutkenhaus, & Hendrych, 2006). Consequently, the average number of detected photons will not exceed $\mu_{\text{APD}} = 0.01..\ 0.02$. In this case, using the formula

$$\Pr\left\{n \middle| \mu_{\text{APD}}\right\} = \frac{\mu_{\text{APD}}^{n}}{n!} \exp\left(-\mu_{\text{APD}}\right), \tag{7}$$

we find that the proportion of gated intervals in which received two or more photons do not exceed 0.005%. The proportion of pulses where there will be no photons increases to 99%.One photon is detected in 0.99% pulses.

Due to sifting stage will be excluded gated intervals in which the photons are not detected. Due to this, the rate of key sequence generation decrease to values

$$V_1 = \left[1 - \exp\left(-\mu_{\text{APD}}\right)\right] \cdot f_{\text{OTM}}. \tag{8}$$

Since the value $V_0 = f_{\text{OTM}}$ can be interpreted as the maximum rate of key distribution, so

$$K_1 = \left[1 - \exp\left(-\mu_{\text{APD}}\right)\right] \tag{9}$$

is the factor of slowing the rate of key sequence generation because the photon is not detected.

At the sifting stage can occur simultaneously click of two ROM. Moreover, click one of the two ROM is associated with the pulses of the dark current and afterpulsing effect.

Because this response are not correlated the probability of such event according to (6) and (7) will be

$$\begin{gathered}\Pr\left\{n \geq 1 \middle| \mu_{\text{APD}}\right\} \Pr\left\{n \geq 1 \middle| \nu_{\text{dark}} \tau_{strobe}\right\} = \\ \left[1 - \Pr\left\{n = 0 \middle| \mu_{\text{APD}}\right\}\right] \cdot \left[1 - \Pr\left\{n = 0 \middle| \nu_{\text{dark}} \tau_{strobe}\right\}\right] = \\ = \left[1 - \exp\left(-\mu_{\text{APD}}\right)\right] \cdot \left[1 - \exp\left(-\nu_{\text{dark}} \tau_{strobe}\right)\right].\end{gathered}$$

After exclusion the positions in the key sequence in which the double click of ROM is occur, the rate of key generation decrease by

$$V_2 = \left[1 - \exp\left(-\mu_{\mathrm{APD}}\right)\right] \cdot \left[1 - \exp\left(-\nu_{\mathrm{dark}} \tau_{strobe}\right)\right] \cdot V_1. \tag{10}$$

According to (10) the factor of slowing the rate of key sequence generation from double click of ROM is

$$K_2 = \left[1 - \exp\left(-\mu_{\mathrm{APD}}\right)\right] \cdot \left[1 - \exp\left(-\nu_{\mathrm{dark}} \tau_{strobe}\right)\right]. \tag{11}$$

Commercial QKD systems (Golubchikov, & Rumiantsev, 2008) using the protocols BB84 and SARG04. To implement the protocol BB84 (Gisin, Ribordy, Tittel, & Zbinden, 2002) at the station Alice delayed optical pulse is modulated in phase by one of four randomly selected values Φ_A the series 0, π/2, π, 3π/2. At the Bob station randomly selected measuring basis Φ_B of the phase shift of the first photon pulse by 0 or π/2.

The probability of a correct choice of the basis is defined as the Equations shown in Box 1.

In a perfectly tuned QKD system that probability is that shown in Box 2.

Consequently, due to the mismatch bases of Alice and Bob in the implementation of the BB84 protocol every second bit of the key sequence will be rejected. The rate of the key sequence generation reduce by the value

$$V_3 = \mathrm{Pr}_{bc}\, V_2. \tag{12}$$

The expression shows that the probability of a correct choice of basis Pr_{cb} can be interpreted as a factor of reducing the length of the key sequence of bits by $\mathrm{Pr}_{cb} = K_3 = 0.5$ at the sifting stage as the result of the mismatch measuring bases on stations Alice and Bob.

Note that the coefficient in (12) $\mathrm{Pr}_{cb} = K_3$ is 0.25 when the B92 protocol is use.

In a real QKD system factor of slowing of key sequence generation as the result of the mismatch bases in Alice and Bob is that shown in Box 3.

An analysis of Formulas (2)-(7) and (14) shows that the rate of reduction $K_{\mathrm{ph.level}} = K_1 \cdot \mathrm{K}_2 \cdot \mathrm{K}_3$ of length of key sequence of bits on sifting stage is defined by:

- The energy E_{OTM}, repetition rate f_{OTM} and duration of optical pulses τ_{OTM},

Box 1.

$$\mathrm{Pr}_{bc} = \mathrm{Pr}\left\{\Phi_{\mathrm{A}} = 0,\, \Phi_{\mathrm{B}} = 0\right\} + \mathrm{Pr}\left\{\Phi_{\mathrm{A}} = \pi/2,\, \Phi_{\mathrm{B}} = \pi\,/\,2\right\} +$$
$$\mathrm{Pr}\left\{\Phi_{\mathrm{A}} = \pi,\, \Phi_{\mathrm{B}} = 0\right\} + \mathrm{Pr}\left\{\Phi_{\mathrm{A}} = 3\pi/2,\, \Phi_{\mathrm{B}} = \pi/2\right\}.$$

where $\mathrm{Pr}\left\{\Phi_{\mathrm{A}},\, \Phi_{\mathrm{B}}\right\} = \mathrm{Pr}\left\{\Phi_{\mathrm{A}}\right\} \cdot \mathrm{Pr}\left\{\Phi_{\mathrm{B}}\right\}$

Box 2.

$$\mathrm{Pr}\left\{\Phi_{\mathrm{A}} = 0\right\} = \mathrm{Pr}\left\{\Phi_{\mathrm{A}} = \pi/2\right\} = \mathrm{Pr}\left\{\Phi_{\mathrm{A}} = \pi\right\} = \mathrm{Pr}\left\{\Phi_{\mathrm{A}} = 3\pi/2\right\} = 0{,}25$$
$$\mathrm{Pr}\left\{\Phi_{\mathrm{B}} = 0\right\} = \mathrm{Pr}\left\{\Phi_{\mathrm{B}} = \pi/2\right\} = 0{,}5$$

whence $\mathrm{Pr}_{bc} = 0{,}5.$

Therefore, as a result of the error correction the rate of the key sequence generation is reduced in K_{cor1} times, where

$$K_{\mathrm{cor1}} = \frac{N_{general} - N_{cor1}}{N_{general}} = \frac{N_{err.cor} + N_{cor0}}{N_{general}}. \tag{22}$$

With (19)-(21) we find the average length of the consistent key sequence after error correction stage

$$\overline{N_{cor1}} = \sum_{N_{cor1}} N_{cor1} \Pr\left\{N_{cor1}\right\}$$

where $\Pr\left\{N_{cor1}\right\}$ is the probability of consistent key sequence of length N_{cor1} after error correction stage.

Since the cascade algorithm of error correction is not deterministic, the number of disclosed bits N_{cor1} depends on the amount of mutual information $I\{A,B \mid E\}$ of Alice and Bob taking into account the Eve actions. The amount of information available to Eve is determined after the error correction and estimated as error rate in the approved key sequence.

There is a nonzero probability that number of errors found in key sequence of length $N_{general}$ exceeds a critical limit $\Pr_{err.general.ad} = 11\%$. Thus, it is necessary to take into account the probability of exception of all approved key sequence $N_{general}$ if a probability of error $\Pr_{err.general} = N_{err.cor} \big/ N_{general}$ is more than the maximum threshold $\Pr_{err.general.ad}$.

Let $N_{cr} = \left\lfloor N_{general} \cdot \Pr_{err.general.ad} \right\rfloor$ is a critical quantity of errors in the key sequence of length $N_{general}$ bit. The sign $\lfloor x \rfloor$ means the greatest integer not exceeding this real x. Then

$$\Pr_{err.general} = \Pr\left\{N_{err.cor} \geq N_{cr}\right\} = \sum_{N_{err.cor}=N_{cr}}^{N_{general}} \Pr\left\{N_{err.cor}\right\}.$$

In this case all approved key sequence of $N_{general}$ length is excluded. OTM generates a new train of N_0 optical pulses. Naturally, the length of the new approved key sequence and critical errors in it will be different.

Let z_2 is the number of the current generation cycle of train of optical pulses. Then the error

Box 7.

$$\Pr_{err.general.z2} = \Pr\left\{N_{err.cor.z2} \geq N_{cr.z2}\right\} = \sum_{N_{err.cor}=N_{cr.z2}}^{N_{general.z2}} \Pr\left\{N_{err.cor.z2}\right\}. \tag{23}$$

Box 8.

$$K_{\mathrm{rej}} = \sum_{z_2 \geq 1} \left(1 + \frac{\left(z_2 - 1\right) N_0}{N_{cor1.z2}}\right) \Pr_{err.general.z2} \left(1 - \Pr_{err.general.z2}\right)^{z_2 - 1}. \tag{24}$$

Consequently, the number of bits disclosed in all $N_{block.i} = N_{block} \cdot 2^{1-i}$ blocks size of $n_{block.i} = n_{block} \cdot 2^{i-1}$ during *i*-th step is equal to

$$k_i = m_i\left(1 + \log\left(n_{blocki}\right)\right) = m_i\left(i + \log\left(n_{block}\right)\right). \tag{18}$$

The error probability at each next step is reduced (Brassard, & Salvail, 1993).

Iterative procedure includes N_{step} steps of searching and correcting single errors. The $k_i,\ i = \overline{1, N_{step}}$ is the value of the cost of error correction in the key sequence at the *i*-th step. Note that according to (18) the cost of correction of one error in a block at each next step increases by 1 bit.

Iterative procedure ensures reduction of errors at each next step, i.e. $\lim\limits_{i \to \propto} m_i = 0$. In this case the best solution is to remembering the location of bit positions in the blocks where single errors detected in the previous steps. This minimizes the number of disclosed bits.

The resulting number of disclosed $N_{err.cor}$ bits in the approved key sequence after the parity check is that shown in Box 4.

If the key sequence has no errors, then only one bit will be disclosed in each block. Number of blocks at the *i*-th step. In which no single errors detected is equal

$$k_{0i} = N_{block.i} - m_i = N_{block} \cdot 2^{1-i} - m_i.$$

Consequently, after the parity check will be dropped an additional bits (see Box 5).

The length of the consistent key sequence after the error correction will be that shown in Box 6.

Box 4.

$$N_{err.cor} = \sum_{i=1}^{N_{step}} k_i = \sum_{i=1}^{N_{step}} m_i\left(i + \log n_{block}\right) = \sum_{i=1}^{N_{step}} i \cdot m_i + \log n_{block} \sum_{i=1}^{N_{step}} m_i. \tag{19}$$

Box 5.

$$\begin{gathered} N_{cor0} = \sum_{i=1}^{N_{step}} k_{0i} = \sum_{i=1}^{N_{step}}\left(N_{block} \cdot 2^{1-i} - m_i\right) = \\ N_{block}\sum_{i=1}^{N_{step}} 2^{1-i} - \sum_{i=1}^{N_{step}} m_i = N_{block}\left(2 - 2^{1-N_{step}}\right) - \sum_{i=1}^{N_{step}} m_i. \end{gathered} \tag{20}$$

Box 6.

$$\begin{gathered} N_{cor1} = N_{general} - N_{err.cor} - N_{cor0} = \\ N_{general} - \sum_{i=1}^{N_{step}}\left(i-1\right) \cdot m_i - \log n_{block}\sum_{i=1}^{N_{step}} m_i - N_{block}\left(2 - 2^{1-N_{step}}\right). \end{gathered} \tag{21}$$

removed from the key sequence after the end of correction process. So the key sequence in the process of error correction reduces its length.

The process of iterative error correction has the following operations: the division into blocks, parity check, error correction, permutation of sequence. Permutation operation is performed for uniform distribution errors per blocks.

Let the approved key sequence length is N_{general} and quantity of errors is k_{err}. The probability of this event is defined by

$$\Pr\left\{k_{err}\right\} = C_{N_{general}}^{k_{err}} p_{bit}^{\ k_{err}} \left(1 - p_{bit}\right)^{N_{general} - k_{err}} \tag{16}$$

At the first step of cascade algorithm the sequence is divided into the blocks $N_{block1} = N_{block}$ of $n_{block1} = n_{block}$ bits in each, and

$$n_{block} \geq \frac{\alpha}{p_{bit}},$$

where the constant α = 0,73 is determined empirically(Brassard, & Salvail, 1993).

Note that in practice for implementation of the algorithm the length of the block n_{block} is selected multiple of two, i.e. $n_{block} = 2^k$. Consequently, the parameter of block length must satisfy the condition

$$k = \left\lceil \log\left(\frac{\alpha}{p_{bit}}\right) \right\rceil. \tag{17}$$

The sign $\lceil x \rceil$ in (17) means the smallest integer no less than a real x.

The error will be distributed in blocks uniformly after the permutation if the condition (17) is performed.

Error bits are statistically independent. Therefore, the appearance of error in any of the blocks of length n_{block} is uniformly.

Consequently, single-errors should be detected and corrected at the first step as the most probable errors.

Therefore. In each block of N_{block} check the parity, which detects a single-error by bisectional search method.

Let an odd number of errors detected in m_1 blocks on the first step.

In the process of correcting the quantity of disclosed bits in the key sequence is calculated as

$$k_1 = m_1 \cdot (1 + \log(n_{block1})) = m_1 \cdot (1 + \log(n_{block})).$$

After the first step will be $k_{err} - m_1$ errors. With increasing a priori probability of single errors increases the number of detected and corrected errors at the first step.

The block size is doubled $n_{block2} = 2n_{block1}$ after permutation at the second step. The operation of permutation is performed and single errors is correcting in double sized blocks.

Consequently, if the number of blocks with a single error at the second step is equal to m_2, then the number of bits disclosed in a key sequence is

$$k_2 = m_2\left(1 + \log\left(n_{block2}\right)\right) = m_2\left(2 + \log\left(n_{block}\right)\right).$$

In the second step corrects double errors, which at the first step was in one block.

The number of errors after the second step further reduced to m_2 and becomes equal to $k_{err} - m_1 - m_2$ errors.

Double errors of the second step will correct at the third step, with an increase of the cost of error correction at 1 bit.

Box 3.

$$K_3 = \mathrm{Pr}_{bc} = \left(\Pr\{\Phi_{\mathrm{A}} = 0\} + \Pr\{\Phi_{\mathrm{A}} = \pi\}\right)\cdot \Pr\{\Phi_{\mathrm{B}} = 0\} + \left(\Pr\{\Phi_{\mathrm{A}} = \pi/2\} + \Pr\{\Phi_{\mathrm{A}} = 3\pi/2\}\right)\cdot \Pr\{\Phi_{\mathrm{B}} = \pi \,/\, 2\}. \qquad (13)$$

The expression (8)-(13) allow us to calculate general expression for the rate of the sifted key sequence generation after the second stage(13)

$$V_{\mathrm{ph.level}} = K_1 \cdot \mathrm{K}_2 \cdot \mathrm{K}_3 \cdot f_{\Pi OM}. \qquad (14)$$

- The length L_{link} of FOL and linear attenuation α_{OF} of the optical fiber,
- The duration gating pulses τ_{strobe} in optical receiver modules ROM-B1 and ROM-B2,
- The SPAD parameters such as quantum efficiency η_{APD}, frequency of dark current pulses and afterpulsing effects ν_{dark},
- The precise of phase shifts in PM-A and PM-B,
- The protocol of quantum key distribution.

7. ESTIMATION OF THE REDUCING OF KEY RATE GENERATION AT THE LOGICAL LEVEL

Logic level carry out the generation of approved, consistent and the secret key sequences of bit (Figures 13-15).

Approved the key sequence generation: Let the error estimates for the selected subset of N_{control} bits in the sifted key sequence length N_{sift}. If the measured error in a subset of $\varepsilon_{err}\left\{N_{control}\right\}$ does not exceed a target level ε_{task}, i.e. $\varepsilon_{err}\left\{N_{control}\right\} < \varepsilon_{task}$, then a key sequence is approved. Let the probability of this event is $P_{\mathrm{task}} = \Pr\left\{\varepsilon_{err}\left\{N_{control}\right\} < \varepsilon_{task}\right\}$.

Approved sequence is formed by elimination of subsets N_{control} from sifted sequences of bits. In the event of $\varepsilon_{err}\left\{N_{control}\right\} \geq \varepsilon_{task}$ then excluded all the N_{sift} bits.

Therefore, an evaluation of the probability of error rate of a key sequence generation is reduced in K_4 time, where

$$K_4 = \sum_{z_1 \geq 1} \left(\left(\mathrm{z}_1 - 1\right) N_0 + \frac{N_{\mathrm{sift.z1}} - N_{control}}{N_{\mathrm{sift.z1}}} P_{\mathrm{task}} \left(1 - P_{\mathrm{task}}\right)^{z_1 - 1} \right). \qquad (15)$$

Here z_1 is the number of the current cycle of generation of OTM train of N_0 optical pulses.

Error correction: At the 4-th stage as the result of error correction in approved key sequences are searched and corrected wrong values of the bits.

In (Brassard, & Salvail, 1993) proposed a cascade algorithm for errors correction in the approved key sequence. This method allows to correcting errors in the sequences with the percentage of errors up to 15%. The cascade algorithm for error correction based on the calculation of the parity of individual blocks. The approved key sequence is divided into that blocks.

In the process of error correction of the approved key sequence length N_{general} Alice and Bob stations exchange the information about the parity data blocks over open channel. Bit corrects the value if an error is detected. The error bit is

CONCLUSION

Based on the analysis of existing commercial systems produced by id Quantique (Switzerland), MagiQ Technologies (USA) and Quintessenc Labs Pty Ltd (Australia) proposed the generalized structure of the QKD systems with phase coding of photon states. The structure includes all the modules that have a direct influence on the propagation and processing of quantum states.

The stages of the raw, sifted, approved, consistent and secret key sequences are analyzed. Combining the block-diagrams of five stages of key sequences generation provides the Model of information security infrastructure with quantum key distribution.

The expressions (1)-(27) establish the dependence of length of secret key sequence to the parameters of the transmitter and receiver modules, optical fiber, the duration of gate pulses, the precision of the phase shifts, protocol of key distribution, the allowable level of bit-error probability, the iterative algorithm of error correction and size of the hash function on the stage privacy amplification.

As an example shows that the use of QKD model allows to estimate the reduction rate of key sequence generation at the stages of error correction and privacy amplification.

REFERENCES

Advanced Encryption Standard (AES). (2001). *National institute for standards and technology*. Gaithersburg, MD: AES.

Bennett, C. (1992). Quantum cryptography using any two non-orthogonal states. *Physical Review Letters*, *68*, 3121–3124. doi:10.1103/PhysRevLett.68.3121 PMID:10045619.

Biham, E., Boyer, M., Boykin, P. O., Mor, T., & Roychowdhury, V. A. (n.d.). *Proof of the seurity of quantum key distribution.* Retrieved from http://arxiv.org/abs/quant-ph/9912053v1

Bouwmeester, D., Ekert, A. K., & Zeilinger, A. (2000). *The physics of quantum information: Quantum cryptography, quantum teleportation, and quantum computation*. Berlin: Springer.

Brassard, G. (2007). *Modern cryptology: A tutorial*. New York: Springer-Verlag.

Brassard, G., & Salvail, L. (1993). Secret-key reconciliation by public discussion: Advances in cryptology. In *Proceedings of Eurocrypt '93*. Lofthus, Norway: IEEE Press.

Bychkov, S. I., & Rumiantsev, K. E. (2000). *Search and detection of optical signals*. Moscow, Russia: Radio and Connection Publisher.

Center for KvanteInformatik. (n.d.). *Implementation of the B92 QKD protocol.* Retrieved from www.cki.au.dk/experiment/qrypto/doc/QuCrypt/b92prot.html

Dixon, A. R., Yuan, Z. L., Dynes, J. F., Sharpe, A. W., & Shields, A. J. (2010). Continuous operation of high bit rate quantum key distribution. *Applied Physics Letters*. doi:10.1063/1.3385293.

Dusek, M., Lutkenhaus, N., & Hendrych, M. (2006). Quantum cryptography. *Progress in Optics*, *49*, 381–454. doi:10.1016/S0079-6638(06)49005-3.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*, 145–195. doi:10.1103/RevModPhys.74.145.

Golubchikov, D. M. (2008). Structure and operation principles of Id 3000 Clavis system. *Proceedings of the South Federal University Technical Sciences*, *3*(80), 149–157.

Golubchikov, D. M., & Rumiantsev, K. E. (2008). Quantum cryptography: Principle, protocol, system. *All-Russian competitive selection analytical survey in priority guidelines of information and telecommunication systems.* Retrieved from http://www.ict.edu.ru/ft/005712/68358e2-st14.pdf

Figure 17. The dependence of the rejection coefficient to the bit-error probability

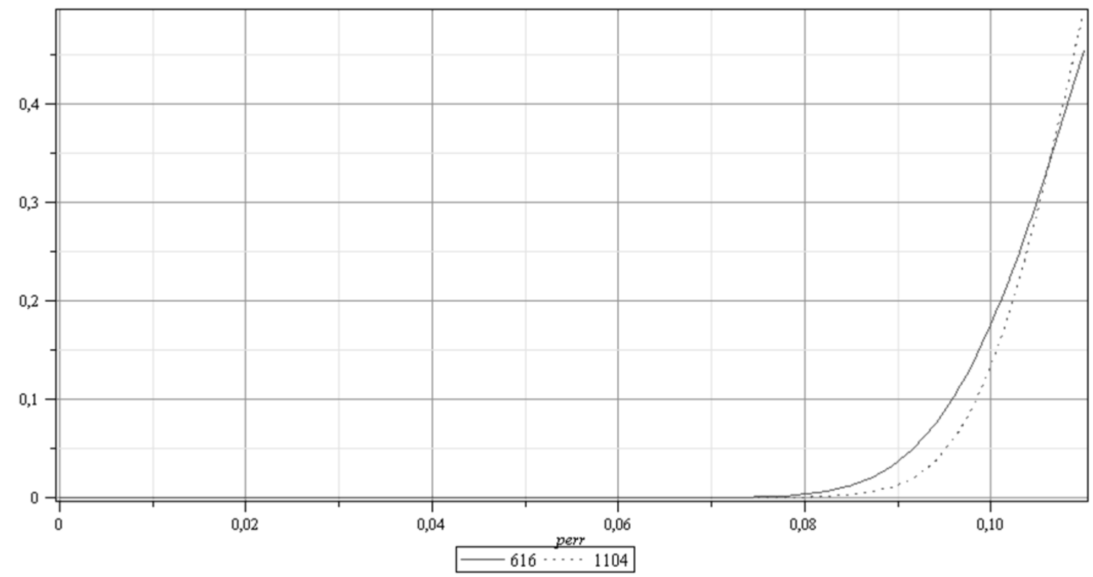
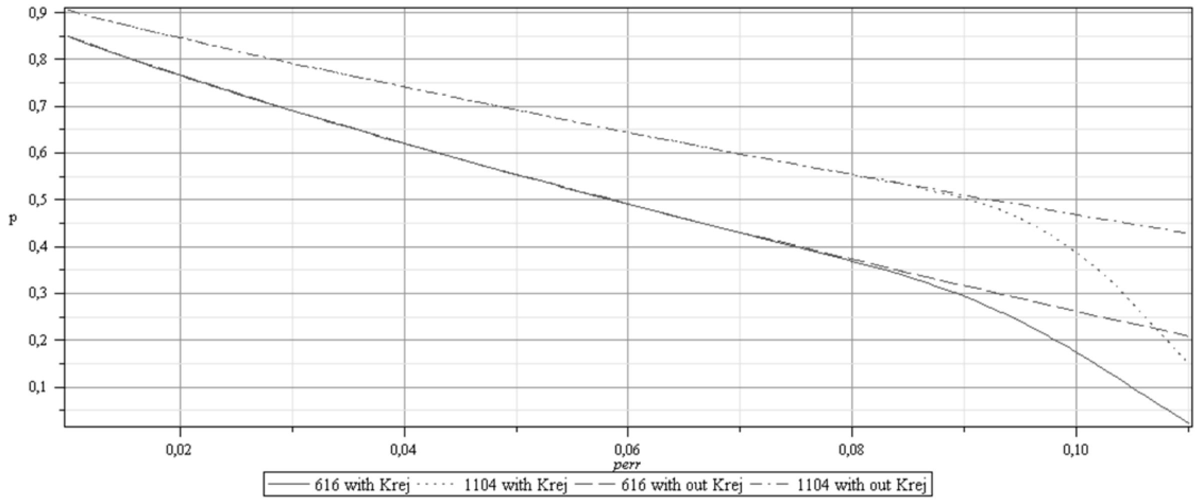


Figure 18. The probability of generation one private key bit to one sifted key bit



of bit-error probability in sifted key without the rejection coefficient taken into account. If the rejection coefficient is taken into account, within range of the bit-error probability of 0..9% the rate of key generation is similar to the case without the rejection coefficient considered, but within range of the bit-error probability of 9..11% the rate of key generation decreases by average of 17.5% per one percent of bit-error probability for 1104 bits sifted key. The safety factor *s* is the main parameter that determines the difference between decreases of rate of generation of different length keys.

An additional analysis needs to determine the optimal values of the security factor *s* with relation to values of P_{bit}

Total decrease of the rate of private key generation is 98% and 86% for the 616 and 1104 bits sifted key length respectively, with the bit-error probability value close to 11%.

tion and privacy amplification stages on the key distribution process.

As an example of the developed model, we estimate the length of the sifted key sequence required to generate secret keys with lengths of 128, 192 and 256 bits. These lengths are typical for the algorithm AES used in commercial quantum cryptography.

The length N_{sift} of sifted key sequence is estimated with expression (27) with no account taken of stage of generation of approved key sequence $(\varepsilon_{task} = 0)$.

The curves on Figure 16 show that more than 158 bit sifted key N_{sift} is needed to generate $N_{\text{secret}} = 128$ bit private key with safety factor $s = 30$ and bit-error probability $P_{bit} = 0$ conditions, but the sifted key N_{sift} should be more than 610 bits if safety factor $s = 30$ and bit-error probability $P_{bit} = 0.11$. The 256 bit private key generation demands 1104 bits of sifted key length with bit-error probability $P_{bit} = 0.11$. The 610 and 1104 bits values define the least upper limit of sifted key length used for estimation of sifted key rejection coefficient K_{rej}.

The further quantitative analysis uses length of sifted key that is divisible by 8 bits. This assumption is needed in order to use the computational modeling.

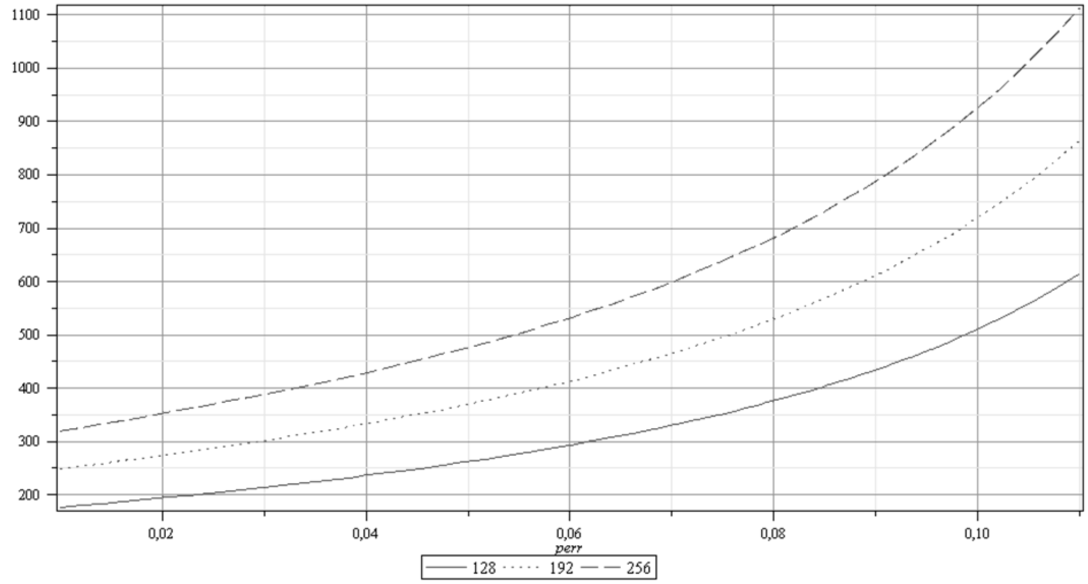
Let's estimate the coefficient of rejection of sifted key if it has eavesdropper known bits quantity of more than the critical limit.

The curves on Figure 17 show that if the bit-error probability P_{bit} is high the coefficient of rejection is high too and may reach value of 0.5. This fact means that every second key will be rejected completely.

The curves on Figure 18 show the dependence of the probability of generation of one private key bit from one sifted key bit to the bit-error probability. The figure also shows the influence of rejection coefficient K_{rej}.

From the dependences in Figures 16–18 found that for the range of parameters appropriate to Id3100 Clavis2 commercial system we can state that the error correction stage decreases the rate of key generation average on 3.9% per one percent

Figure 16. The dependence of sifted key length to the error probability



Box 9.

$$K_6 = \sum_{z_3 \geq 1} \frac{\left(z_3 - 1\right) N_0 + N_{hash.z3} - N_{priv}}{N_{cor.z3}} p_0 \left(1 - p_0\right)^{z_3 - 1}. \qquad (26)$$

probability in z_2 generation cycle is that shown in Box 7.

The rate of key sequence generation is reduced in the K_{rej} time, where Equation (24) in Box 8.

Taking into accountant (22)–(24) the resulting factor reducing the length of key sequence during the error correction is

$$K_5 = K_{cor1} \cdot K_{rej}. \qquad (25)$$

After the error correction in the approved key sequence formed a consistent key sequence of bits $N_{\text{cor}} = N_{\text{cor1}} - N_{\text{cr}}$ length.

It should be remembered that the cascade algorithm for correcting errors has finite and non-zero probability of resulting error because it has the finite number of steps.

Privacy amplification: The transformation (1) building on the matrix Toeplitz is use in quantum cryptography systems at the step of privacy amplification. The dimension of the matrix and the length of the converted sequence is $N_{\text{hash}} < N_{\text{cor}}$.

Alice and Bob check for errors in N_{priv} control bits in the converted sequence. If the selected bits have no errors then the secret key sequence is $N_{\sec ret} = N_{hash} - N_{\text{priv}}$ bits. In the case of $\varepsilon_{err}\left\{N_{\text{priv}}\right\} \neq 0$ all consistent key sequence is excluded and OTM generates a new train of N_0 optical pulses.

Consequently, after the privacy amplification reducing the length of the sequence is given by that shown in Box 9.

Here z_3 is the number of the current cycle of generation of train of N_0 optical pulses. The value $p_0 = \Pr\left\{\varepsilon_{err}\left\{N_{\text{priv}}\right\} = 0\right\}$ is the probability of no errors in the selected N_{priv} bits.

Parameters in (26) are the length N_{cor} of the consistent key sequence, the size N_{hash} of the hash function, the compression option *s*, the amount of Eve known information and the number N_{priv} of control bits.

8. THE RATE OF A SECRET KEY SEQUENCE GENERATION

The resulting reduction of the length of key sequences estimated with accountant to (9), (11), (13), (15), (25) and (26) as coefficient

$$K_{QKD} = K_1 \cdot K_2 \cdot K_3 \cdot K_4 \cdot K_5 \cdot K_6. \qquad (27)$$

Importantly, the decrease of the rate of key sequences generation on all stages is a random process. Where the coefficient $K_1 - K_3$ are the mathematical expectation of random variables. As for the coefficient $K_4 - K_6$ they require averaging over a number of generating cycles of optical pulses trains, the number of blocks with an odd number of errors and some other parameters.

In these circumstances, the union of block-diagrams in Figures 11-15 provides an algorithm for simulating the process of secret key sequence generation. The model allows to estimating the influence of various parameters of physical elements of the QKD system and the error correc-

Hammond, A. (2006). *MagiQ and Verizon smash distance and cost barriers with world's longest cascaded network for practical quantum cryptography. New Technology Enables Ultra Secure Communications*. Business Wire.

Id Quantique. (2011). *Swiss bank encrypts critical low-latency backbone links with the Id Quantique centauris encryptors.* Retrieved from http://www.idquantique.com/news/swissquote.html

Id Quantique, S. A. (2005). Id 3000 Clavis: Plug & play quantum cryptography. *Specifications, 2.1*. Retrieved from http://www.idquantique.com/images/stories/PDF/clavis2-quantum-key-distribution/clavis2-specs.pdf

Id Quantique, S. A. (2005). Id 5000 Vectis. *Specifications, 1.2.* Retrieved from http://www.idquantique.com/images/stories/PDF/clavis2-quantum-key-distribution/clavis2-specs.pdf

Id Quantique, S. A. (2008). Quantum cryptography. *The Key to Future-Proof Confidentiality, 3.1*. Retrieved from http://www.idquantique.com/images/stories/PDF/clavis2-quantum-key-distribution/clavis2-specs.pdf

Id Quantique, S. A. (2010). *Practical quantum cryptography*. Paper presented at the Session of Second Winter School. New York, NY.

Kilin, S. Y., Nizovtsev, A. P., & Horoshko, D. B. (2007). *Quantum cryptography: Ideas and practice*. Minsk, Belarus: Belaruskaya Nauka.

Kotenko, V. V., & Rumiantsev, K. E. (2009). *Information theory and telecommunication security.* Rostov-on-Don, Russia: SFedU publishers.

MagiQ Technologies, Inc. (2004). QPN 5505. *Reference Manual.*

Mao, W. (2003). *Modern cryptography: Theory and practice*. Upper Saddle River, NJ: Prentice Hall.

Mayers, D. (2001). Unconditional security in quantum cryptography. *Journal of the ACM*, *48*, 351–406. doi:10.1145/382780.382781.

News. (n.d.). Retrieved from http://www.gap-optique.unige.ch

Pauli, D. (2009). Aussie govt considers quantum leap in secure comms. *Computer World.* Retrieved from http://www.computerworld.com.au/article/278658/aussie_govt_considers_quantum_leap_secure_comms/

Ribordy, G., Gautier, J.-D., Gisin, N., Guinnard, O., & Zbinden, H. (2000). Fast and user-friendly quantum key distribution. *Journal of Modern Optics*, *47*, 517–531.

Rumyantsev, K. E. (2010). Quantum communication: Theory, experiments, applications. *Info-Telecommunication and Computer Technology, Equipment, and Systems in South Federal University.* Rostov-on-Don, Russia: SFedU Publishers.

Scarani, V. (2006). *Quantum physics: A first encounter: Interference, entanglement, and reality*. Oxford, UK: Oxford University Press.

Shor, P. W., & Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, *85*, 441–444. doi:10.1103/PhysRevLett.85.441 PMID:10991303.

Singh, S. (2000). *The code book: The secret history of codes and code breaking*. London, UK: Forth Estate.

Smart, N. (2004). *Cryptography: An introduction*. New York: McGraw-Hill College.

Stucki, D., Gisin, N., Guinnard, O., Ribordy, G., & Zbinden, H. (2002). Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics, 4*, 41.1– 41.8.