Quantum Electronics **48** (9) 777–801 (2018)

REVIEW

https://doi.org/10.1070/QEL16732

Quantum cryptography and combined schemes of quantum cryptography communication networks

A.Yu. Bykovsky, I.N. Kompanets

Contents

Abstract. **We discuss cryptographic data protection network schemes combining the approaches of quantum cryptography with advanced computer information processing methods. The use of the latter is due to the presence of a number of unsolved problems in the existing quantum key distribution systems and is also associated with projects for the development of network-centric quantum communications and photonic networks, which involves the employment of multi-agent control models. Developments based on the Y-00 protocol with data encoding by the quantum noise of a transmitting laser are considered, and achievements in the field of quantum-optical random number generators are presented. The latter can be also used to design secure multi-valued logic encoding schemes that are promising for increasing the dimension of the key space in the 'one-time pad' method, for solving the tasks of position-dependent cryptography and for implementing multi-agent models.**

A.Yu. Bykovsky, I.N. Kompanets P.N. Lebedev Physical Institute, Russian Academy of Sciences, Leninsky prosp. 53, 119991 Moscow, Russia; e-mail: ayubykov@sci.lebedev.ru

Received 16 May 2018; revision received 25 July 2018
Kvantovaya Elektronika **48** (9) 777–801 (2018)
Translated by I.A. Ulitkin

Keywords: *quantum key distribution, optical communication, photonic network, network-centric system, fibre-optic communication line, secure encoding, multi-valued (or multiple-valued) logic protected encoding, multi-agent network management system.*

1. Introduction

Much attention to research in the field of quantum cryptography, which has been conducted for more than 30 years, is determined by the importance of data protection in modern communication networks based on fibre-optic communication lines (FOCLs) and quantum optics. A general idea of this subject can be pieced together from a number of early works [1–5], reviews [6, 7, 31–35, 42, 56–70], books [197–204], and educational popular publications [205, 206].

In fact, the term 'quantum cryptography' means [2, 6] the method of confidential quantum key distribution (QKD) between network participants, when the QKD link or network solves the task of a trusted 'courier' to deliver secret keys to subscribers.

In 2016, Journal of Optics [7] published a 'roadmap' for the development of optical communications, where quantum cryptography was included by leading experts in the 17 most cutting-edge areas. Under consideration is the issue of using

QKD schemes in network-centric systems [8–10], which are global computer and communication networks serving critical infrastructure, military equipment and devices for various purposes, including unmanned ground and aerial vehicles. Moreover, QKD schemes are supposed to be employed in photonic (purely optical) networks [11–14]. Interesting experiments have recently been carried out to implement satellite-to-ground and ground-to-sattelite QKD [15–17]. Active research is being conducted abroad and experiments with field (ground-based) multi-user (multi-node and branched) QKD networks have begun in Russia [18–28].

However, the practical implementation of the QKD method in mass communication networks was not as rapid as expected in the early 2000s [29, 30] and faced a number of problems [6, 31–35], a large part of which has not been solved to date. In 2016, the UK's National Cyber Security Centre (NCSC) [36] released a white paper, which outlined a number of fundamental limitations of existing QKD systems and set the direction for priority development of traditional cryptographic systems within the framework of so-called post-quantum cryptography [37, 38].

As follows from the data [39, 40], work on European commercial standards for the QKD equipment has not yet been completed. Also indicative is the fact that the US National Institute of Standards and Technology (NIST), which is the leading developer of commercial standards in the field of communications and cryptography, has so far published methodological materials on QKD at its website [41] only within the framework of the 'Quantum Communications' project and does not include them in the direction of 'cybersecurity'. Of the more than ten known QKD protocols, only the BB84 protocol is presented at the NIST site [2–4, 42]. This indicates that NIST has not yet formulated an open project for mass implementation of the QKD method, leaving it in the status of a promising secure means of communication for a network of quantum computing devices. In 2016, NIST launched a new project for post-quantum, or quantum-resistant cryptography [37, 38], aimed at developing high-security encryption algorithms protected both from conventional and quantum computers. The analysis of patents in the field of QKD [43] also revealed delays in the selection of priorities by a number of key developers.

We should also note B. Schneier's sceptical statements [44] (Schneier is an authoritative expert in the field of computer security) which were published in popular Internet resources and commented on by a reviewer of one of computer websites [45, 46].

The problems that have not been solved so far hamper the wide implementation of the QKD schemes in mass communication networks and complicate the procedures for managing aggregate cryptographic network facilities. This forces the implementation of multi-agent methods [47] that facilitate the simulation of human intellectual functions in key management systems, and also motivates the development of advanced network schemes that combine quantum optics and sophisticated computer data processing techniques [8–12, 48–51].

The above facts served as motivation for writing this review, the purpose of which is:

1) to analyse the factors delaying the long-promised introduction of the QKD schemes into mass telecommunications networks [29, 30];

2) to discuss the reasons that have led to the active development of cryptographic systems based on the Y-00 protocol [48–51], in which the quantum noises of the transmitting laser and traditional encryption methods are used for double encoding of signals transmitted by intense laser pulses;

3) to consider the motivation for the development of network-centric systems and photonic networks [8–14], in which the QKD schemes are integrated into multi-agent cryptographic management systems; and

4) to identify the trends in the development of quantum random-number generators (QRNGs) [52, 53] and the prospects for constructing secure multi-valued logic encoding circuits [54, 55] of high dimensionality on their basis.

For brevity, for some issues we present references to reviews and articles that better correspond to the goals of this work rather than to primary sources.

2. Quantum cryptography

2.1. Basic concepts

The main task of a QKD link [2–4, 6, 32–35, 42, 56–61] is a confidential exchange of a public cryptographic key between two subscribers, usually referred to as Alice and Bob, who keep this key secret from Eve, an eavesdropper. A set of unauthorised actions by Eve, allowing her to partially or completely learn the secret key distributed between Alice and Bob [4, 31, 32, 56, 57, 62], is considered in QKD schemes as an attack. In this case, the peculiarities of schemes, procedures and equipment that facilitate attacking and hacking information by an eavesdropper are called vulnerabilities.

The task of protecting a quantum line from eavesdroppers involves so many issues of quantum optics, computer data processing and information protection that none of the published reviews [6, 7, 31–35, 42, 56–70] covers all aspects of this task. Since the recent review of 2016 by Jain et al. [57] was purposefully devoted to the structure and interconnection of the means used in a quantum line to protect it from adversaries, these issues are only briefly discussed in this paper.

As with any cryptographic system, the basic concepts for QKD schemes are the notions of confidentiality, data integrity and authentication of subscribers, discussed in the literature on information security of computer systems [71, 72] and in reviews [6, 56, 57, 70]. The same basic concept is the no-cloning theorem discussed in [6, 42, 57–59]. The methods for constructing the measurement bases in QKD links are described in detail in [6, 31, 42] and are briefly discussed in [57, 59, 63, 64].

The QKD protocols, which are a connecting link for all components of the quantum line protection system, are discussed to some extent in the reviews [6, 7, 31–35, 42, 58–66, 69]. The most popular BB84 protocol is described in detail in [4, 6, 31, 42, 63], and a brief account of it and several other well-known protocols is presented in [33, 58, 60, 64, 68].

The principles of the BB84 protocol operation, necessary for understanding its aspects, are briefly described in Section 2.3. It also discusses a method for detecting an eavesdropper who measures quantum states in a QKD link [6, 31, 42, 57, 59], which requires the calculation of the quantum bit error rate (QBER).

Section 3.4 discusses possible scenarios of attacks on the components of the QKD link and countermeasures against

them in order to emphasise their difference from the methods of data protection in computer networks presented in Section 3.5. Previously, attack schemes were discussed in detail in reviews [31, 56, 57, 60, 62].

The relationship between the BB84 protocol and the quantum computing network circuits, for the protection of which QKD schemes will be needed in the future, is discussed in detail in a review paper [42] published by NIST in 2002.

2.2. Physical principles of QKD

As a result of a special procedure when Alice and Bob exchange quantum states by means of single photons or attenuated laser pulses (with one or less photons per pulse), both subscribers form two identical random bit sequences, called a 'raw' key. The raw key is further processed by statistical methods, using sifting procedures, error correction and secrecy enhancement [6, 28, 31, 42, 59, 73]. The final key is then used in the cryptographic 'one-time pad' protocol [6, 42, 56, 57, 72, 74], which is guaranteed to be the most secure kind of encoding and implements the perfect (i.e. unbreakable) Vernam cipher that can be only broken by an exhaustive key search, i.e. a brute force attack. The keys can be 'spent' more economically, applying them in less secure encryption techniques, for example, the advanced encryption standard (AES), a symmetric block cipher algorithm chosen in the US as the communication encryption standard [41, 56, 72].

The physical principle of the operation of the QKD schemes is based on the no-cloning theorem (impossibility of creating an identical copy of quantum states) [75], which is founded on the postulates of quantum mechanics [42]. This theorem is often interpreted as the impossibility of non-destructive measurements, as a result of which measurements of the states of qubits (two-level quantum system) secretly performed by Eve in a quantum channel will lead to an increase in the number of errors in the random bit sequence of the key produced by Alice and Bob. The below-discussed increase in the quantum bit error rate QBER [6, 31, 42, 59, 76–81] allows one to establish the fact of eavesdropping.

The inevitable losses of part of the photons in a real atmospheric channel or in a FOCL forced some authors [31] to recognise the inefficiency of the idea of direct communication of secret messages with the help of single photons, which was discussed in early works on QKD. Accordingly, in any modern project, the QKD scheme is integrated with conventional cryptographic protection network facilities.

The procedure for generating a secret key for a pair of subscribers (Alice and Bob) is called the QKD protocol [2–4, 6, 31, 42, 56–60, 62, 63]. The first and most popular QKD protocol, named BB84 after its inventors [2], is shown in Fig. 1 in the form of a scheme with polarisation encoding of light (see Ref. [65]). In contrast to the state of an ordinary bit, the state of the qubit is described by a superposition of the corresponding wave functions [2, 4, 6, 31, 42, 59]. To construct the QKD scheme, it is necessary to use two communication channels: a quantum-optical channel (straight black line in Fig. 1) in the form of a FOCL span or an atmospheric laser line, and an open non-quantum channel (not shown in the figure) realised with the same FOCL or a separate communication link. In the case of using electronic coincidence (or gated) circuits to detect weak optical signals, mandatory clocking of the quantum and non-quantum channels is required [57].

The sender Alice and the receiver Bob use two orthogonal bases (two pairs of polariser axes) to measure four different polarisation states. The first (direct) basis defines the values of 0 and 1 by means of the horizontal (↔) and vertical (↕) polariser axes. The second (diagonal) basis uses the diagonal axes −45° (↘) and +45° (↗) to transmit 0 and 1.

In the process of key distribution, Alice sends single photons along the quantum channel. Each photon can have four possible (↔, ↕, ↘, ↗) polarisation values chosen by Alice with her random number generator. The generated random set of 0 and 1, shown in Fig. 1 in the 'bit

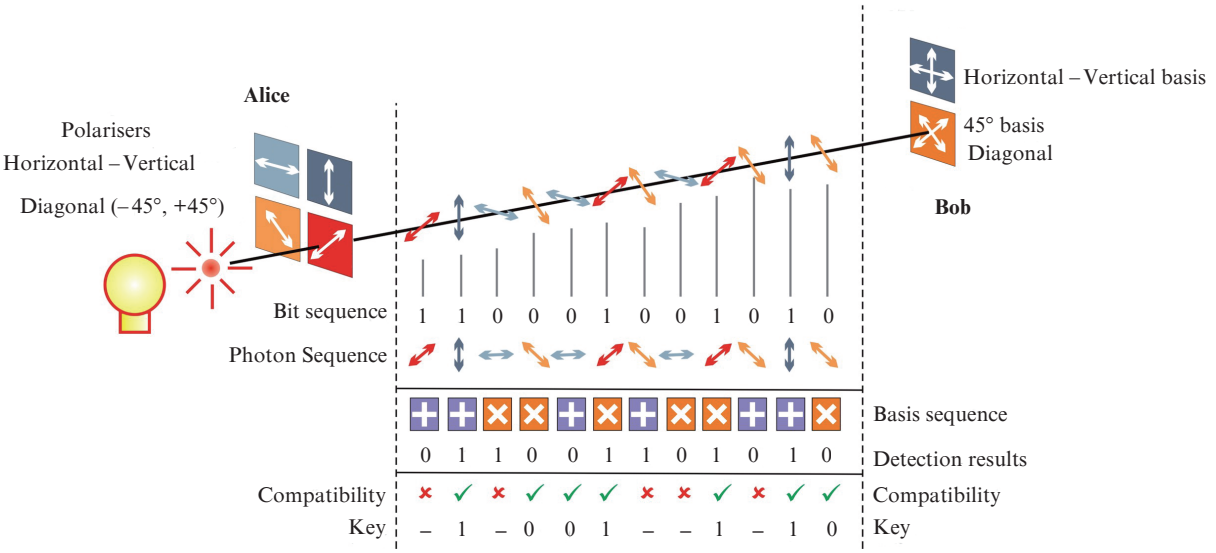

Figure 1. Quantum key distribution system using BB84 Protocol [65].

sequence' line, is encoded by a set of photon polarisations represented in the 'photon sequence' line. Bob measures the polarisation of the received photons, randomly choosing with the help of his random number generator a set of horizontal or diagonal bases indicated by the symbols (+ and ×) in the 'sequence of bases' line. After completing the reception cycle, Bob sends Alice a given sequence of selected bases via a non-quantum channel, and Alice responds to Bob with a sequence of bases used by her. Then they discard those measurement results (indicated by crosses in the 'compatibility' line) for which the bases they used did not match. At the same time, the raw key is shortened and is further called a sifted key consisting of the remaining 0 and 1 shown in the 'key' line.

The sifted key contains a number of errors (Alice's and Bob's bit mismatches) associated with non-removable optical losses in the channel, noise of photodetectors, technical malfunctions and possible interference by an eavesdropper. Therefore, statistical processing procedures are needed to detect an eavesdropper, to correct errors and to amplify the privacy [4, 6, 31, 42, 60, 73, 82]. Eve's attempts to eavesdrop the transmitted data in the quantum link are accompanied by a process of destructive measurements of qubits and by an increase in the total number of errors in the sifted key [2–4, 6, 31, 73, 82]. In this regard, the fact of unauthorised eavesdropping can be detected by checking the number of bit matches for Alice and Bob in a random sample from the sifted key. When an eavesdropper intervenes in the work of a quantum link, Alice and Bob will find an increase in the number of errors compared to the level observed in the absence of Eve.

The above procedure for detecting the fact of illegal eavesdropping of a quantum link is based on calculating QBER and is discussed, for example, in reviews [6, 31, 57, 63]. The QBER, generally expressed as the relative fraction of wrong bits in the detected sequence, can be evaluated as the ratio of the probability of detecting bit errors to the total probability of detection per pulse.

It follows from the theoretical model presented in [76] that, with the use of classical statistical processing algorithms in the procedures of error correction and privacy amplification, an increase in QBER results in a nonlinear decrease in the length of the resulting final key. Among a number of other studies confirming the same nature of the dependence, we can point to a later paper [77], where a detailed analysis of the experimental data obtained for the BB84 protocol was carried out, which was realised in a QKD wavelength division multiplexed link. In this work, theoretical estimates are made of the final secret key rate and the QBER values. In particular, it was clearly shown that one fraction of the bits of the sifted key that was generated per unit of time was discarded during the error correction procedure, while the other fraction of the bits was used for privacy amplification. In this case, each of the fractions of the sifted key, used in its statistical processing, nonlinearly increased with increasing QBER. Eraerds et al. [77] implemented error correction using the well-known CASCADE algorithm and privacy amplification using hashing functions based on Toeplitz matrices.

From the examples presented above, it follows that exceeding a certain threshold value of QBER [6, 63, 76–81, 83] dramatically reduces the secret key rate and forces subscribers to interrupt the communication session or switch to another channel [57]. In this case, the number of detected wrong bits in the QKD quantum channel essentially depends on the protocol used and the parameters of the particular link, and therefore the threshold value of QBER is calculated for a specific protocol [76–81, 84–89].

For the BB84 protocol, Zhao and Li [79] obtained a limiting value of QBER, which was ∼11% and calculated using the concept of entropy within the framework of Shannon's information theory. At the same time, the theoretical model, which took into account the possibility of performing only the so-called individual attacks by Eve (see Section 3.3), made it possible to evaluate the limiting probability of knowledge of a certain key fraction at various stages of its statistical processing by an eavesdropper. The limiting value of QBER, calculated for coherent attacks on the BB84 protocol in [6], was also ∼11%. As emphasised in review [57], the QBER values close to 11% were obtained for BB84 in a number of publications, but the models used in them in most cases did not take into account the real characteristics of laser sources, photodetectors and optical fibres. Therefore, manufacturers of commercial QKD system Clavis2 (ID Quantique, Switzerland) in practice recommended that users work with maximum values of QBER equal to ∼8%.

Considerable attention was paid to the issue of the relationship between the QBER value and the maximum length of the quantum channel [6, 31, 32, 76–81]. Zhao and Li [79] noted that most researchers consider QBER to be a constant, whereas they showed that QBER increases exponentially with increasing transmission distance of the quantum channel. This result was obtained for the BB84 protocol with decoy states (discussed in Section 2.2). A similar character of the dependence of the QBER on the transmission distance of the quantum channel was also justified theoretically in work [80] for the BB84 protocol utilising polarisation encoding of qubits in a wavelength division multiplexed quantum link. However, in the same paper it was shown that for a time-division multiplexed scheme, a regime with a linear growth of QBER is potentially possible with increasing transmission distance (the total length of the FOCL is no more than 200 km). The increase in the length of the quantum link can also be limited by the negative effect of the cross-talks produced by the transmission of quantum signals via a single FOCL along with the usual data signals [80].

It was shown in Refs [81, 83] that the value of QBER depends not only on the optical losses in the link, noise and errors of the photodetector in a specific QKD scheme, but also on uncontrolled external destructive factors and the quality of the QKD link stabilisation system. For example, in [81], the time of stable generation of the final secret key was about 30 min. Consequently, the QBER value in the QKD link must be constantly and carefully controlled by its control system.

Calculations of the final secret key generation rate and the maximum value of QBER are closely related to the theoretical justification of the level of cryptographic resistance (security) of the QKD protocols [6, 31, 57]. This requires the elaboration of a quantum mechanical model that describes the actions of Alice, Bob and Eve, and also evaluates how successfully error correction and privacy amplification proce-

dures allow the part of the key that could become known to the eavesdropper to be reduced to a negligible value [6, 31–33, 57, 59, 78–81, 86, 87]. To this end, in cryptographically secure models discussed, for example, in [33, 78], expressions were obtained for estimating the parameter ε characterising the measure of the deviation of the key distribution from the random one and determining the probability that the eavesdropper knows a certain part of the key after the protocol procedures are completed.

A separate problem is the correct description of the actual noise level and optical losses in optical fibre, account for the probability of false operations of single-photon detectors and also allowance for the non-optimal alignment of modulators in the optical scheme [57, 76–81, 87–99]. It should also be taken into account that several different cryptographic models can theoretically be substantiated for the same protocol [6, 89].

When constructing theoretical models of QKD protocols, developers first of all try to justify the unconditional security of the cryptographic protocol, which does not depend on the computing power of the eavesdropper [6, 31, 32, 84, 88]. The authors of reviews [32, 57] paid special attention to such an important issue of theoretical analysis of cryptographic security, as accounting for the finite length of a real key in models originally constructed on the assumption of an infinite key length [84, 90]. Research is also being conducted on other complex issues, such as the correctness of the estimates of the cryptographic strength obtained in describing the process of measuring a signal with the help of a projector (operator) in a Hilbert space of small dimension [91]. Nevertheless, there is no yet a sufficiently comprehensive and unambiguously interpreted set of methods for the theoretical evaluation of the security level of QKD schemes, the need for which was pointed out by Scarani and Kutsiefer [32].

2.3. Varieties of QKD protocols

The BB84 protocol (1984) still remains the most popular one [2–4]. Apart from it, there are more than ten other QKD protocols that are discussed, for example, in [6, 31, 34, 35, 60, 64, 68]. This protocol utilising phase and polarisation encoding of qubits was used in most of the projects of the field QKD networks, as can be seen from Table 1 in Section 2.5. The most common version of BB84 is a protocol with decoy states [92]. In this case, the transmitted sequence of attenuated laser pulses are combined with false pulses containing a randomly given number of photons (usually $\sim$1 photon per pulse). This makes it possible to distort randomly the statistics of the number of photons in a quantum channel, which is necessary for an eavesdropper to perform attacks using beam-splitting elements [31]. For such a protocol, a long transmission distance of guaranteed secure QKD is theoretically justified [33].

The BB92 (1992) and SSP (1999) protocols differ from BB84 primarily by the number of bases used and the application of two and six quantum states for the encoding of the qubits, respectively [31]. It was noted in [64] that the SARG04 protocol (2004) differs from the BB84 mainly by the encoding procedure designed to counteract photon splitting number attacks. The differences in the procedures used by the KMB09 (2009) and S13 (2013) protocols in the quantum and non-quantum channels, from the similar procedures of BB84, are briefly commented.

In the widely known differential phase shift (DPS) protocol (2003) analysed in detail in [93], the information about the key is encoded into the relative phase difference of the coherent states in each neighbouring premise. Alice's laser works in the regime of mode phase locking and produces a series of phase-locked pulses. The modulator generates a sequence of attenuated laser pulses of equal intensity, separated by identical time intervals. In this case, all the pulses in different premises are mutually coherent, i.e., the frequency 'packing' has the same phase. Then the phase modulator either changes the phase, $|\alpha\rangle \rightarrow |-\alpha\rangle$, or leaves it unchanged, depending on the need to transmit 0 or 1. To receive signals, Bob uses an asymmetric (unbalanced) Mach–Zehnder interferometer.

The so-called coherent one way (COW) protocol (2004) discussed in detail in Refs [19, 94], originated on the basis of DPS and uses amplitude modulation of sequences of mutually coherent laser pulses of equal intensity, separated by identical time intervals. At the same time, 0 is encoded by a sequential transmission of a pair of 'vacuum level–coherent state' pulses, and 1 is transmitted by sending a pair of 'coherent state–vacuum level' pulses. Signals are also recorded by an asymmetric Mach–Zehnder interferometer.

The main disadvantage of the DPS and COW protocols is the insufficient level of theoretical substantiation of their cryptographic strength [57].

In recent years, much attention has also been paid to the so-called QKD schemes that are independent of measuring devices and are denoted as DI-QKD or MDI-QKD (device-independent or measurement-device-independent) [95, 96].

From the point of view of the originality of the principle of action, we may single out the E91 protocol (1991), often referred to in the literature as EPR and based on the properties of the 'entangled' states of quantum particles proposed by Einstein, Podolsky and Rosen [97]. In this protocol, based on the evaluation of the verification of the Bell-type inequalities [98, 99], an entangled photon pair is created by the method of spontaneous parametric light scattering. In connection with the development of space QKD systems [34], interest in this protocol is still preserved.

The QKD schemes based on continuous variable (CV) measurements and encoding in quadrature amplitudes of the modes of the quantised electromagnetic field have also been studied in detail [100].

2.4. Challenges in the development of global QKD networks

It is known that the size of the encoded data set for the 'one-time pad' method cannot exceed the total length of the used random one-time keys [72, 74], i.e. the key generation rate determines the size of the set transmitted per unit time. Since fibre-optic links with a transmission rate of 100 Gbit s^{-1} per frequency channel are already created [35, 101] and networks with a total capacity of 54.2 Tbit s^{-1} are tested under the field conditions [102], streaming encryption using the 'one-time pad' method requires the QKD rate at a level of 100 Gbit s^{-1} and higher. However, the presently reached QKD rates are only $\sim$1 Mbit s^{-1} for a quantum link with a transmission distance of up to 50 km (see, for example,

[11, 35, 103]). At the same time, external factors reduce the QKD rate in a fibre-optic field network. For example, in [24] for a fibre-optic link on a coil, it exceeded 1 Mbit s^{-1} in the laboratory, but was reduced to 304 kbit s^{-1} under the field conditions.

On the other hand, an increase in the transmission distance of the quantum link of more than 80–100 km [33, 76–81, 103] led to a sharp decrease in the rate of the guaranteed secure QKD, which is theoretically justified, for example, in Refs [78, 84, 104] and caused by FOCL losses and characteristics of modern single-photon receivers. In particular, the length of a 80-km quantum channel corresponded to the highest QKD rate of about 100 kbit s^{-1} [103], but the length of a 100-km fibre-optic link made it possible to obtain the QKD rate of ~10 kbit s^{-1} only [105]. For a FOCL with an ultra-low loss of 0.16 dB km^{-1}, which provided a record transmission distance of 307 km, the QKD rate was only 3.18 bit s^{-1} [106].

It should be emphasised that in order to correctly compare the key rates of QKD protocols, it is necessary to take into account not only the level of optical losses in the fibre (0.2 dB km^{-1} in majority of publications), but also the features of the key processing algorithm, as well as the value of the design parameter ε characterising the degree of deviation of the key from the ideal statistical model and the level of its cryptographic security [33, 35, 106]. However, for simplicity, some authors estimate the QKD rate in FOCLs to be ~1 Mbit s^{-1} and the transmission distance of quantum key distribution to be 150–200 km.

Thus, the achieved level of QKD rates allows the use of quantum keys for encryption using the 'one-time pad' method only for 'niche' tasks, when attempts to read data from the communication channel are possible, but high performance is not required.

In addition, the transmission distance of presently available QKD schemes can be increased by using repeaters [6, 10, 11, 19, 21, 24, 31, 35, 56]. Since practically operative repeaters with quantum memory for qubits have not yet been designed, the experimental development of the QKD networks is based on so-called trusted repeaters (see, for example, [8–12, 18–27]) constructed on the basis of conventional computers. Another possibility is the development of space QKD systems [6, 34], when it is easier to implement QKD at long transmission distances under vacuum conditions, rather than in a fibre-optic link. This explains the long-awaited surge in activity in the development of space QKD platforms [15–17].

Another unsolved problem is connected with the implementation of effective schemes of combining single QKD links into a branched (or extensive) multi-user network [8, 9, 11–13, 18–28, 69]. Quantum coupling has not yet been implemented, and the use of passive optical switches and splitters [107, 108], as well as optical multiplexers [109, 110], leads to an unacceptably large increase in optical losses and noise and, in addition, turns out to be technically challenging. On the other hand, the use of pure computer trusted repeaters based on the AES standard [8–12, 18–28] for branching the QKD network reduces its level of protection to the level of protection of conventional computer systems. Therefore, at present, of interest is a technique based on passive fibre splitters [107, 108].

The technical difficulties of developing QKD schemes include problems of reducing FOCL losses to a level below 0.16 dB km^{-1} as well as improving optical components and temperature, phase and polarisation stabilisation circuits [8–13, 83]. The experimental results [83], in which the authors investigated the relationship between the number of fibre connectors and weldings with a value of QBER, require additional verification. In this case, the single-mode fibre TELECOM network consisted of a delay line necessary to ensure synchronisation, as well as of a 6.5-km fibre segment prolonged with consecutive up to five or seven additional 1–72-m long fibre pieces connected together with standard FC/PC connectors. This link was connected to a two-pass QKD system Clavis2 (ID Quantique) utilising phase encoding of qubits. For each set of additionally connected fibre pieces, statistics were collected for 20–50 hours, and the received 512-bit raw keys were processed using cluster data analysis methods. The main result was that even by adding five 2-m long fibre patchcords, an increase in optical losses on plug-in connectors increased the QBER to values exceeding 11%, which did not provide protection from eavesdropping. Investigations of FOCLs with welded joints of fibre pieces led to similar results.

2.5. Example of a QKD transceiver for fibre-optic networks

As a successful example of implementation of the variant of the decoy-state BB84 protocol, Fig. 2 shows the schematic of the QKD system with phase encoding of qubits, which was developed by Toshiba Research Group (UK) within the framework of the Tokyo QKD network project [24]. This system in the field tests showed a record-high final secure key rate of 304 kbit s^{-1} in a 45-km long fibre-

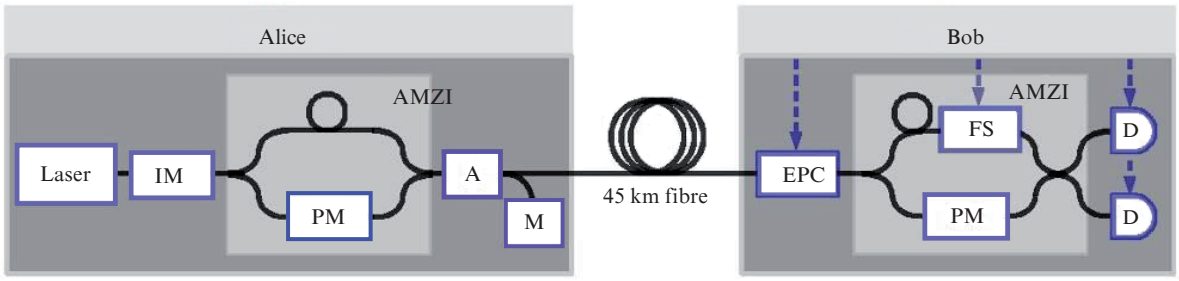

Figure 2. Schematic of the QKD system utilising phase encoding of qubits and decoy-state BB84 protocol [24]: (IM) intensity modulator; (PM) phase modulator; (A) attenuator; (M) intensity monitor; (EPC) electronic polarisation controller; (FS) fibre stretcher; (D) SD-APD detector; (AMZI) asymmetric Mach–Zehnder interferometer.

optic link, despite the relatively high level of optical losses (14.5 dB) due to the fact that fibre was partially suspended in the air.

The transmitting module of Alice contained a distributed feedback (DFB) laser, which generated 1550-nm pulses with a duration of 50 ps and a repetition rate of 1 GHz. The intensity modulator (MI) created three averaged pulse intensities: single pulses of 0.5 photon per pulse and two decoy pulses of 0.1 and 0.0007 photons per pulse. The useful information was encoded by a phase modulator (PM) in one of the arms of an asymmetric Mach–Zehnder interferometer (AMZI). The signal level in the scheme was controlled by an attenuator (A) and an intensity monitor (M).

The receiving module of Bob consisted of an electronic polarisation controller (EPC) and a second AMZI, one of the arms of which contained a phase modulator and the other contained a fibre stretcher (FS) to compensate for the drift in the fibre length. The detectors (Ds) were InGaAs self-differencing avalanche photodiodes (SD-APDs) cooled to –30 °C operating at 1 GHz to compensate for the effect of afterpulse

Table 1. Parameters of field multi-node networks.

Paper/ Year	Country/Project	Place/Participants	Number of nodes	Application/Length /Loss level	QKD rate/QBER	QKD protocol/ Encoding
[18]/2005	US/Quantum Network	Cambridge/DARPA, BBN, Harvard and Boston Universities	10	Urban network/ 10.2 km/5.1 dB Urban network/ 19.6 km/11.5 dB	500 bit s^{-1} (field tests) 10 bit s^{-1} (lab tests)/NA	BB84, SARG04/PhE
[19]/2009	Austria/ SECOQC	Vienna/Siemens, 59 universities and companies	6	6.2 km/2.8 dB 16 km/UA 19 km/UA 22 km 25 km/6 dB 33 km 85 km	8 kbit s^{-1}/NA 2.5 kbit s^{-1}/3.5% NA NA ~1 kbit s^{-1}/<2.8% 3.1 kbit s^{-1}/2.6% NA	CW/HD EPR BB84, SARG04/PhE UA UA Decoy-st./PhE COW/TE
[20]/2009	US/ATD-net	Colledge Park/ Lab for Telecommunications ciences	3	25 km 10 km (coil) 5 m	1090 bit s^{-1}/5.9% UA NA	BB84/PhE
[21]/2010	China/Untitled	Hefei, Wan Ang, Wangxi/USTC	5	4 urban networks/ from 8.4 km/2.65 dB to 10 km/2.82 dB 1 intercity line/ 60 km/17 dB	>1.2 kbit s^{-1}/2% (average value) 4.5 kbit s^{-1}/1.13%	Decoy-st./PE
[22]/2010	South Africa/ QuantumCity	Durban/ KwaZulu-Natal	4	2.6–27 km	891 bit s^{-1}/1.7%	BB84/plug&play PhE
[23]/2011	Spain/Untitled	Madrid/ Polytechnic University	3	Backbone urban network/6 km 10 km Urban access network/1 km 3.5 km	0.5 kbit s^{-1}/NA 100 bit s^{-1}/NA ~200 bit s^{-1}/NA 20 bit s^{-1}/NA	Decoy-st./PhE
[24]/2011	Japan/QKD Network	Tokio/NICT, 9 companies from Japan and EU	6	1 km/1 dB 13 km/11 dB 24 km/13 dB 45 km/14.5 dB 45 km/14.5 dB 90 km/27 dB	0.25 kbit s^{-1}/5%–7% 400 bit s^{-1}/2% 2 kbit s^{-1}/4.5% 81.7 kbit s^{-1}/2.7% 304 kbit s^{-1}/3.8% 2.1 kbit s^{-1}/2.3%	EPR (BBM92) SARG04/PhE Decoy-st./PhE Decoy-st./TE Decoy-st./PhE DPS/ PhE
[10]/2013	US/NQC	Los-Alamos Lab	3	25 km 50 km (coil)	NA NA	Decoy-st./PhE
[25]/2014	China/HCW	Hefei, Chaohu, Wuhu/USTC	9	8 urban lines/ from 0.9 km/1.2 dB to 16.9 km/6.1 dB 2 intercity lines/ 69.7 km/14.1 dB 85 km/18.4 dB	from 16.2 kbit s^{-1}/NA to 1 kbit s^{-1}/NA 0.77 kbit s^{-1}/NA 0.8 kbit s^{-1}/1.16%	Decoy-st./PhE
[26]/2017	Russia/ Untitled	Moscow/RQC	3	15 km/7 dB 30 km/13 dB	0.1 kbit s^{-1}/NA 0.02 kbit s^{-1}/NA	BB84/PhE

Note: (PhE) phase encoding; (PE) polarisation encoding; (TE) time encoding; (NA) not available; (HD) homodyne detection.

noise and parasitic capacitive elements [111]. In this case, the detection efficiency was 19%, and the dark count rate was about 10 kHz.

The authors [24] explained the achievement of record rates in the field tests by the following innovations:

– taking into account the APD count rate as a feedback signal to adjust the delay position of the detector gate;

– taking into account the QBER value in the fibre stretcher scheme to correct the tensile stress and minimise the negative effect of the finite key size, which is considered infinite in theoretical models;

– decreasing the drift of parameters and increasing the time of stable operation of the system to tens of minutes, which was achieved through careful study of the synchronisation scheme and the use of data (classical) fibre and quantum fibre in the same fibre bundle;

– decreasing the active temporal width of the gated photodetectors to 100 ps; and

– using improved procedures for sifting a random key, correcting errors in it and amplifying its privacy, based on the calculations of Toeplitz matrices with a block size of several hundred kilobits per multi-core processors.

2.6. Multi-user field networks implemented on the basis of QKD links

On the basis of 'point-to-point' QKD links servicing a pair of subscribers, a number of projects of multi-user field QKD networks were implemented [18–27], in which fibre optic links and atmospheric lines were deployed on the ground, being subject to a maximum environmental impact. Several projects of links and field QKD networks were also launched in the Russian Federation (see, for example, [26, 28]).

The main parameters of the most characteristic projects of field multi-user (multi-node) networks are presented in Table 1. From the QKD projects listed in the Table, the most large-scale projects are those described in Refs [19, 24, 25], which combine the QKD links of various developers. The most popular protocol is the decoy-state BB84 protocol, which is implemented both for polarisation and for phase encoding. The QBER values obtained by different authors in the operating range from 0 to 11% characterise the irreducible noise and loss level in the quantum channels realised by them. This level, as can be seen from Table 1, does not directly correlate with the final secure key generation rate and its transmission distance.

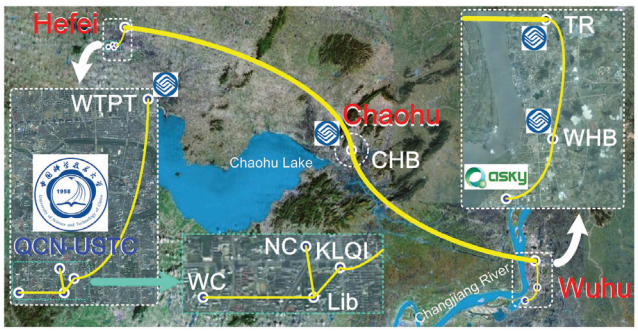

Figure 3. Geographic distribution of the Hefei – Chaohu – Wuhu wide area QKD network, which connects three cities – Hefei, Chaohu, and Wuhu [25].

Table 1 presents the projects of QKD networks, each of which implements from 3 to 10 network nodes. The distances between them vary from 12 to 85 km, and the key distribution rate is 0.9–304 kbit s^{-1}. At the same time, the authors of Ref. [23] estimated the rate of ~1 kbit s^{-1} as potentially sufficient to serve AES cryptographic protocols with a key length of 256 bits per network and a data transmission rate of 2.4 Gbit s^{-1}.

Since quantum retranslators [6, 33, 35, 56, 57] have not yet been implemented in practice, computer trusted nodes and optical switches are combined in various versions of the QKD networks presented in Table 1.

For example, the authors of Ref. [23] (see Table 1) present an example of integration of quantum FOCLs into the existing urban network at two levels: 1) high-speed backbone lines and network segments (also called trunk, core or skeleton) for 'all-to-all' interconnections, and 2) access networks, delivering content from backbone lines to end users.

Serious efforts in China to develop QKD networks are demonstrated in work [21, 25] (see Table 1). Chen et al. [21] describe a network of five nodes with a star topology and polarisation encoding of qubits in a single-mode fibre where trusted repeaters are combined with optical switches and a wavelength division multiplexing method. In addition, between the cities of Hefei and Wuhu, a QKD network was deployed (Fig. 3) with phase encoding of qubits [25], which develops the concept of mixed use of trusted repeaters and optical switches. In this project, QKD keys were also used in a virtual private network (VPN), i.e. in a network with an additional layer of security created on top of the physical network. In this case, a 150-km-long backbone line contained three trusted repeater nodes. The Hefei metropolitan area QKD network with five nodes used full-mesh optical switches for 'all-to-all' interconnections, allowing seamless operation of several quantum links. The Wuhu metropolitan network was designed as an access network with time division multiplexing (TDM), which provided seamless operation of only one quantum link.

Table 2 presents the features of the structure of multi-user QKD networks, the main parameters of which are given in Table 1. We should note the original scheme of the main backbone network in [23], implemented as a ring of three network nodes on the basis of controllable coarse wavelength division multiplexers (CWDM) and a system of reconfigurable optical add-drop multiplexers (ROADMs), described in detail in [109]. The authors of Ref. [25] used three optical circulators for similar purposes.

In all the projects listed in Table 2, the branching factor was no more than 1:4 (one node is connected to four), whereas the gigabit-capable passive optical network (GPON) standard for passive fibre-optic links provides this coefficient up to 1:128 [112]. In general, the branching of a network based on optoelectronic devices is still far behind the capabilities of a computer trusted relay [8–10], and the hopes are primarily connected with passive fibre splitters [109, 110].

The problems of optimising the deployment of trusted nodes were considered, for example, in [19]. The appearance of noise in fibre-optic QKD networks due to spontaneous

Table 2. Properties of the structure of field QKD networks and practical problems to be solved.

Paper/Year	Method of communication of nodes	Network type and branching factor	Implemented useful functions
[18]/2005	Programmable optical 2×2 switch	City network of star topology with four-node optical switching	QKD with not fully functional nodes: only receiving or transmitting data. Quantum authentication is built into the regular IPsec architecture and IKE key exchange system
[19]/2009	Trusted repeater	Urban mesh type network with computer-controlled four fully connected nodes and two nodes at the ends of the QKD links	QKD with full-function nodes. Telephone communication with the one-time pad encryption. Videoconferencing with AES encryption between all nodes. Stream re-routing of data
[20]/2009	2D-MEMS optical 4×4 switch 2D-MEMS Optical DWDM multiplexer	Laboratory network with one field FOCL segment and optical dynamic line re-commutation	QKD (node functions and encryption method are not specified). The QKD data is transmitted by the standard FOCL traffic
[21]/2010	Trusted repeater Optical eight-port CWDM multiplexer	Network with intercity and city lines. Star topology with optical switching of four fully connected nodes and automatic routing	QKD with not fully functional nodes. Telephone communication with real-time one-time pad encryption. Videoconference with AES encryption
[22]/2010	Software switching control Optical CWDM multiplexer	Star topology with complex switching and optical branching of four fully connected nodes	QKD. Entering the key into a standard AES encryption system
[23]/2011	Optical CWDM multiplexer with a ROADM system for remote channel switching	City backbone network with ring topology of three CWDM multiplexers and a GPON network	QKD with fully functional nodes (encryption method is not specified)
[24]/2011	Trusted repeater Hierarchical network of agents that manages: – key structure – authentication – data routing	City mesh type network with computer switching to a ring of four incompletely connected nodes and two nodes at the end of individual lines. Autonomous routing of data with rerouting in the event of eavesdropping	QKD with full-function nodes. Switching of the one-time pad/AES protocol with account for the key volume. Secure real-time video conferencing. Secure mobile telephone communication. Detection of eavesdropping by removing a part of the photon flux from fibre with compensation of the total power level
[10]/2013	Trusted repeater The computer server implements a trusted third party in the AES standard with a key length of 256 bits	Star topology with computer switching: – 1:3, experimentally implemented: – 1:1000, technically possible – 1:1000, possible on a powerful server	QKD with full-function nodes. Identification, authentication, AES encryption and digital signature. The network-centric system for the protection of procedures for the collection of critical data on the operation of the power grid
[25]/2014	Trusted repeater A router is a 'ring' of three circulators with software control and an optical 2×2 switch	Backbone intercity line with trusted complex repeaters optical switching. Urban access network with an optical 1×2 splitter and TDM	QKD. Full-function nodes. Telephone communication with the one-time pad encryption in the public network. QKD keys are used by a VPN gate (router) for symmetric 256-bit AES encryption
[26]/2017	Trusted repeater	City channel connecting two QKD links	QKD. Full-function nodes. One-time padencryption between two bank offices

Raman scattering was discussed in [20, 109, 110], and a possible approach to solving this problem in access networks was considered in [107, 108]. In the project from Ref. [24], the length of the aerial fibres was half the length of all the fibre-optic links used, which was a record.

3. Combined networks based on quantum optics and an extended set of computer data processing techniques

Among the publications on multi-node networks, of interest is the work on the application of QKD in network-centric systems [8–10] and in photonic networks (photonic networks) [11, 12], demonstrating the tendency of integration of QKD networks with multi-agent models of artificial intelligence [47].

3.1. Network-centric system with a trusted third party architecture

Works related to the development of network-centric systems [113, 114] were started in 1999 by the Defense Advanced Research Projects Agency (DARPA, US). Their goal is to create global peer-to-peer (P2P) computer networks for military and civil purposes. In such networks, in contrast to usual 'client–server' architectures, all nodes have equal communication capabilities and allow arbitrary routing of messages through any node. This guarantees self-recovery and stability of work when nodes fail to operate in critical control structures, and also implements close information interaction between people and various types of unmanned autonomous robots with host computers, space vehicles and telecommunication networks. In this case, the rules of agent interaction and the hierarchical agent-based management models of teams are built directly into the model of each agent's behav-

iour [47]. In addition to the results of Refs [8–10], the space-based QKD facilities fit well into the concept of network-centric systems [15–17, 34], as well as the results of the experiment [115] on the transmision of quantum keys from an aircraft to a ground station.

Hughes et al. [8–10] reported the results of the Los Alamos National Laboratory project on the deployment of a network-centric system that controls the critical infrastructure of the power grid under the conditions of rigid centralised network administration of the operation of nodes with limited computing resources. The purpose of using QKD was to prevent eavesdropping or modification of control commands. The basis of this project, protected by several US patents, was a multi-level hierarchical star topology (Fig. 4).

In the diagram in Fig. 4 at the level of physical objects (below), a large number of N clients are connected to a server via quantum links. At the QKD management level (the middle part of the figure), the server supports the functions of a trusted security certificate management centre that monitors inter-node scenarios. At the application layer (top), a so-called trusted third party (essentially a software robot agent), traditionally known as Trent, is implemented. At the same time, all the components of the trusted third party are interpreted as unconditionally secure for any client node that sends a request to it (Alice, Bob, Charlie), and the structure of the keys distributed by the quantum protocols ensures confidentiality, authentication of the user for the trusted network and the impossibility of bit commitment.

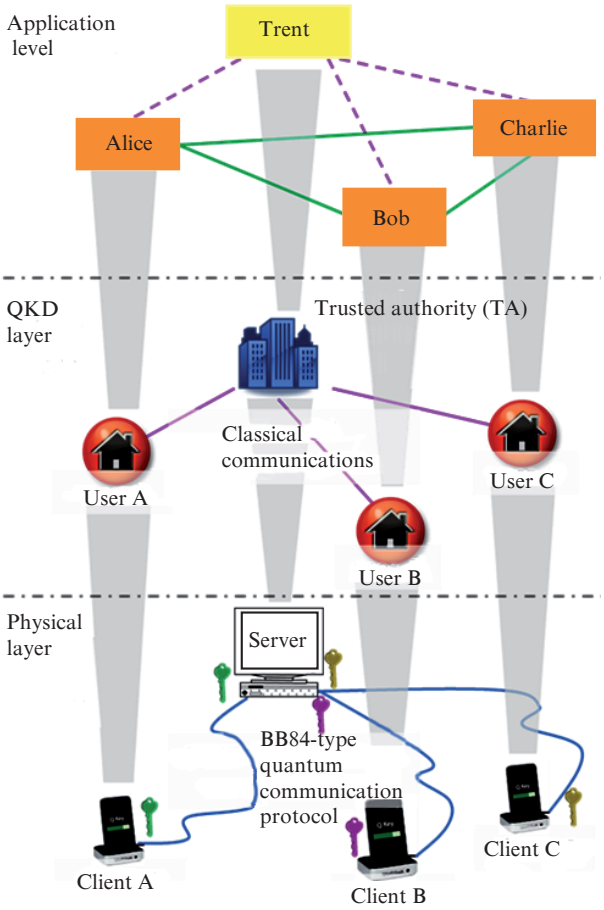

Figure 4. Network centric quantum communications architecture [10].

The QKD scheme in [8–10] relied on the decoy-state BB84 protocol, where the developers encoded the qubits with polarisation states, considering the phase encoding to be too 'demanding' for interferometric schemes, as well as too cumbersome and expensive. This, however, required elimination of the effect of birefringence in fibre and the development of a self-adjusting polarisation system. The integrated quantum key transmission module included a distributed feedback laser and an intensity modulator providing a repetition rate of 10 MHz for short (less than 1 ns) attenuated laser pulses at $\lambda = 1550$ nm and an average photon number of less than one per pulse. To measure the quantum states in the scheme, InGaAs APDs were used with a detection efficiency of 15% and a probability of dark counts of $\sim 10^{-5}$ in a time interval of 1 ns.

During a long (two and a half years) testing, use was made of a trusted server (Trent node) only with three client nodes (Alice, Bob, Charlie), but the equipment allowed one to connect up to 100 nodes in principle, and in the case of special server equipment the number of clients could be increased to 1000 In the trusted (Trent) node, signals from the transmitting modules of client nodes are time multiplexed. The optical signals received from the FOCL were processed using a standard 1000Base-LX module. The system ensured the simultaneous operation of quantum links for several pairs of nodes.

A quantum random-number generator of original design with a performance of more than 5 Gbit s^{-1} was applied to each node [8–10]. Random keys were used for encryption using the AES algorithm, and the digital one-time signature algorithm was based on the Winternitz scheme. In non-quantum bidirectional communication channels, the nodes were authenticated using hash functions and a technique for calculating a checksum using cyclic redundancy code.

The network-centric QKD system [8–10] has been successfully tested in the regime of secure collection of the parameters of the power grid operation, including the procedures for verifying subscriber access rights. The vulnerabilities of the trusted server in these works were not discussed.

3.2. Photonic network with a multi-agent QKD key management system

Paper [11] published in 2011 by leading specialists from several Japanese universities and companies considered in detail a quantum architecture, which is a kind of photonic networks [12–14], that is, purely optical telecommunication networks oriented to mass maintenance of cloud computations or a digital cinema network. It is characteristic that the developers of the architecture [11] envisaged in it the hierarchical structure of hardware agents of the multi-agent system of artificial intelligence, controlling the quantum keys and conventional cryptographic means, and also carrying out the routing of the data stream with the help of optical multiplexers and switches. This reduced the number of trusted repeaters. To make this network cost effective, the same FOCL was provided for the quantum and non-quantum QKD channels [11].

As shown in Fig. 5, the network architecture [11] has five data exchange levels, where the QKD scheme is used to communicate agents managing the distribution of the keys. Unlike

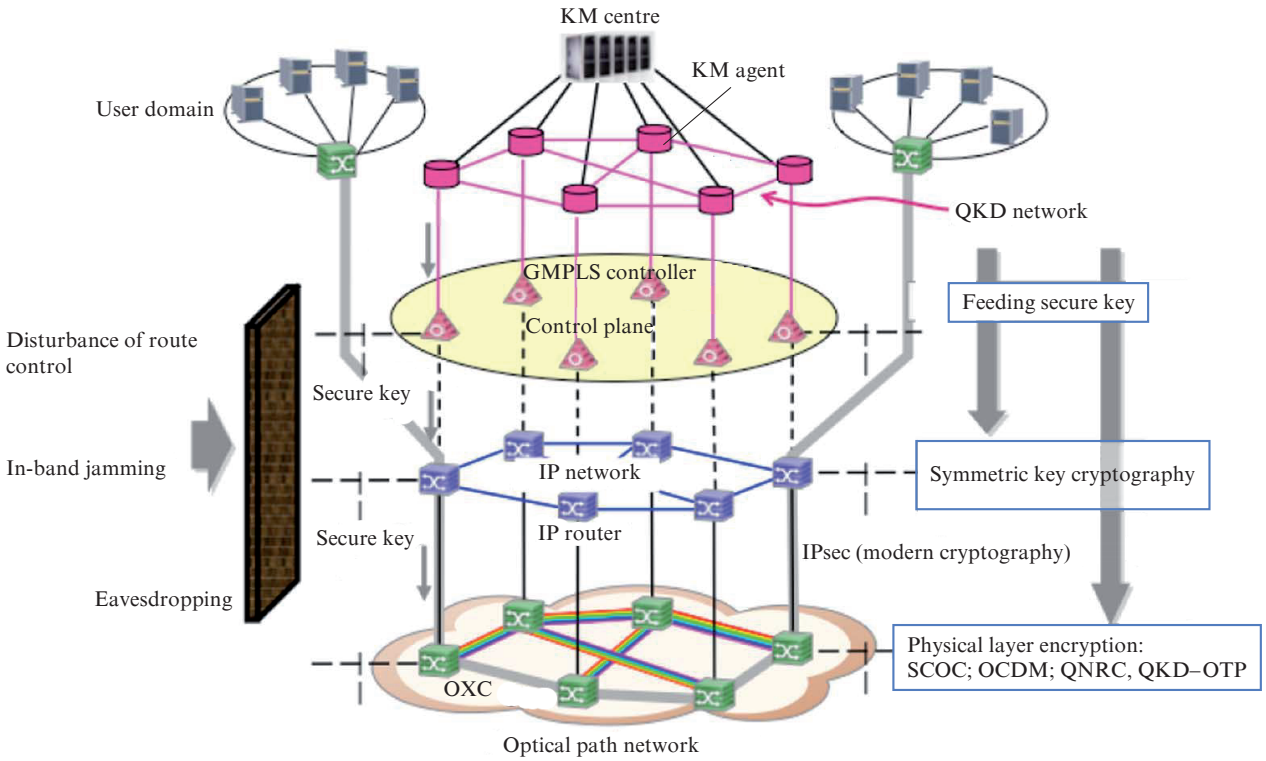

Figure 5. Conceptual model of a secure photonic network with a hierarchical multi-agent system of cryptographic means management [11]: (KM) key management; (SCOC) secure communication using optical chaos; (QNRC) quantum noise randomized cipher; (QKD–OTP) QKD– one time pad; (OXC) optical cross connect.

the architecture used in [8–10], the control structure of hardware agents in [11] is hierarchical and has a single key management centre. The dedicated subnet of hardware agents monitors the operation of optical cross connects using wavelength division multiplexing at the level of physical devices and optical commutation channels (below in the figure). At the same time, users' domain computers interact with IP routers at the level of conventional IP network protocols and traditional symmetric key encryption. At the protocol and network management level, a so-called generalised multiprotocol label switching (GMPLS) is used. The necessity of servicing the above multi-level architecture in the automatic regime without the access of personnel to the processed data structures seems to be the main incentive for the introduction of multi-agent models into the QKD schemes [8–10, 11, 12], originally created to simulate human intellectual functions in control schemes [47]. In addition, such models are needed to solve several important problems of classical cryptography, the impossibility of solving which by means of quantum cryptography has already been theoretically justified.

These problems, briefly noted in [6, 31], were discussed in detail in 2016 in review [70]. They include such as bit commitment, secure two-party computation, zero-knowledge proof, random oracle, and position based cryptography. To solve all these problems requires simulating human behaviour, which can be conveniently implemented with the help of multi-agent systems of artificial intelligence [47].

In addition to the joint application of QKD schemes and the one-time pad method (shown in Figure 5 as QKD–OTP), the authors of [11] proposed using somewhat simpler and cheaper methods in photonic networks: for example, block ciphering in an optical code division multiplexing (OCDM) scheme [116, 117], as well as a quantum noise randomised cipher (QNRC) encryption technique based on the Y-00 protocol [48–51]. In addition, Kitayama et al. [11] pointed out the expediency of applying the scheme of secure communication using optical chaos (SCOC) [118], which arises in the emission of an ultra-long fibre laser [119].

Thus, the authors of Refs [8–12] demonstrated the line of research aimed at developing a whole set of cryptographic means with different price and security levels for fibre-optic links. At the same time, the multi-agent system [47] in the above-mentioned works is a flexible tool for computer modelling of human intellectual functions that allows a complex set of quantum and traditional cryptographic tools to be managed.

3.3. Cryptographic encoding by the quantum noise of a transmitting laser

The quantum Y-00 protocol (also referred to as Yu00 and αη) was developed in 2000 in the USA as part of the DARPA project, then presented in [48, 49, 120] and other papers of this group, as well as in a number of articles by Japanese scientists [50, 51, 121–128]. This protocol ensures secure data encoding using a transmission laser quantum noise component and special randomisation procedures for two secret keys, which are either preliminary known to the sender and the receiver, or distributed by a separate QKD

scheme. The Y-00 protocol is designed to protect against data readout in mass telecommunications networks and, unlike the QKD protocols, can be directly used for high-performance gigabit streaming encryption. In 2003 [48], the level of cryptographic security of the encoding system was ensured at the level of the AES standard, and later the Y-00 protocol's cryptographic resistance level to a number of classical and quantum attacks was substantiated in [121–128] and subsequent works within the framework of Shannon's information theory.

The regime of the secure transmission for Y-00 [48, 49] was carried out by connecting special transceiver modules at the input and output of an already existing conventional fibre-optic link. Unlike QKD, the Y-00 protocol does not require high-quality optical fibres, allows the use of fibre amplifiers, and also enables the use of wavelength division multiplexing to increase the FOCL bandwidth.

In the original papers [48, 49], the Y-00 protocol was implemented according to a scheme in which coherent quantum states were transferred by phase values of the optical signal. This made it possible to achieve a rate of 2.5 Gbit s^{-1} in a laboratory data link of length 210 km by the year 2007 [120], as well as the transmission rate of 622 Mbit s^{-1} in a field network 850 km in length. For mass networks based on fibre-optic links, the authors of Refs [50, 51, 121–128] developed a variant of the Y-00 protocol using optical intensity modulation. In 2014, an encryption rate of 100 Gbit s^{-1} in a 120-km fibre optic link was demonstrated for this protocol [127].

The general principle of the secure multi-level (so-called M-ary) Y-00 encryption protocol [48] is shown in Fig. 6 for the case of optical signal encoding [128]. Use is made of M different optical signal levels (or phase for phase encoding), which are determined by the coherent states of the laser light. A pair of such optical signal levels, referred to as a basis, serves to encode 0 or 1 in the transmitted bit sequence. For each transmitted bit, the basis is chosen randomly or quasi-randomly using a running key generated from a seed key K.

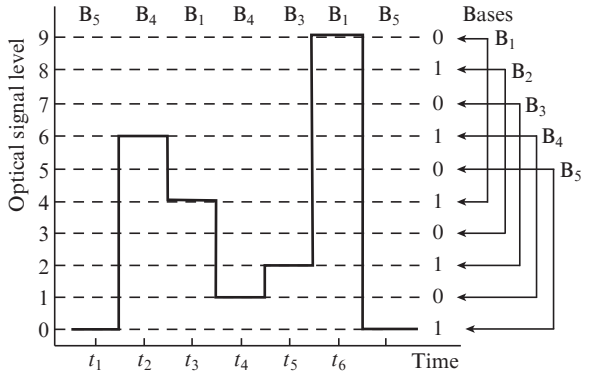

Figure 6. Principle of the Y-00 encryption protocol [128].

For clarity, Fig. 6 shows $M = 10$ and the arrows indicate five bases (B_1–B_5), that is, their total number is $M/2$. In the case of odd-numbered bases, the value 0 is encoded with a higher intensity in the pair, and 1 with a lower intensity. For example, for basis B2, 1 will be assigned by the optical signal level 8, and 0 will be assigned by the optical signal level 3. Accordingly, in bases with even numbers, 0 will be assigned by the low level, and 1 will be assigned the high level. The difference between any two adjacent optical signal levels is so small that the distributions of the quantum noise components for adjacent signal levels overlap and prevent an eavesdropper from distinguishing between 0 and 1 in the transmitted data.

For example (Fig. 7), if an optical signal level 6 is transmitted at some instant of time with the help of basis B_4 (the encoded bit contains 1), the eavesdropper (Eva) measures the optical level but cannot decide whether it is the 5th, 6th or 7th level because of the quantum noise. In this case, the 5th and 7th levels are assigned '0', and the 6th level is assigned '1'. Accordingly, in the transmission of 0 and 1, all values of M will be equally probable for the eavesdropper, and cryptographic analysis will require measurements of the entire set of transmitted data. At the same time, using synchronisation signals, a regular receiver (Bob), who knows the seed key K, can decipher the data, quickly switching the measurement basis and performing measurements only for two possible optical signal levels by a double threshold device. Of course, measuring the intensities at the level of quantum noise requires high quality emitters and single-photon detectors.

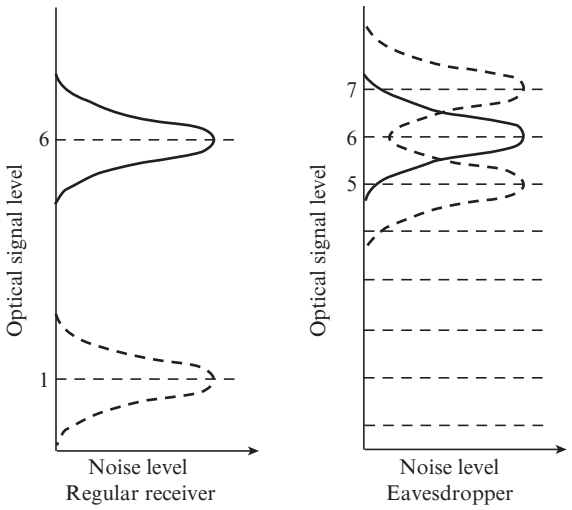

Figure 7. Overlap of quantum noise distributions for adjacent optical signal levels denoted by 5–7 [128].

In the Y-00 protocol, data cryptanalysis is counteracted not only by increasing the $M/2$ parameter used in M-ary encoding, but also by increasing the uniformity of the distribution of various blocks 0 and 1 in the transmitted data set [125]. To this end, the authors of Refs [48–51, 120–128] used the known methods of working with block ciphers and linear feedback shift registers (LFSRs), which allow one to obtain a large array of quasi-random values of the running key from the seed key K. In this case, the characteristic features and the 'weak' point of the seed key are 'smeared' over a large array of interconnected data blocks of length M bits, called a block chain (in the literature the term block chain indicates certain analogies with techniques from the sphere of crypto currency).

Analysis of the cryptographic strength of the Y-00 protocol was accompanied by a large number of discussions [129–134]. The authors of Refs [129, 130] performed a cryptoanalysis of the stream encryption scheme combining the

Y-00 protocol and the 'one-time pad' method, for which they considered a known plaintext attack. As a result, a conclusion was made that the real cryptographic resistance of the Y-00 protocol cannot be higher than that of traditional streaming encryption.

The response arguments of the developers [135–137] were reduced to the proof of the incorrectness of the method used in [129–134] to determine a set of bits in the running key by the eavesdropper in which the level of quantum noise for coherent states was unjustifiably neglected. The need to take quantum noise into account was confirmed by detailed studies of O. Hirota's group (Tamagawa University, Tokyo, Japan) [138]. Thus, the authors of Ref. [129] mistakenly ignored the procedure for privacy amplification. The discussion in [135] also demonstrated the ineffectiveness of a fundamentally possible attack using the heterodyne measurement scheme proposed in [129] for cracking the Y-00 protocol. In order to theoretically substantiate the cryptographic resistance of the Y-00 protocol, the authors [139] analysed several schemes of quantum individual attacks based on the Shannon entropy calculations. They also considered the variants of ciphertext-only attacks on data and on key and discussed separate attacks with measurements of so-called direct and indirect observable parameters.

In addition, the authors of Ref. [139] considered known and intentially prepared plaintext attacks, as well as conventional and modified Lo–Ko attacks [131], which are named after their developers and suggest the splitting of the signal sent by Alice into a large number of channels, as well as the measurement of the signal in each of them by a separate receiver. In particular, the authors of [139] succeeded in demonstrating the infeasibility of Lo–Ko attacks, which require too many channels for a real device. As a result, for a number of attacks the authors of [139] presented a proof of the Y-00 security level, justified within the framework of information-theoretic security. At the same time, the analysis of the so-called indirect attacks on quantum observable parameters led these authors to conclusion that the length of the original seed K should be increased by more than 100 bits, whereas in the early works the developers of the Y-00 protocol considered 32-bit length to be sufficient.

In addition, Yuen et al [140] considered in detail a wider set of quantum attacks for Y-00, the results of which confirmed the conclusions of Ref. [139]. In addition, critical publications [132–134] with respect to the Y-00 protocol have made it possible to introduce a number of adjustments to the experimental schemes. During the theoretical modelling of Y-00 circuits, the authors of [133] found that if the signal attenuation and signal amplitudes measured by Bob and Eve differ by more than 3 dB, the number of wrong bits recorded by Bob and Eve is significantly redistributed in favour of the Eve eavesdropper, i.e. there is an additional leakage of information. As a result, the developers of Y-00 had to complicate the experimental scheme of the layout, and for the additional randomisation of the signal they added special high-speed modules introducing a second pseudo-random signal independently obtained from the second seed key; in this case, the length of the seed keys K increased to 1000 bits. In addition, as a result of discussions [129–134], the theoretical justification of the Y-00 cryptographic resistance was corrected.

As a result of the above studies, a TU-Cipher-0 transceiver was introduced in 2016 [51], implementing the Y-00 protocol with gigabyte speeds over a standard fibre-optic Ethernet link and using 4096 intensity levels. The general appearance of the device is shown in Fig. 8a. The initial signal of a gigabyte Ethernet network and its encrypted version obtained with the Y-00 protocol in an 80-km-long fibre optic link with a standard transmission 1000Base-LX module are shown in Figs 8b and 8c. In the system the optical signal from the FOCL is intensity modulated using the quantum noise of the sender's laser and two randomised classical keys that can be distributed using the QKD scheme.

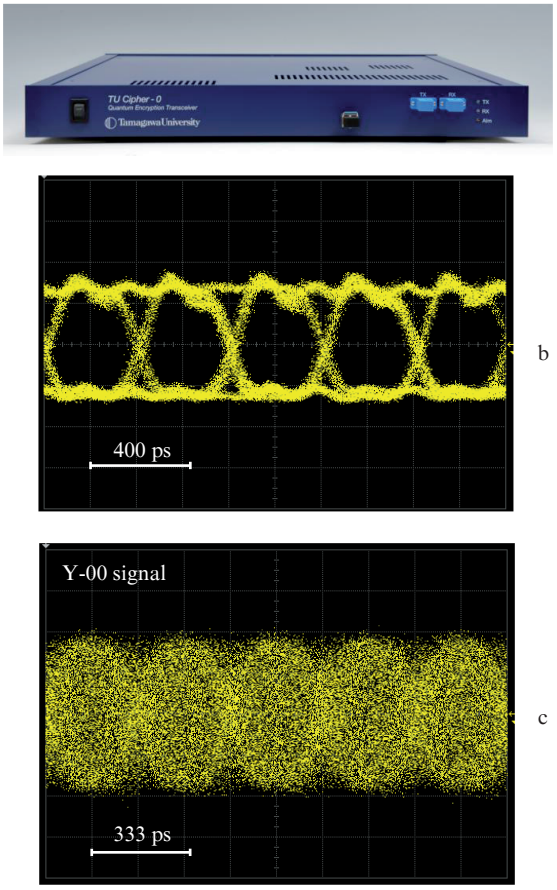

Figure 8. Y-00 transceiver 'TU Cipher-0':
(a) general appearance, (b) a waveform of the gigabyte Ethernet signal, (c) Y-00 encrypted signal.

For photonic network users with modest financial resources, optical code division multiplexing (OCDM) mentioned above and optical code division multiple access (OCDMA) were proposed instead of the Y-00 protocol [116, 117, 141–144]. Both versions use the WDM principle, where each channel is encoded by its own set of optical wavelengths (for example, by two values of λ) to order access to the common frequency band of the transmitting FOCL. In addition, in each channel during the transmission time T of a single data bit, an additional short optical pulse, controlled by the shift register and the M-ary block cipher driver, is time shifted (similar to the scheme in [51]). The element base of the multi-level M-ary encoding involves the development of optoelectronic encoding devices, star-topology splitters and routers, multiplexers/demultiplexers based on arrayed wave-

guide gratings (AWGs), fibre splitters, delay lines, and optical switches.

Thus, developments based on the Y-00 protocol [48–51, 121–128, 135–140] and OCDM/OCDMA optical circuits [116, 117, 141–144] demonstrate the formation of a whole set of cheaper alternative schemes allowing, in contrast to QKD schemes, the change in the configuration of the link, its repair and replacement of damaged FOCL segments.

3.4. Possible schemes of attacks in quantum links

Attacks against the optical QKD scheme are divided into quantum ones performed by measuring the quantum states and classical ones implemented with the help of ordinary measurements [6, 31, 57]. Quantum attacks are subdivided into individual and coherent, depending on the measurements of one or more quantum states. Coherent attacks can be collective and joint, depending on the effect of one or more measuring devices on a qubit.

Back in the late 1990s, Lütkenhaus [78, 87] discussed possible schemes for quantum individual attacks, where each qubit is measured using additional beam-splitting elements and qubit intercept/resent schemes, as well as schemes of collective attacks [145], in which each of quantum states is measured using a separate probe.

Review [32] briefly discusses schemes of attacks on incorrect theoretical models of cryptographic security. In addition, methods are being developed for so-called weak measurements [146], which, in contrast to strong measurements, do not lead to an irreversible collapse of the quantum state.

After the publication of the experimental work [99], which demonstrated the possibility of producing time-shift attacks by means of 'insertion' of additional fibre segments, there are almost no other publications on the experimental implementation of quantum attacks, which can be explained by the absence of practical quantum memory devices. Therefore, at the present time, the most likely attacks are non-quantum-type attacks [6, 31], affecting laser sources, light modulators or single-photon photodetectors, whose review was presented, for example, in Refs [6, 31–33, 57]. The danger of non-quantum-type attacks is that they do not use the interaction of the measuring means of the eavesdropper with the qubits and, accordingly, do not increase the number of error bits that allow the hacking to be detected. In view of the complexity and cost of QKD equipment, in most cases, attacks are modelled theoretically.

In attacks *on a laser signal source* [32], use can be made of

– beam-splitters for action on a multiphoton component in a weak (or attenuated) laser pulse [4, 87], which led to the development of decoy-state BB84 protocols [92];

– high-energy destruction of optical devices or partial modification of their parameters (so called laser damage attack) [147, 148];

– several laser diodes with individual features of spectra or other characteristics in some QKD schems [32, 149]; and

– correlation of light pulses in the emitted sequence [150].

Attacks on light modulators used in the transmitting and receiving parts of the QKD scheme can be performed using large pulse attacks [147]. When Eve sends an intense laser pulse into the transmission link in the direction of Alice or Bob, it will result in the reflection of part of the signal by the circuit components; the measurement of the signal characteristics will enable Eve to estimate the transmission coefficients of the modulators and the quantum states specified by them. The second possibility here is the high-energy destruction of the optical components (laser damage attack), for example, an attenuator at the output of the Alice device, a decrease in the transmittance of which will lead to an increase in the efficiency of a quantum attack with a beam splitter and of a non-quantum attack using high intensity laser pulses. Gisin et al. [151] presented more complex Trojan-horse attack schemes using optical frequency reflectometry methods for estimating the states of light modulators and other devices.

Attacks on single-photon photodetectors [32, 57] can, first of all, use bright blinding pulses (tailored bright attack or blinding loophole) [152, 153]. In 2010, a fundamental vulnerability in this attack was demonstrated for two commercial QKD systems developed by ID Quantique and MagiQ Technologies [152], and in 2011 this hacking method was implemented experimentally on the 290-m-long QKD link at the National University of Singapore [153]. In an experiment with a blinding loophole, the vulnerability of pairing APDs installed in the Bob module was used. During the attack, the eavesdropper 'blinded' all APDs of Bob using an external laser diode with continuous radiation and circular polarisation, and then, if was necessary, added linearly polarised pulses from four other laser diodes, artificially generating the desired response signal in any of Bob's detectors. The quantum bit error rate QBER remained at the level considered safe.

In other types of attacks on photodetectors, one can use:

– broadband parasitic light emitted by a silicon APD in the event of an avalanche [154] and incident into a short section (pigtail) of a fibre interferometer;

– above-mentioned scheme for the formation of time shifts [99] with the help of 'insertion' additional fibre segements;

– input of false optical signals (faked-state attack), generating output signals analogous to those registered when detecting single photons [155], which is feasible in man-in-the-middle attack schemes;

– analysis of time parameters of the signal, measured 'too' accurately, with the transfer of an excessive number of characteristic sets of significant digits [156];

– the dependence of the efficiency of detecting photons on time in gated pairs of photodetectors, where small differences in the characteristics of the photodetectors and the change in the time of arrival of the photon relative to a clocking pulse by the eavesdropper affect the count of 0 and 1 and facilitate the fake-state attack [57, 157, 158]; and

– input of pulses by the eavesdropper that probe the QKD circuit at wavelengths significantly different from λ, for example, at $\lambda = 1924$ nm instead of 1536 nm (Trojan horse attack) [159].

In addition, an eavesdropper can use date leakage from auxiliary technical channels [6, 31, 57]. A model for estimating the possible volume of such leakage was proposed in [160].

It should be noted that the above schemes of attacks do not exhaust all possible options described in the literature.

The above works helped to form a more realistic view of the level of sophistication and reliability of the existing QKD schemes. For example, V. Scarani, a co-author of a number of QKD protocols and works on vulnerability analysis, stressed

in [32] that the concept of 'cryptographic security based on physical laws' became largely an advertising slogan, often incorrectly interpreted as 'cryptographic security based *only* on laws of physics'.

The complexity of the task of constructing an integrated QKD model is evident, for example, from the fact that five years after the successful use of the SOW protocol [161] in an international European SECOQC project [19], article [93] proving its vulnerability was published. In addition, in response to the publication of 2016 [162], which describes a new QKD scheme with the transmission of a quantum signal at the side bands (subcarrier frequency) of a strong classical optical signal, the method of its hacking was substantiated in [163]. Therefore, in a recent review [57], special attention was paid to methods of counteracting attacks.

The main approaches to counteracting attacks [57] primarily involve the improvement of the hardware and software parts of the QKD schemes. Modifications of the hardware scheme include the installation of:

– additional optical isolators (Faraday rotators) and filters preventing the propagation of optical signals introduced by Eve; and

– additional watchdog photodetectors at the input to the Alice's and Bob's devices that track the levels of the input signals.

However, for optical isolators, the issue of controlling the entire range of wavelengths that can propagate in the QKD scheme remains open, and for watchdog photodetectors it may be necessary to vary the modes of their synchronisation, i.e. the switching times and the widths of the time window used.

Improved software in the QKD schemes is necessary to counteract attacks that exploit the differences in the spectral characteristics of laser sources [57]. In this case, additional procedures are required to amplify privacy.

A separate direction is the development of new QKD schemes, in which special hopes are placed on the schemes that are independent of the hardware (DI–QKD, MDI–QKD) [57].

Experiments with QKD schemes require complex techniques [18–28] and systems costing tens of thousands of Euros; therefore, the methods against quantum and non-quantum-type attacks have not yet developed into a coherent methodology, which would allow one to form, using the open publications, an independent opinion on the reliability of this or that QKD scheme.

3.5. Vulnerabilities of computers serving QKD networks

In contrast to the development of QKD systems based on academic research in the field of quantum optics, in computer networks, the analysis of vulnerabilities and possible attacks is based on a detailed understanding of the joint work of specific software code and hardware, tested using commercial software and hardware tools. At the same time, the results of most tests are published in the analytical reports of specialised state, private and public organisations. These organisations, in addition to the already mentioned NIST, include SANS (USA, http://www.sans.org/), CSI (USA, http://www.gocsi.com), ASIS (https://www.asisonline.org). Among Russian companies we should mention JSC Kaspersky Lab (https://www.kaspersky.com/). In addition, Infowatch (Russia) (https://www.infowatch.ru/), as well as smaller analytical and information agencies, for example TAdvisor (http://www.tadviser.ru/), publish their own analytics. Great influence on the computer community is provided by such authoritative publications and websites as http://www.schneier.com/, http://www.wired.co.uk/, http://www.pcworld.com, http://www.cnews.ru/, and http://www.cybersecurity.ru/.

Any modern quantum link in a multi-user QKD network [8–12, 18–27] is a system of distribution of random keys used by conventional network cryptographic tools for encoding messages rather than an autonomous means of secure communication. At the same time, the issue of the vulnerability of computers, programmable logic integrated circuits (PLICs) and microcontrollers serving the QKD scheme and subscriber workstations is beyond the scope of laser physics and quantum optics and has not been practically considered in the literature on quantum key distribution. When describing commercial projects discussed, for example, at the website of ID Quantique [164], which specialises in the development of QKD systems, the problem of information protection of a computer component is outlined only in the general form. Meanwhile, in accordance with the complex approach practiced in the Russian Federation [71, 72, 165, 166] to ensure the information security of computer systems, all possible channels for data leakage through computing devices, auxiliary equipment and personnel should be blocked for comprehensive system protection. A typical set of information protection tools used for the Internet and mass telecommunications networks [72, 165–178] includes:

– antivirus software;

– means of counteracting data leakage and controlling staff loyalty;

– antispam software;

–- means of counteracting the false flow requests (i.e. DDoS-attacks);

– firewalls for filtering network packets in order to protect against unauthorised access;

– encryption facilities, which include quantum cryptography;

– means of password access and biometrics for identity and access management;

– special systems for controlling technological processes of critical objects;

– storage and backup systems;

– means of preventing data leakage on auxiliary technical channels (power networks, transformers, etc.); and

– means of protection against physical hacking devices.

In this case, direct reading of the encoded data from the communication channel, which is counteracted by the QKD scheme, is not singled out as a separate category of protection, which can be explained by the wide distribution of the Diffie–Hellman algorithm in mass networks, which allows for the open distribution of secret keys [72]. The literature lacks the data on cases of mass breaking of telecommunication networks through the vulnerabilities of this toolkit. Accordingly, QKD networks that protect against reading from the communication channel should be positioned as specialised or niche means related to the above-mentioned category of special process control systems for critical facilities. In such systems, the computer platform of the QKD network must counteract all types of network threats, but we should point out here that there are still many unresolved problems.

The most urgent threats for mass telecommunications networks include viruses, trojans and other types of malicious programs distributed over Ethernet and Wi-Fi networks [167–171]. As pointed out in [168], it is necessary to search for fundamentally new approaches to the organisation of antivirus protection systems, because, for example, in 2012 the number of calls to the McAfee technical support service (USA) to analyse infected files exceeded 100 billion within a month. Measures are needed to counteract new types of viruses that do not allow antivirus programs to collect and analyse their malicious code by encrypting it with such machine-dependent keys that are unique to each infected computer [169, 170]. In addition, in 2017 WannaCry and a number of other malicious programs [171] made it possible to mass-encrypt files of users with the demand for redemption.

Another serious problem of protecting information in computer networks is associated with data leakage [172–175], arising from the malicious actions of disloyal personnel. In 2014, global losses due to data leakage amounted to about $18.5 billion. According to [174], in 2016, 128 million confidential data records were compromised in the Russian Federation as a result of leakage, which is 100 times higher than in the previous year. In work [176] numerous facts of targeted attacks were reported, including those using specific features of banking software.

It was stressed in [173] that the critical vulnerability for companies is represented by their own employees and insider information flowing through them. This makes it necessary to develop tools for analysing human behaviour, multiple verification of biometric information throughout the entire work session, as well as methods for counteracting digital photograph imitations. Developers, including Microsoft, are forced to introduce artificial intelligence technologies [177, 178] aimed at analysing network activity, traffic content and controlling employee loyalty, and minimising staff involvement in key processing and storage procedures.

B. Schneier, an acknowledged authority in the field of traditional cryptography, previously claimed [44] that 'Mathematical cryptography, even with all its current flaws, is the strongest link in most security chains…'. However, the traditional cryptographic methods of discrete logarithm, searching for integer factorisation and computations on elliptic curves also have some problems. In particular, in 2012 at www.cryptography.en, it was noted in the editorial review: 'Over the last few years, there have been no fundamentally new ideas in the problem of discrete logarithm search and factorisation…'. In addition, the resilience of all schemes of asymmetric cryptography is based only on assumptions about the impossibility of an effective computational solution of a number of so-called NP-complete problems, including factorisation, integer factorisation of large numbers and evaluation of logarithms in discrete fields of large size.

The NIST competition for the development of algorithms for post-quantum cryptography [37, 38], stable to classical cracking methods and to Shore's quantum algorithm, was initiated by the discovery of vulnerabilities in the previously recommended scheme of calculations on elliptic curves [41, 46], which was revealed precisely in the process of analysing algorithms for a quantum computer. On the other hand, new techniques [37, 38], promising as a means of amplifying non-quantum cryptography, do not provide solutions to problems with viruses, data leakage and disloyal personnel. In this case, one-time pad, or the perfect (i.e., unbreakable) Vernam cipher is still the most secure, and the use of truly random-number sequences in it can provide absolute cryptographic stability [74].

4. Trends in the development of combined schemes

4.1. Quantum random-number generators for cryptographic and computer systems

A truly random choice of bases and values of the encoding parameters in the QKD schemes and the Y-00 protocol is of a fundamentally important character [2, 4, 6, 31, 57, 59]. Therefore, considerable efforts have been made in the work on laser sources and QKD schemes to produce high-quality quantum random-number generators (QRNGs) [52, 53, 179–185].

In the review of 2016 [52], four main QRNG schemes are outlined:

– a scheme with the passage of a photon in the form of a superposition of horizontal and vertical polarisations through an asymmetric (polarising) beam splitter that transmits a horizontal component and reflects a vertical component, where the bit value is determined by a pair of single-photon detectors;

– a scheme with the passage of a photon in the form of a superposition of the reflected and transmitted parts through a symmetric (unpolarised) beam splitter, after which 0 or 1 is generated by the measurement for one of the two available photon paths;

– a scheme with one photodetector and measurement of the arrival time of a photon, where the random bits are determined by measuring the time interval between two consecutive detected photon counts; and

– a scheme in which the generated random number depends on the spatial position of the photon readable by the array of single-photon detectors.

A more detailed classification of the QRNG schemes can be found in [179].

The rate of generation of random numbers depends significantly on the chosen scheme [52]. For example, for a symmetric beam splitter [164, 180], which is used in commercial IDQ Quantis devices of the Swiss company ID Quantique, the random bit generation rate reaches 4 Mbit s^{-1} (in the PCI-E bus version) and is limited by the speed of single-photon uncooled detectors [181]. The resulting random number sequences satisfy the cryptographic tests (standards) of NIST, Diehard, New01, and such QRNGs are certified in several EU countries. At the same time, the performance of QRNGs with a change in the photon arrival time is more than 100 Mbit s^{-1} [182]. It can be increased to $\sim$1 Gbit s^{-1} due to the use of circuits based on measurements of fluctuations of the vacuum (zero) states of the field [183] or the phase of the laser light [53].

Zhang et al. [53] demonstrated a QRNG module measuring 304 × 250 × 78 mm with integrated temperature control and phase stabilisation systems, capable of generating real numbers at a rate of up to 3.2 Gbit s^{-1} and generating random numbers satisfying NIST cryptotests. The schematic and the general appearance of the QRNG device are shown in Fig. 9.

The light of the laser diode (LD) is injected into a compact asymmetric interferometer through a circulator and a 50/50 symmetrical beam splitter (BS), whose external ports are connected to two Faraday rotator mirrors (FRMs), which form a polarisation-insensitive Michelson interferometer. The thermoelectric cooler (TEC) is based on a Peltier element. The phase shifter (PS) is located in one of the arms of the interferometer, which provides a difference of about 0.8 ns in the time of passage of both arms. The photodetector (PD) (InGaAs, 9.5 GHz) is connected to the external port of the interferometer through the circulator, and the other external port of the interferometer is controlled by an optical power meter (PM) based on another photodetector with an ADC. Further, the field programmable gate array (FPGA) operates in the regime of the proportional-integral-differentiating controller (also called the PID controller), which controls the phase shifter (PS) stabilising the interferometer through the DAC and the high-voltage module (HVM).

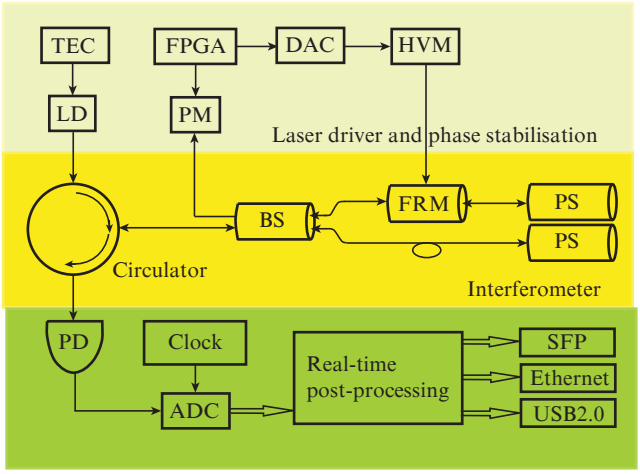

Figure 9. Schematic of the 3.2 Gbit s^{-1} QRNG module [53]: (TEC) thermoelectric cooler; (FPGA) field-programmable gate array; (DAC) digital-to-analog converter; (HVM) high-voltage module; (LD) laser module; (PM) power meter; (BS) beam splitter; (PS) phase shifter; (FRM) Faraday rotator mirror; (PD) photodetector; (ADC) analog-to-digital converter.

Random data from the photodetector (PD) arrive through an eight-bit ADC to the FPGA, performing a complex algorithm of pipeline real time post-processing. The stream of random numbers with a rate of up to 3.2 Gbit s^{-1} is output using a small form-factor pluggable optical transceiver (SFP). In addition, there is a gigabyte Ethernet port (968.7 Mbit s^{-1}) and a universal USB 2.0 serial port (259.5 Mbit s^{-1}).

According to estimates [181], the optimised values of the laser power and the sampling rate of the phase fluctuation data make it possible to generate raw (unprocessed) random numbers with rates up to 80 Gbit s^{-1}. However, as follows from [53, 181], the method of their subsequent processing, presented, for example, in [184], is very costly and significantly limits the QRNG performance. Therefore, in [53], a high-speed Virtex-6 FPGA (Xilinx, USA) was used for real-time processing with a specially developed pipeline-processing algorithm, which eventually provided a generation rate of up to 3.2 Gbit s^{-1}.

Thus, QRNGs are now an independent line in the development of quantum technologies, based on the same elemental and computational base as the QKD schemes. However, the possibility of deliberate attack of eavesdroppers on QRNGs has been discussed very scarcely [185].

4.2. One-time pads on the basis of QRNGs and calculations of multi-valued logic

Modern developments of QRNGs make it possible to take advantage of the method of protected multi-valued logic (MVL) encoding [54, 55], which is an analogue of the QKD method. This method even on an 8-bit platform allows one to increase the dimensions of the space of random one-time keys up to 10^{500} or more, and also to build secure logic control models for trusted devices of multi-agent and network-centric systems. The increase in the size of the key space is thus aimed at counteracting brute-force attacks (with direct key enumeration) [72], which is dangerous in the case of using cloud services or a quantum computer.

The MVL method is based on the k-valued Allen–Givone algebra [186], where the input and output variables of multi-valued logic functions take discrete truth values $\{0,1,2,\ldots,k-1\}$ [187]. An arbitrary function $y = F(x_1,\ldots,x_n)$ can be represented both in the form of a truth table, shown in Fig. 10 (top), and in the form of an equivalent logic expression composed of the constants $\{1,2,\ldots,k-1\}$, binary operators MINIMUM, MAXIMUM and unary operators $X(a,b)$, called 'literals' and given for input variables $x_1,\ldots,x_n$. A multi-valued logic function can be written in memory in the form of a matrix that consists of pairs of parameters (a_i,b_j) describing all the literals in its logic expression. It is sufficient to use functions with $n = 30$ input variables and $k = 256$ truth values 54] to implement the one-time pad method. In a minimised form, this function can be written in a memory volume of ~16 kbytes [54, 55]. Given the values of k and n, the logic function is calculated using a rigidly defined algorithm, which is convenient to use by default. In addition, such an algorithm is well 'parallelised' and allows the use of FPGAs.

Traditional cryptographic techniques usually work with key-space dimensions up to $\sim 10^{30}$, but modern mathematics essentially allows one to work with much larger dimensions [188–190], and the toolkit of multi-valued logics [55, 191, 192] is convenient for implementing high-security one-time pad techniques in global network systems with a large number of active agents. In addition, the MVL method makes it possible to generate $\sim 10^{70}$ different random one-time keys on an 8-bit platform without overwriting the memory of the encoding module, which is important for long-term autonomous work [54, 55, 193]. The gain in dimension in the MVL method in comparison with binary logic is due to the fact that for a multi-valued logic function the number of rows in its truth table is k^n instead of 2^n for Boolean logic [187], and the number of different logic functions is k^{k^n} instead of 2^{2^n}.

To encrypt messages by MVL, Alice and Bob, like in the QKD schemes, need to install separate QRNGs in their encoders/decoders. In addition, it is necessary to generate confidentially in advance a secret multi-valued logic function with randomly assigned parameters with the help of QRNGs [54, 55] and write it in the memory of the transceivers of both subscribers. In order to construct such a func-

tion, it is sufficient to generate two arrays of randomly assigned k-digit numbers, and then, according to certain rules, form a matrix of parameter pairs (a_i, b_j), which completely describes the function and the truth table equivalent to it.

The method of formation and use of random one-time keys in the MVL method, presented in Fig. 10 (top), is described in detail in [54, 55]. At the beginning of the secure communication session, Alice, with the help of her QRNG, generates a one-time key-prompt, i.e., a sequence of $n-1$ randomly assigned k-digit numbers. Alice introduces this data set as input variables $x_2, \ldots, x_n$ into a logic expression for the secret function. Then, successively substituting the values of x_1 from 0 to $k-1$, it calculates a sequence of k random values of the output variable $y = f(x_1, \ldots, x_n)$.

This procedure is clearly illustrated in Fig. 10, where the secret function $y = f(x_1, \ldots, x_n)$ is represented as a truth table in which the set of $x_2, \ldots, x_n$ values is separated by a dashed oval, and the random sequence $f(0,0,\ldots,0)$, $\ldots, f(0, 0, \ldots, k-1)$, calculated by searching all possible x_1, is denoted by an oval in column y.

A random one-time key R (Fig. 10) represents a random permutation of a fixed initial sequence $R_0 = \{0, 1, \ldots, k-1\}$, produced in the cells of the memory chip with the help of a random sequence $f(0,0,\ldots,0), \ldots, f(0,0,\ldots,k-1)$. For clarity, Fig. 10 shows an example of an eight-bit platform, where Alice computed the key $R = \{102,5,\ldots,237\}$, with which she encrypts a fragment of 256 eight-bit numbers. Next, Alice openly sends the used key-prompt $x_2, \ldots, x_n$ together with the encoded fragment to Bob. Bob substitutes the key-prompt in his copy of the secret function and calculates the key R used by Alice for encoding. With its help Bob further finds the inverse (i.e., decoding) sequence.

In addition to the original way of realising the high dimensions of random key space [54, 55], the MVL method provides new data for the development of cryptographically important schemes of bit commitment and position-dependent cryptography. Initially, the authors of the pioneering work on the quantum key distribution [2], along with the distribution of the keys, considered it possible to implement a bit commitment scheme, which is necessary when both partners do not fully trust each other. The main idea here is the possibility to send the receiver a 'box' with confidential information, the key to which is sent later, while ensuring the integrity of the information stored in it. The inability to solve this problem with the help of the QKD schemes discussed in reviews [6, 70] limited the functions of quantum cryptography to only the key distribution problems.

However, among the developments of MVL there is an algorithm that seems to be used to solve the above problem in trusted network nodes that are not unconditionally cryptographically secure, but are protected at the level of one-time pad codes with a record key space dimension. This algorithm was proposed in [191] for controlled ordering/disordering of the structure of fuzzy logic knowledge in the scheme of remote switching off/switching on of robotic devices. Because the set of fuzzy logic rules 'if…, then…' and associated functions, used by the robot's control system, can represent a valuable knowledge structure, then when the robot is switched off it is advisable to encrypt it, making it unavailable for eavesdroppers. Such an algorithm for MVL-based secure encoding can be implemented in an

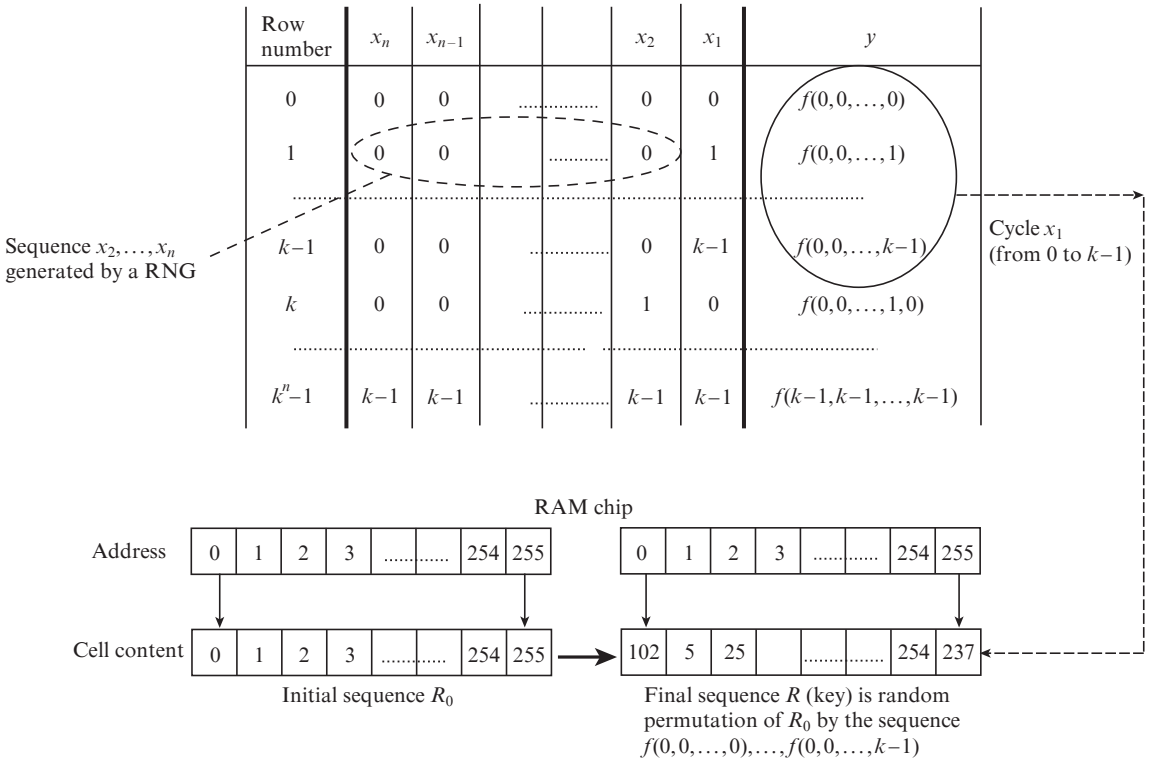

Figure 10. Key generation in the MVL method by computation of a random sequence $f(0,0,\ldots,0), \ldots, f(0,0,\ldots,k-1)$ with the help of a randomly selected key-prompt $x_2, \ldots, x_n$ and a sequential search for x_1 from 0 to $k-1$ [55].

atmospheric laser communication link connecting a remote digital 'key' and a digital 'lock' installed on the robot. The 'lock' regulates the access of its internal subsystems to the recoding tables stored in the random access memory (RAM). With the help of several multi-valued logic functions and auxiliary sequences, the 'key' allows one to remotely erase and subsequently restore transcoding sequences in RAM that control the access of the agent subsystems to the control knowledge structure.

For the algorithm [191] to implement the basic part of the bit commitment scheme [70], it is enough to use it in the device of the sender (Alice) and to send the already encrypted data structure (i.e., the secret contents of the 'box'!) to the recipient (Bob), and at the stage of its deciphering, to send him a set of missing transcoding sequences to decode it. To fully implement the entire bit commitment scheme, it is necessary to convince Bob in the absence of abuses by Alice, providing him with an algorithm for verifying the uniqueness of the message being restored. The development of such an algorithm has not yet been completed.

The approach to solving another important problem, namely position-dependent cryptography, was presented in [192] when discussing the algorithm for constructing a multiparametric terrain map described by the multi-valued logic formalism. If the coordinates, time and characteristics of the terrain map objects are described as part of the input variables of the truth table of the multi-valued logic function, and the other part of its input variables is used to enter the password, the corresponding logic expression can serve as a protected digital map of high information capacity. If necessary, such a digital map of the area can be further MVL encrypted by encoding a set of logic constants and parameters of the literals.

To implement intelligent algorithms for the behavior of agents of multi-agent systems and to work with inaccurately measured positioning data of objects, the corresponding fuzzy logic apparatus (a set of membership functions and fuzzy rules 'if…, then…') can be written as logic expressions of the Allen–Givone algebra [193] within the framework of the heterogeneous logic agent model [194]. Thus, the MVL method allows one, within the framework of a single mathematical formalism, to describe (for the network of agents) their encoding protocols by the one-time pad method, the rules of teamwork of agents and the rules of the agent's response to the readings of digital and analog sensors. At the same time, the MVL method guarantees obtaining an exact logic model for an arbitrary number of variables and truth table contents, although for fast computations a costly procedure of logical minimisation of the obtained function by the consensus method [186] is needed, which requires the use of multi-criterion optimisation methods [195].

4.3. Problems, trends and challenges for the development of QKD systems and combined circuits

As was shown above, modern QKD schemes are a network means of key distribution in a computer network, rather than an independent type of communication networks. Therefore, in order to solve new practical tasks and design appropriate types of networks, for example, network-centric systems [8–10] or photonic networks [11–13], new methods of information processing are used in addition to the QKD and computer networks, including multi-agent approaches and Y-00 and MVL encryption protocols. With this in mind, let us single out a number of problems that restrain the development of quantum optics and communication networks and require priority solutions.

1. In the field of QKD research, the development of working quantum memory devices for repeaters and network branching QKD schemes [6, 8–12, 18–27, 31–33, 35, 69, 196] is of great importance. Such devices would solve the problem of the transmission distance of the distribution of quantum keys over fiber-optic links and the deployment of multi-user communication networks, and also move from trusted repeaters on the basis of ordinary computers to quantum trusted nodes. In this case, the problems of the vulnerability of quantum memory devices call for a separate analysis.

2. For quantum lines, the problem of increasing the QKD rate, the maximum value of which (more than 1 Mbit s^{-1} in the laboratory and 304 kbit s^{-1} in the field [24]) is very urgent for stream encryption by the one-time pad method even for fibre lengths less than 50 km [24, 35, 103, 121, 122]. Modern fibre-optic communication lines are principally capable of mastering the rates of 100 Gbit s^{-1} and more, which implies that new QKD schemes of greater performance are needed.

3. The increase in the length of an 80–100-km-long quantum channel is accompanied by a sharp decrease in the QKD rate to a level of 1–10 kbit s^{-1} and less [18–27, 33, 35, 103, 106]. This is sufficient only for niche applications, examples of which are multi-agent photonic network control systems [11, 12] and secure telephony systems [19, 21, 24, 25]. In addition, while the use of less efficient AES algorithms instead of one-time pad in the trusted node or trusted third party architectures [8, 11, 19, 21–25] allows the critical power grid management infrastructure [8–10] and secure video transmission [19, 21, 24] to be serviced, the level of the system security as a whole, determined by the weakest components, is reduced in this case to the level of security of conventional networks. An alternative solution is either the development of fundamentally new QKD schemes, or the development of space systems [15–17, 34,], providing the QKD transmission distance of more than 1000 km under the space vacuum conditions.

4. The problem of efficient branching of a QKD link into a multi-user network is still not solved [8–12, 18–27, 35] due to the absence of practical quantum memory devices and the presence of high losses in optical fibres using optical switches, circulators and multiplexers. Field networks with a branching factor of no more than 1:4 are deployed for QKD [18, 19, 21, 22, 24], which is much smaller than the branching factor of 1 : 128, provided by the GPON standard for passive fibre-optic links. At the same time, based on the purely computer architecture of the trusted person (server) in the star topology, a branching factor of up to 1:1000 is provided [8–10].

5. Complete hacking of two commercial QKD mock-ups in 2010–2011 [152, 153] drew significant attention of researchers to the development of techniques of protection against various types of quantum and non-quantum attacks [32, 33, 147–151, 154–159, 161, 162], and also showed the importance of correlation of vulnerability studies with experimental research of real fibre-optic links and networks. However, until now, new vulnerabilities have been identified

for the already known and new QKD schemes [160, 163]. The methods of protection against possible quantum attacks have not been sufficiently investigated. In addition, the literature lacks the description of techniques that allow the reader, independently of the developers and equipment manufacturers, to assess the vulnerabilities of the QKD scheme in question.

6. QRNG devices [52, 53, 179–185], implemented on the elemental basis of the QKD schemes, have reached gigabit performance and are suitable not only for the maintenance of the QKD protocols, but also for use in many other areas of computer technology. Reducing their size and weight will open the possibility for wider use, including in stationary and mobile devices of network-centric systems. However, the vulnerability of the QRNG itself to quantum and non-quantum attacks still remains poorly understood.

7. In modern multi-node QKD schemes, a large amount of effort is spent to design auxiliary systems for stabilising temperature, phase, and polarisation of light in a fibre optic link [8–13, 19, 83]. In this case, a set of QKD equipment for one pair of subscribers costs tens of thousands of dollars and Euros. At the same time, additional branching of a fibre optic link or its repair by replacing individual short segments is problematic due to a significant increase in optical losses in connectors or weldings [83].

8. The improvement of photodetectors, as well as fibre-optic and integrated optical components, is of great importance for the further development of QKD schemes, the level of the development of which is discussed in reviews [33, 35]. A separate problem is also the improvement of the optoelectronic elemental base of photonic networks.

9. The relevant literature almost lacks open publications on the analysis of the vulnerabilities of a computer network that is interfaced with a QKD system. At the same time, in the framework of the complex approach [71, 72] to solving the problems of information security of computer systems practiced in the Russian Federation, quantum and conventional means of information protection should be analysed as a single whole. When working with the global network, the most dangerous are the effects of malicious code and malicious actions of personnel [167–178].

For QKD-based communication networks, the development of global telecommunications means [7, 24, 33, 35, 63–70, 143, 144] is the most important direction, requiring gigabit key distribution rates, which exceeds by several orders of magnitude the capabilities of the known developments of QKD. To date, the most secure one-time pad method can be used only in specialised niche network schemes with a limited flow of particularly valuable data [19, 21, 24, 25], the probability of attempts of direct readout of which from the fibre optic link is large. For mass telecommunication networks, where the direct eavesdropping of the channel by an intruder is less likely, the field of application of the one-time pad method is substantially limited by the cost of specific developments. This makes a wide range of combined schemes with different levels of cryptographic resistance potentially important.

For combined QKD-based schemes created on the basis of photonic networks [11–13], a promising direction is the use of multi-agent hierarchical schemes. This is due, on the one hand, to significant optical losses in splitters and multiplexers, forcing to use complex schemes for switching optical channels, and on the other hand, to the need for multi-level intelligent control of the complex structure of switching devices and protocols. The second important aspect of the application of multi-agent schemes for managing photonic networks is the ability to implement stand-alone trusted nodes and to minimise the access of maintenance personnel to key structures and transmitted data. In addition, using the agent model, it is possible to facilitate the development of intelligent means of detecting and classifying unauthorised actions of disloyal personnel [172–177].

In the project of a network-centric system for secure power grid management [8–10], a combined scheme with a trusted third party was forcedly interfaced with traditional AES encryption, despite the need for maximum protection for all network components. Accordingly, for network-centric critical infrastructure management systems, the task of using the one-time pad schemes at all levels of the protocol processing architecture is urgent. It is for this type of communication networks that the schemes that combine the operation of QKD with the MVL method for implementing trusted nodes are most in demand. Such systems also call for the development of autonomous intelligent devices for verification of subscribers and sensor control of the physical integrity of the nodes of the QKD network.

Another important task of developing global network-centric systems is connected with the need to protect the communication channels of stationary and mobile agents [113, 114]. The development of space network-centric systems can be a priority in the deployment of trunk (backbone) communication lines for a network of stationary objects managing logistics and unmanned vehicles. However, for terrestrial mobile robots of a network-centric system operating under conditions of vibration and dust, connection to the cosmic trunk lines of quantum key distribution [15–17, 34] is problematic. In this case, it is possible and feasible to implement the one-time pad method based on the QRNG, MVL and non-quantum atmospheric communication lines. As it is possible to assume, for specialised types of networks, it is technically and economically feasible to duplicate data transmission regimes by intense laser pulses using the MVL protocol triggered in the event of external artificial interference or long-range transmission.

Of importance is the deployment of combined network systems for the implementation of position-dependent cryptography and bit commitment schemes that now cannot be realised in QKD networks [70]. Here, the method of a multi-valued multi-parameter encrypted map can be applied [188], describing as a logical expression the relationship of spatial coordinates and time with the characteristics of objects displayed on the terrain map. For remote access to data of such a secret card stored in a trusted node or in an agent, part of the access code can be entered through a quantum line with limited performance, and the other part of the code can be transmitted by the MVL method through a faster non-quantum line.

MVL circuits can also be used to combine low-optical-loss QKD links and FOCL segments with high-optical-loss optical connectors, multiplexers, or weldings into a single network.

5. Conclusions

1. Theoretical and experimental studies of quantum optics, as well as the development of laser and fibre technology and single-photon detectors, have recently resulted in the successful implementation of a number of protocols for transmitting qubits over considerable distances. Various QKD schemes realised on the basis of fibre-optic links with low (0.2 dB km^{-1}) and ultra-low (0.16 dB km^{-1}) optical losses have been investigated. The operation of QKD links as part of network fibre-optic communication lines with cryptographic encoding by one-time pad and AES methods, including telephone and image transmission lines, has been demonstrated. A number of projects of multi-user QKD networks have been implemented.

2. The introduction of QKD schemes into mass telecommunication fibre-optic networks is currently constrained by the following factors:

– the actual key distribution rate in a fibre-optic link up to 50 km long is ~1 Mbit s^{-1}, whereas gigabit telecommunication FOCLs with stream encryption by the most secure 'one-time pad' method require a QKD rate of 1 Gbit s^{-1} and higher;

– the length of a fibre-optic link exceeding 80–100 km leads to a sharp decrease in the QKD rate to a level of ~1 kbit s^{-1}, which limits practical applications;

– the absence of working quantum memory devices for repeaters and trusted nodes hinders an increase in the length of QKD links and their branching into a network, as well as forcedly results in their integration with traditional trusted servers;

– the high requirements of the QKD schemes to the level of optical loss in a fibre optic link sharply limit the number of welded and detachable optical fibre connectors.

3. The presence of the above unresolved problems is the reason for the development of joint network schemes combining sophisticated computer processing methods with QKD schemes. Such network topologies demonstrate forced convergence of quantum optics and computer methods to solve all the more complicated tasks of information security. In recent years, variants of combined schemes have been developed, such as network-centric systems for managing power grid networks and photonic networks for mass telecommunications and cloud services, where software and hardware multi-agent systems imitating human intellectual functions are used to effectively manage the complex structure of cryptographic facilities.

4. For mass telecommunication applications, several variants of combined quantum-classical network devices of secure encoding based on the Y-00 protocol have been designed in the US and Japan. These devices support double cryptographic encoding combining AES encryption with intensity or phase modulation of an optical signal by quantum laser noise of a transmitting device. At the same time, for the Y-00 protocol with intensity modulation, the AES standard was encrypted with rates up to 2.5 Gbit s^{-1} for a fibre-optic link of length up to 120 km without a fibre amplifier. In contrast to the QKD schemes, these developments allow the use of standard fibre amplifiers and multiplexers.

5. The platform of modern hardware developments of QRNGs can accommodate combined network schemes of multi-valued logic secure encoding that allow the implementation of the analogue of the one-time pad method with a space of random high-dimensional (more than 10^{500}), one-time keys on an 8-bit platform. Such schemes calculate discrete functions of the k-valued Allen–Givone algebra and allow the long-term operation of the transmitting devices of autonomous agents without overwriting the secret functions. The MVL methodology is well compatible with multi-agent approaches of artificial intelligence, as well as with the model of a multi-parameter digital terrain map. Due to this, new opportunities appear to solve the problem of position-dependent cryptography and bit commitment, which are important from the point of view of constructing trusted nodes.

In general, the relevance and variety of information security problems in the field of global communication networks require a significant expansion of the scope of developments and improvements of both purely quantum cryptographic devices and combined optoelectronic systems for which the achievements of quantum technologies are supplemented by modern computer technologies and artificial intelligence methods.

Acknowledgements. The work was supported by the Ministry of Education and Science of the Russian Federation (unique identifier RFMEFI61615X0060).

6. References

1. Wiesner S. *SIGACT News*, **15**, 78 (1983).
2. Bennett C.H., Brassard G., in *Proc. IEEE Intern. Conf. Comput., Syst. Signal Proces*. (New York: IEEE, 1984) p. 175.
3. Bennett C.H., Brassard G. *IBM Tech. Discl. Bull*., **28**, 3153 (1985).
4. Bennett C.H., Bessette F., Salvail L., Brassard G., Smolin J. *J. Cryptology*, **5**, 3 (1992).
5. Brassard G.A. https://www.cs.mcgill.ca/~crepeau/CRYPTO/Biblio-QC.html.
6. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys*., **74** (1), 145 (2002).
7. Agrell E., Karlsson M., Chraplyvy A.R., Richardson D.J., Krummrich P.M., Winzer P., Roberts K., Fischer J.K., Savory S.J., Eggleton B.J., Secondini M.,Kschischang F.R., Lord A., Prat J., Tomkos I., Bowers J.E., Srinivasan S., Brandt-Pearce M., Gisin N. *J. Opt*., **18**, 063002 (2016).
8. Hughes R.J., Nordholt J.E., McCabe K.P., Newell R., Peterson C.G., Somma R.D., in *Proc. 3rd Int. Conf. Quantum Cryptography* (Canada, Waterloo, 2013) LA-UR-13-22718; http://2013.qcrypt.net/program/#invited.
9. Hughes R.J., Nordholt J.E., McCabe K.P., Newell R., Peterson C.G., Somma R.D., in *Proc. Frontiers in Optics 2013* (USA, Orlando, Florida, 2013) FW2C, FW2C.1; https://www. osapublishing.org/conference.fm?meetingid=56&yr=2013#FW2C or https://doi.org/10.1364/FIO.2013.FW2C.1.
10. Hughes R.J., Nordholt J.E., McCabe K.P., Newell R., Peterson C.G., Somma R.D. http://lanl.arxiv.org/ftp/arxiv/papers/1305/1305.0305.pdf.
11. Kitayama K-I., Sasaki M., Araki S., Tsubokawa M., Tomita A., Inoue K., Harasawa K., Nagasako Y., Takada A. *J. Lightwave Technol*., **29** (21), 3210 (2011); DOI: 10.1109/JLT.2011.2166248; https://www.researchgate.net/publication/224255782.
12. Kitayama K.-I., Hiramatsu A., Fukui M.,Yamanaka N., Jinno M., Tsuritani T., Okamoto S., Koga M. https://ieeexplore.ieee.org/document/6825163/.
13. Hughes R.J., Chapuran T.E., Dallmann N., Hiskett P.A., McCabe K.P., Montano P.M., Nordholt J.E., Peterson C.G., Runser R.J., Sedillo R., Tyagi K., Wipf C.C. *Proc. SPIE*, **5893**, 589301 (2005).
14. Makkaveev V. *Komponent. Tekhnol*., **55**, 142 (2006); http: // www.kit-e.ru/articles/telecommunication/2006_2_142.php.

15. Yin J., Cao Y., Li Y.-H., Liao S.-K., Zhang L., Ren J.-G., Cai W.-Q., Liu W.-Y., Li B., Dai H., Li G.-B., Lu Q.-M., Gong Y.-H., Xu Y., Li S.-L., Li F.-Z., Yin Y.-Y., Jiang Z.-Q., Li M., Jia J.-J., Ren G., He D., Zhou Y.-L., Zhang X.-X., Wang N., Chang X., Zhu Z.-C., Liu N.-L., Chen Y.-A., Lu C.-Y., Shu R., Peng C.-Z., Wang J.-Y., Pan J.-W. *Science*, **356** (6343), 1140 (2017); DOI: 10.1126/science.aan3211; http://science.sciencemag.org/content/356/6343/1140/tab-pdf.
16. Liao S.-K., Cai W.-Q., Liu W.-Y., Zhang L., Li Y., Ren J.-G., Yin J., Shen Q., Cao Y., Li Z.-P., Li F.-Z., Chen X.-W., Sun L.-H., Jia J.-J., Wu J.-C., Jiang X.-J., Wang J.-F., Huang Y.-M.,Wang Q., Zhou Y.-L., Deng L., Xi T., Ma L., Hu T., Zhang Q., Chen Y.-A., Liu N.-L., Wang X.-B., Zhu Z.-C., Lu C.-Y., Shu R., Peng C.-Z., Wang J.-Y., Pan J.-W. *Nature*, **549**, 43 (2017); DOI: 10.1038/nature23655; http://www.nature.com/articles/nature23655.
17. Ren J.-G., Xu P., Yong H.-L., Zhang L., Liao S.-K., Yin J., Liu W.-Y., Cai W.-Q., Yang M., Li L., Yang K.-X., Han X., Yao Y.-Q., Li J., Wu H.-Y., Wan S., Liu L., Liu D.-Q., Kuang Y.-W., He Z.-P., Shang P., Guo C., Zheng R.-H., Tian K., Zhu Z.-C., Liu N.-L., Lu C.-Y., Shu R., Chen Y.-A., Peng C.-Z., Wang J.-Y., Pan J.-W. *Nature*, **549**, 70 (2017); DOI: 10.1038/nature23675, http://www.nature.com/articles/nature23675.
18. Elliott C., Colvin A., Pearson D., Pikalo O., Schlafer J., Yeh H. *Proc. SPIE*, **5815**, 138 (2005); https://arxiv.org/ftp/quant-ph/papers/0503/0503058.pdf.
19. Peev M., Pacher C., Alléaume R., Barreiro C., Bouda J., Boxleitner W., Debuisschert T., Diamanti E., Dianati M., Dynes J.F., Fasel S., Fossier S., Fürst M., Gautier J.-D., Gay O., Gisin N., Grangier P., Happe A., Hasani Y., Hentschel M., Hübel H., Humer G., Länger T., Legré M., Lieger R., Lodewyck J., Lorünser T., Lütkenhaus N., Marhold A., Matyus T., Maurhart O., Monat L., Nauerth S., Page J.-B., Poppe A., Querasser E., Ribordy G., Robyr S., Salvail L., Sharpe A.W., Shields A.J., Stucki D., Suda M., Tamas C., Themel T., Thew R.T., Thoma Y., Treiber A., Trinkler P., Tualle-Brouri R., Vannel F., Walenta N., Weier H., Weinfurter H., Wimberger I., Yuan Z.L., Zbinden H., Zeilinger A. *New J. Phys*., **11**, 075001(2009).
20. Chapuran T.E., Toliver P., Peters N.A., Jackel J., Goodman M.S., Runser R.J., McNown S.R., Dallmann N., Hughes R.J., McCabe K.P., Nordholt J.E., Peterson C.G., Tyagi K.T., Mercer L., Dardy H. *New J. Phys*., **11**, 105001 (2009).
21. Chen T.-Y., Wang J., Liang H., Liu W.-Y., Liu Y., Jiang X., Wang Y., Wan X., Cai W.-Q., Ju L., Chen L.-K., Wang L.-J., Gao Y., Chen K., Peng C.-Z., Chen Z.-B., Pan J.-W. *Opt. Express*, **18** (26), 27217 (2010); DOI: https://doi.org/10.1364/OE.18.027217; https://www.osapublishing.org/oe/abstract.cfm?uri=oe-18-26-27217.
22. Mirza A., Petruccione F. *J. Opt. Soc. Am. B*, **27** (6), A185 (2010).
23. Lancho D., Martinez J., Elkouss D., Soto M., Martin V. *First Int. Conf. Quantum Comm*. (Italy. Naples, 2009) p. 142; DOI: 10.1007/978-3-642-11731-2_18; https://arxiv.org/abs/1006.1858v2.
24. Sasaki M., Fujiwara M., Ishizuka H., Klaus W., Wakui K., Takeoka M., Miki S., Yamashita T., Wang Z., Tanaka A., Yoshino K., Nambu Y., Takahashi S., Tajima A., Tomita A., Domeki T., Hasegawa T., Sakai Y., Kobayashi H., Asai T., Shimizu K., Tokura T., Tsurumaru T., Matsui M., Honjo T., Tamaki K., Takesue H., Tokura Y., Dynes J.F., Dixon A.R., Sharpe A.W., Yuan Z.L., Shields A.J., Uchikoga S., Legré M., Robyr S., Trinkler P., Monat L., Page J.-B., Ribordy G., Poppe A., Allacher A., Maurhart O., Länger T., Peev M., Zeilinger A. *Opt. Express*, **19** (11), 10387 (2011).
25. Wang S., Chen W., Yin Z.-Q., Li H.-W., He D.-Y., Li Y.-H., Zhou Z., Song X.-T., Li F.-Y., Wang D., Chen H., Han Y.-G., Huang J.-Z., Guo J.-F., Hao P.-L., Li M., Zhang C.-M., Liu D., Liang W.-Y., Miao C.-H., Wu P., Guo G.-C., Han Z.-F. *Opt. Express*, **22** (18), 021739 (2014).
26. Kiktenko E.O., Pozhar N.O., Duplinskiy A.V., Kanapin A.A., Sokolov A.S., Vorobey S.S., Miller A.V., Ustimchik V.E., Anufriev M.N., Trushechkin A.T., Yunusov R.R., Kurochkin V.L., Kurochkin Yu.V., Fedorov A.K. *Quantum Electron*., **47** (9) 798 (2017) [*Kvantovaya Elektron*., **47** (9), 798 (2017)]; DOI: 101070 / QEL16469.
27. Wang S., Chen W.,Yin Z.-Q., Zhang Y., Zhang T., Li H.-W., Xu F.-X., Zhou Z., Yang Y., Huang D.-J., Zhang L.-J., Li F.-Y., Liu D., Wang Y.-G., Guo G.-C., Han Z.-F. *Opt. Lett*., **35** (14), 2454 (2010).
28. Kiktenko E.O., Trushechkin A., Kurochkin Y., Fedorov A. *J. Phys.: Conf. Ser*., **741**, 012081 (2016).
29. Williams C.J. https://math.nist.gov/mcsd/Seminars/2004/2004-03-23-williams-presentation.pdf.
30. Graham-Rowe D. https://www.technologyreview.com/s/415073/quantum-cryptography-for-the-masses/.
31. Scarani V., Bechmann-Pasquinucci H., Cerf N.J., Dŭsek M., Lütkenhaus N., Peev M. *Rev. Mod. Phys*., **81**, 1301 (2009); https://arxiv.org/abs/0802.4155v3.
32. Scarani V., Kurtsiefer C. *Theor. Comp. Sci*., **560**, 27 (2014); https://doi.org/10.1016/j.tcs.2014.09.018.
33. Lo H.-K., Curty M., Tamaki K. *Nature Photon*., **8**, 595 (2014).
34. Bedington R., Arrazola J.M., Ling A. *npj Quant. Informat*., **3**, 30 (2017); DOI: 10.1038/s41534-017-0031-5; https://www.nature.com/articles/s41534-017-0031-5.
35. Diamanti E., Lo H.-K., Qi B., Yuan Z. *npj Quant. Informat*., **2**, 16025 (2016).
36. https://www.ncsc.gov.uk/whitepaper/quantum-key-distribution.
37. https://csrc.nist.gov/projects/post-quantum-cryptography.
38. Chen L., Jordan S., Liu Y.-K., Moody D., Peralta R., Perlner R., Smith-Tone D. DOI: 10.6028/NIST.IR.8105; https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.
39. https://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution.
40. Länger T., Lenhart G. *New. J. Phys*., **11** (5), 055051 (2009).
41. http://www.nist.gov.
42. Black P.E., Kuhn D.R., Williams C.J. *Adv. Comput*., **56**, 189 (2002).
43. Rumyantsev K.E., Rozova Ya.S. *Elektrotekh. Inform. Kompleksy Sist*., **7** (1), 58 (2011).
44. Schneier B. http://www.schneier.com/crypto-gram-0312.html#6.
45. Byrd K. http://old.computerra.ru/xterra/206486/.
46. Byrd K. https://3dnews.ru/940050.
47. Russell S., Norvig P. *Artificial Intelligence: A Modern Approach* (New Jersey: Prentice Hall, 1995; Moscow: Izd. dom Vil'yams, 2006).
48. Barbosa G.A., Corndorf E., Kumar P., Yuen H.P. *Phys. Rev. Lett*., **90** (22), 227901 (2003).
49. Corndorf E., Barbosa G., Liang C., Yuen H.P., Kumar P. *Opt. Lett*., **28** (21), 2040 (2003).
50. Hirota O., Sohma M., Fuse M., Kato K. *Phys. Rev. A*, **72**, 022335 (2005).
51. Futami F., Kato K., Hirota O. *Proc. SPIE*, **9980**, 99800O (2016); DOI: https://doi.org/10.1117/12.2237852; https://www.spiedigitallibrary.org/confeence-proceedings-of-spie/9980/99800O/A-novel-ransceiver-of-the-Y-00-quantum-stream-cipher/10.1117/12.2237852.full.
52. Ma X., Yuan X., Cao Z., Qi B., Zhang Z. *npj Quant. Informat*., **2**, 16021 (2016).
53. Zhang X-G., Nie Y-Q., Zhou H., Liang H., Ma X., Zhang J., Pan J.-W. *Rev. Sci. Instrum*., **87**, 076102 (2016).
54. Antipov A.L., Bykovsky A.Yu., Vasiliev N.A., Egorov A.A. *J. Rus. Laser Research*, **27** (5), 492 (2006).
55. Bykovsky A.Yu., Egorov A.A., Rager B.Yu. *Pacific Sci. Rev*., **3**, 140 (2011).
56. Alleaume R., Branciard C., Vasiliev N.A., Egorov A.A. *Theor. Comp. Sci*., **560**, 62 (2014); https://doi.org/10.1016/j.tcs.2014.09.018.
57. Jain N., Stiller B., Khan I., Elser D., Marquardt C., Leuchs G. *Contemp. Phys*., **57** (3), 366 (2016); https://doi.org/10.1080/00107514.2016.1148333.
58. Kilin S.Ya. *Phys. Usp*., **52** (5), 435 (1999) [*Usp. Fiz. Nauk*, **169** (5), 507 (1999)].
59. Molotkov S. *Phys. Usp*., **49** (7), 750 (2006) [*Usp. Fiz. Nauk*, **176** (7), 777 (2006)].
60. Lo H.-K., Zhao Y. *Encyclop. Comp. Syst. Sci*., **8**, 7265 (2009); https://arxiv.org/abs/0803.2507v4.
61. Korolkov A.S. *Information Security*, **6**, 42 (2013); http://www.itsec.ru/articles2rypWosovremen-nom-etape-razvitiya-prikladnoy-kvantovoy-kriptografii/.

62. Gupta N.L., Mehrotra D.R., Saxena A. *INFOCOMP* [S.l.], **8** (1), 65 (2009); http://www.dcc.ufla.br/infocomp/index.php/INFOCOMP/article/view/252.
63. Kulik S.P. *Fotonika*, **4**, 28 (2010).
64. Singh H., Gupta D.L., Singh A.K. *IOSR J. Comp. Eng.*, **16** (2), XI, 01 (2014).
65. Iqbal A., Aslam M.J., Nayab H.S. https://www.researchgate.net/publication/298734157.
66. Kute S., Desai C.G. *Indian J. Sci. Technol*., **10** (3) (2017); DOI:1 0.17485/ijst/2017/v10i3/110635.
67. Kulik S.P. *Fotonika*, **2**, 36 (2010).
68. Kulik S.P. *Fotonika*, **3**, 56 (2010).
69. Tokura Y. *NTT Techn. Rev*., **9** (9), 1 (2011).
70. Broadbent A., Schaffner C. *Designs, Codes Cryptogr*., **78** (1), 351 (2016).
71. Gerasimenko V.A., Malyuk A.A. *Osnovy zashchity informatsii* (Fundamentals of Information Protection) (Moscow: OOO Inkombuk, 1997).
72. Ryabko B.Ya., Fionov A.N. *Kriptograficheskie metody zashchity informatsii* (Cryptographic Methods of Information Protection (Moscow: Goryachaya liniya-Telecom, 2005).
73. Makkaveev A.P., Molotkov S.N., Pomozov D.I., Timofeev A.V. *Zh. Eksp. Teor. Fiz*., **128** (2), 263 (2005).
74. Braude-Zolotarev Yu. I*nformation Security*, **4**, 56 (2014).
75. Wooters W.K., Zurek W.H. *Nature*, **299**, 802 (1982).
76. Zbinden H., Bechmann-Pasquinucci H., et al. *Appl. Phys. B*, **67** (6), 743 (1998).
77. Eraerds P., Walenta N., Legré M., Gisin N., Zbinden H. *New J. Phys*., **12**, 063027 (2010).
78. Lütkenhaus N. *Phys. Rev. A*, **59**, 3301 (1999); DOI: https://doi.org/10.1103/PhysRevA.59.3301; https://journals.aps.org/pra/abstract/10.1103/PhysRevA.59.3301.
79. Zhao F., Li J.-L. *Proc. SPIE*, **7846**, 78460J-1 (2010); DOI: 10.1117/12.866065.
80. Muga N.J., Fereira M.F.-S., Pinto A.N. *J. Lightwave Technol*., **29** (3), 355 (2011).
81. Gobby C., Yuan Z.L., Shields A.J. *Appl. Phys. Lett*., **84**, 3762 (2004).
82. Bennet C.H., Brassard G., Robert J.-M. *SIAM J. Comput*., **17** (2), 210 (1988).
83. Jacak M., Melniczuk D., Jacak J., Janutka A., Jóźwiak I., Gruber J., Jóźwwiak P. *Opt. Quantum Electron*., **48**, 363 (2016).
84. Inamori H., Lütkenhaus N., Mayers D. *Eur. Phys. J. D*, **41**, 599 (2007).
85. Shor P.W., Preskill J. *Phys. Rev. Lett*., **85** (2), 441 (2000).
86. Lim C.C.-W., Curty M., Walenta M., Xu F., Zbinden H. *Phys. Rev. A*, **89**, 022307 (2014).
87. Lütkenhaus N. *Phys. Rev. A*, **61**, 052304 (2000); DOI: https://doi.org/10.1103/PhysRevA.61.052304; https://journals.aps.org/pra/abstract/10.1103/PhysRevA.61.052304.
88. Brassard G., Lütkenhaus N., Mor T., Sanders B.C. *Phys. Rev. Lett*., **85** (6), 1330 (2000).
89. Renner R., Gisin N., Kraus B. *Phys. Rev. A*, **72**, 012332 (2005).
90. Scarani V., Renner R. *Phys. Rev. Lett*., **100** (20), 200501 (2008).
91. Beaudry N.J., Moroder T., Lutkenhaus N. *Phys. Rev. Lett*., **101** (9), 093601 (2008).
92. Hwang W.Y. *Phys. Rev. Lett*., **91** (5), 057901 (2003).
93. Molotkov S.N. *Pis'ma Zh. Eksp. Teor. Fiz*., **93** (3), 194 (2011).
94. Inoue K., Waks E., Yamanoto Y. *Phys. Rev. A*, **68** (2), 022317 (2003).
95. Lo H.-K., Curty M., Qi B. *Phys. Rev. Lett*., **108** (13), 130503 (2012).
96. Comandar L.C., Lucamarini M., Sharpe A.W., Tam S., Yuan Z.L., Penty R.V., Shields A.J. *Nature Photon*., **10**, 312 (2016); https://arxiv.org/pdf/1509.08137.pdf.
97. Ekert A.K. *Phys. Rev. Lett*., **67** (6), 661 (1991).
98. Acìn A., Brunner N., Gisin N., Massar S., Pironio S., Scarani V. *Phys. Rev. Lett*., **98**, 230501 (2007).
99. Zhao Y., Fung C.H., Qi B. *Phys. Rev. A*, **78**, 042333 (2008); DOI: 10.1103/PhysRevA.78.042333.
100. Fossier S., Diamanti E., Debuisschert T., Villing A., Tualle-Brouri R., Grangier P. *New J. Phys*., **11**, 045023 (2009).
101. Winzer P.J. *Opt. Photon. News*, **26**, 28 (2015).
102. Huang M.F., Tanaka A., Ip E., Huang Y.-K., Qian D., Zhang Y., Zhang S., Ji P.N., Djordjevic I.B., Wang T., Aono Y., Murakami S., Tajima T., Xia T.J., Wellbrock G.A. *J. Lightwave Technol*., **32** (4), 776 (2014).
103. Dixon A.R., Yuan Z.L., Dynes J.F., Sharpe A.W., Shields A.J. *Opt. Express*, **16**, 18790 (2008).
104. Gottesman D., Lo H.-K., Lütkenhaus N., Preskill J. *Quantum Inf. Comp*., **4** (5), 325 (2004).
105. Yuan Z.L., Dixon A.R., Dynes J.F., Sharpe A.W., Shields A. *New J. Phys*., **11**, 045019 (2009).
106. Korzh B., Lim C.-C.W., Houlmann R., Gisin N., Li M.J., Nolan D., Sanguinetti B., Thew R., Zbinden H. *Nat. Photon*., **9**, 163 (2015); https://arxiv.org/pdf/1407.7427.pdf.
107. Fröhlich B., Dynes J.F., Lucamarini M., Sharpe A.W., Yuan Z., Shields A.J. *Nature*, **501** (6), 9 (2013).
108. Fröhlich B., Dynes J.F., Lucamarini M., Sharpe A.W., Tam S.W.-B., Yuan Z., Shields A.J. *Sci. Rep*., **5**, 18121 (2015).
109. Peters N.A., Toliver P., Chapuran T.E., Runser R.J., McNown S.R., Peterson C.G., Rosenberg D., Dallmann N., Hughes R.J., McCabe K., Nordholt J.E., Tyagi K.T. *New J. Phys*., **11**, 045012 (2009).
110. Choi I., Young R., Townsend P.D. *New J. Phys*., **13**, 063039 (2011).
111. Yuan Z.L., Kardynal B.E., Sharpe A.W., Shields A.J. *Appl. Phys. Lett*., **91** (4), 041114 (2007).
112. *Optika i komponenty setei PON. GPON tekhnologiya* (Optics and Components of PON Networks. GPON Technology). Web-site: xdw.ru, Section. 28 (2018); http://www.xdw.ru/rubrics/28/.
113. Cebrowski A.K., Garstka J.J. *U.S. Naval Institute Proc. Magazine*., **124/1/1**/, 139 (1998); https://www.usni.org/magazines/proceedings/1998-01.
114. Zatuliveter Yu.S., in *Proc. Conf. 'Technical and Software Tools for Control, Monitoring and Measurement Systems'* (Moscow: IPU, 2010) 000492.
115. Nauerth S., Moll F., Rau M., Fuchs C., Horwath J., Frick S., Weinfurter H. *Nat. Photon*., **7**, 382 (2013); DOI: 10.1038/nphoton.2013.46.
116. Heritage J.P., Weiner A.M. *IEEE J. Sel. Top. Quantum Electron*., **13** (5), 1351 (2007).
117. Prucnal P.R. (Ed.) *Optical Code Division Multiple Access: Fundamentals and Applications* (New York: Taylor&Francis, 2006).
118. Argyris A., Syvridis D., Larger L., Annovazzi-Lodi V., Colet P., Fischer I., García-Ojalvo J., Mirasso C.R., Pesquera L., Shore K.A. *Nature*, **438** (17), 343 (2006).
119. Zadok A., Scheuer J., Sendowski J., Yariv A. *Opt. Express*, **16**, 16680 (2008).
120. Fung C.-H.F., Tamaki K., Qi B., Lo H.-K., Ma X. *Quantum Inf. Comput*., **9**, 131 (2009).
121. Hirota E.O. *Tamagawa Univ. Quantum ICT Res. Inst. Bull*., **5** (1), 5 (2015); http://www.tamagawa.jp/en/research/quantum/bulletin/2015.html.
122. Hirota E.O. *Tamagawa Univ. Quantum ICT Res. Inst. Bull*., **5** (1), 37 (2015); https://arxiv.org/abs/1511.04671v1.
123. Hirota O., Kato K., Sohma M., Usuda T., Harasawa K. *Proc. SPIE*, **5551**, 206 (2004).
124. Hirota O., Kato K., Sohma M., Fuse M. *Proc. SPIE*, **5833**, 186 (2005); DOI: https://doi.org/10.1117/12.620487.
125. Hirota O. *Phys. Rev. A*, **76**, 032307 (2007).
126. Kato K., Hirota O. *Proc. SPIE*, **8163**, 81630A (2011).
127. Futami F., Hirota O. *Tamagawa Univ. Quantum ICT Res. Inst. Bull*., **4** (1), 15 (2014); https://pdfs.semanticscholar.org/677b/d1c3c7e3fdd4b647cb77a80d5dd0168501cf.pdf.
128. Ohhata K., Hirota O., Honda M., Akutsu S., Doi Y., Harasawa K., Yamashita K. *J. Lightwave Technol*., **28** (18), 2714 (2010).
129. Nishioka T., Hasegawa T., Ishizuka H., Imafuku K., Imai H. *Phys. Lett. A*, **327** (1), 28 (2004); DOI: https://doi.org/10.1016/j.physleta.2004.04.083; https://arxiv.org/abs/quant-ph/0310168v2.
130. Nishioka T., Hasegawa T., Ishizuka H., Imafuku K., Imai H. *Phys. Lett. A*, **346** (1-3), 7 (2005).

131. Lo H.K., Ko T.M. *Quantum Inform. Comput.*, **5** (1), 041 (2005); https://arxiv.org/pdf/quant-ph/0309127v3.pdf.
132. Donnet S., Thangaraj A., Bloch M., Donnet S., Thangaraj A., Bloch M., Cussey J., Merolla J.-M., Larger L. *Phys. Lett. A*, **356** (6), 406 (2006); https://www.sciencedirect.com/journal/physics-letters-a/vol/356.
133. Ahn C., Birnbaum K. *Phys. Lett. A*, **370** (2), 131 (2007); https://arxiv.org/abs/quant-ph/0612058v2.
134. Ahn C., Birnbaum K. *Phys. Lett. A*, **372** (47), 7097 (2008).
135. Yuen H.P., Kumar P., Corndorf E, Nair R. *Preprint* at arXiv:quant-ph/ 0407067v2 (2004); https://arxiv.org/pdf/quant-ph/0407067v2.pdf.
136. Yuen H.P., Kumar P., Corndorf E., Nair R. *Phys. Lett. A*, **346** (1-3), 1 (2005); https://arxiv.org/pdf/quant-ph/0312029.pdf.
137. Yuen H.P, Kumar P., Corndorf E., Nair R. *Phys. Lett. A*, **349** (6), 516 (2005); https://www.sciencedirect.com/journal/physics-letters-a/vol/349/issue/6.
138. Hirota O., Kato K., Sohma M., Fuse M. DOI: 10.1117/12.620487; https://arxiv.org/abs/quant-ph/0410006v1.
139. Hirota O., Kato K., Sohma M., Usuda T.S., Harasawa K. *Proc. SPIE*, **5551**, 206 (2004); DOI: 10.1117/12.561778; https://arxiv.org/abs/quant-ph/0407062v1.
140. Yuen H.P., Nair R., Corndorf E., Kanter G.S., Kumar P. *Quantum Inform. Comput*., **6** (7), 561 (2006); https://arxiv.org/pdf/quant-ph/0509091.pdf.
141. Huang J.-F., Meng S.-H., Lin Y.-C., Chen K.-S., Huang A-C. *Proc. Comp. Sci*., **34**, 39 (2014).
142. Kitayama K., Wada N., Sotobayashi H. *J. Lightwave Technol*., **18** (12), 1834 (2000).
143. Menendez R., Agarwal A., Toliver P., Jackel J., Etemad S. *J. Opt. Netw*., **6** (5), 442 (2007).
144. Kodama T., Nakagawa N., Kataoka N., Wada N., Cincotti G., Wang X., Miyazaki T., Kitayama K.-I. *J. Lightwave Technol*., **28** (1), 181 (2010); DOI: 10.1109/JLT.2009.2033357; https://www.researchgate.net/publication/243479663_Secure_25_Gbits_16-ary_OCDM_block-ciphering_with_XOR_using_a_single_multi-port_endecoder.
145. Biham E., Mor T. *Phys. Rev. Lett*., **78**, 2256 (1997).
146. Katz N., Neeley M. *Phys. Rev. Lett*., **101**, 200401 (2008).
147. Vakhitov A., Makarov V., Hjelme D. *J. Mod. Opt*., **48** (13), 2023 (2001).
148. Bugge A.N., Sauge S., Mardhiyah A., Ghazali M., Skaar J., Lydersen L., Makarov V. *Phys. Rev. Lett*., **112**, 070503 (2014).
149. Kurtsiefer C., Zarda P., Halder M., Weinfurter H., Gorman P.M., Tapster P.R., Rarity J.G. *Nature*, **419**, 450 (2002).
150. Lo H.-K., Preskill J. *Quantum Inf. Comput*., **7**, 431 (2007).
151. Gisin N., Fasel S., Kraus B., Zbinden H., Ribordy G. *Phys. Rev. A*, **73**, 022320 (2006).
152. Lydersen L., Wiechers C., Wittmann C., Elser D., Skaar J., Makarov V. *Nature Photon*., **4**, 686 (2010).
153. Gerhardt I., Liu Q., Lamas-Linares A., Skaar J., Makarov V. *Nature Commun*., **2**, 349 (2011).
154. Kurtsiefer C., Zarda P., Mayer S., Weinfurter H. *J. Mod. Opt*., **48**, 2039 (2001); DOI:10.1080/09500340108240905; https://arxiv.org/abs/quant-ph/0104103v1.
155. Makarov V., Hjelme D.R. *J. Mod. Opt*., **52**, 691 (2005).
156. Lamas-Linares A., Kurtsiefer C. *Opt. Express*, **15**, 9388 (2007).
157. Makarov V., Anisimov A., Skaar J. *Phys. Rev. A*, **74**, 022313 (2006).
158. Wiechers C., Lydersen L., Whittmann C., Elser D., Skaar J., Marquardt C., Makarov V., Leuchs G. *New J. Phys*., **13**, 013043 (2011).
159. Sajeed S., Minshull C., Jain N., Makarov V. *Sci. Reports*, **7**, 8403 (2017); https://www.nature.com/articles/s41598-017-08279-1.pdf.
160. Molotkov S.N. *Pis'ma Zh. Eksp. Teor. Fiz.*, **97** (10), 693 (2013).
161. Stucki D., Brunner N., Gisin N., Scarani V., Zbinden H. *Appl. Phys. Lett*., **87**, 194108 (2005).
162. Gleim A.V., Egorov V.I., Nazarov Yu.V., Smirnov S.V., Chistyakov V.V., Bannik O.I., Anisimov A.A., Kynev S.M., Ivanova A.E., Collins R.J., Kozlov S.A., Buller G.S. *Opt. Express*, **24** (3), 002619 (2016).
163. Klimov A.N., Kulik S.P., Molotkov S.N., Potapova T.A. *Laser Phys. Lett*., **14**, 035201 (2017).
164. www.idquantique.com.
165. Buzov G.A., Kalinin S.V., Kondratiev V.A. *Zashchita ot utechki informatsii po tekhnicheskim kanalam* (Protection from Information Leakage through Technical Channels) (Moscow: Goryachaya liniya-Telecom, 2005).
166. Rudometov E.A., Rudometov V.E. *Shpionskie strasti. Elektronnye ustroistva dvoinogo primeneniya* (Spy Passions. Electronic Devices of Dual Use) (Moscow: AST, Polygon, 2000).
167. *Bezopasnost' informatsionnykh system 2017* (Security of Information Systems 2017). A Survey of TAdviser, RF; http://www.tadviser.ru/index.php/ Article: Overview: _Security_ information_systems.
168. Chernyshev M. *Information Security*, **4**, 44 (2012); http://www.itsec.ru/articles2/bypub/insec-4-2012.
169. Lemos R. https://www.technologyreview.com/s/428557/the-latest-threat-a-virus-made-just-for-you/.
170. http://www.itsec.ru/newstext.php?news_id=86277.
171. Bakhur V. http://safe.cnews.ru/news/line/2017-06-29_novaya_globalnaya_ ataka_shifrovalshchika_podrobnosti.
172. https://www.infowatch.ru/analytics/reports/24616.
173. https://www.infowatch.ru/report2017.
174. https://www.securitylab.ru/news/486600.php; https://www.infowatch.ru/analytics/reports/17962.
175. https://www.devicelock.com/ru/company/press_releases.html.
176. https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/.
177. https://cloudblogs.microsoft.com/microsoftsecure/2017/06/27/whats-new-in-windows-defender-atp-fall-creators-update/?source=mmpc.
178. https://www.cnet.com/news/microsoft-build-smart-antivirus-using-400-million-computers-artificial-intelligence/.
179. Shi Y., Chng B., Kurtsiefer C. *Appl. Phys. Lett*., **109**, 041101 (2016).
180. Jennewein T., Achleitner U., Weihs G., Weinfurter H., Zeiliner A. *Rev. Sci. Instrum*., **71**, 1675 (2000).
181. Nie Y.-Q., Huang L., Liu Y., Payne F., Zhang J., Pan J.-W. *Rev. Sci. Instrum*., **86**, 063105 (2015).
182. Wayne M.A., Kwiat P.G. *Opt. Express*, **18**, 9351 (2010).
183. Symul T., Assad S.M., Lam P.K. *Appl. Phys. Lett*., **98**, 231103 (2011).
184. Xu F., Qi B., Ma X., Xu X., Zheng H., Lo H.-K. *Opt. Express*, **20** (11), 12366 (2012).
185. Kravtsov K.S., Radchenko I.V., Kulik S.P., Molotkov S.N. *J. Opt. Soc. Am. B*, **32** (8), 1743 (2015); DOI: https://doi.org/10.1364/JOSAB.32.001743; https://www.osapublishing.org/josab/abstract.cfm?uri=josab-32-8-1743.
186. Rine D.C. (Ed.) *Computer Science and Multiple-Valued Logic: Theory and Applications* (Amsterdam, North Holland, 1984) Ch.7-9.
187. Shimbirev P.N. *Gibridnye nepreryvno-logicheskie ustroistva* (Hybrid Continuous-Logic Devices) (Moscow: Energoatomizdat, 1990).
188. Conway J.H., Guy R. *The Book of Numbers* (New York: Springer-Verlag, 1996).
189. Ifrah G. *The Universal History of Numbers. From Prehistory to the Invention of the Computer* (New York: John Wiley&Sons, 1999) Vol. I.
190. Chizhov I.V. *Vestn. Moskovskogo Univer*., **3**, 40 (2009).
191. Antipov A.L., Bykovsky A.Yu., Egorov A.A. *J. Rus. Laser Research,* **29** (4), 322 (2008).
192. Bykovsky A.Yu. *Kr. Soobshch. Fiz. FIAN*, **11**, 9 (2013).
193. Antipov A.L., Bykovsky A.Yu., Egorov A.A., Kompanets I.N. *Radiotekh*., **8**, 97 (2008).
194. Bykovsky A.Yu., Rager B.Yu. *Proc. 12th All-Russian Meeting on the Management Problems of VSPU-2014* (Moscow: IPU, 2014) p. 3917.
195. Bykovsky A.Yu., Sherbakov A.A. *J. Phys. Conf. Ser*., **737** (1), 12059 (2016).
196. Moiseev S.A., Skrebnev V.A. *Phys. Rev. A*, **91**, 022329 (2015); DOI: https://doi.org/10.1103/PhysRevA.91.022329; https://journals.aps.org/pra/abstract/10.1103/hysRevA.91.022329.
197. Brassard G. *Modern Cryptology: A Tutorial, Lecture Notes in Computer Science* (New York: Springer, 1988) Vol. 325.
198. Bouwmeester D., Eckert A., Zeilinger A. *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation* (Berlin: Springer, 2000; Moscow: Postmarket, 2002).

199. Holevo A.S. *Vvedenie v kvantovuyu informatsiyu* (An Introduction to Quantum Information Theory) (Moscow: MTsNMO, 2002).
200. Nielsen M., Chuang I. *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press, 2000; Moscow: Mir, 2006).
201. Kilin S., Khoroshko D.B., Nizovtsev A.P. *Kvantovaya kriptografiya: idei i praktika* (Quantum Cryptography: Ideas and Practices) (Minsk, Belorussian Science, 2007).
202. Samartsev V.V. *Korrelirovannye fotony i ikh primeneniya* (Correlated Photons and Their Applications) (Moscow: Fizmatlit, 2014).
203. Khrennikov A.Yu. *Vvedeniye v kvantovuyu teoriyu informatsii* (Introduction to the Quantum Information Theory) (Moscow: Fizmatlit, 2017).
204. Al'bov A.S. *Kvantovaya Kriptografiya* (Quantum Cryptography) (St.-Petersburg: Stratab, 2016).
205. Gisin N. *Quantum Chance: Nonlocality, Teleportation and Other Quantum Marvels* (New York: Springer, 2012; Moscow: Alpina-nonfikshn, 2016).
206. Ivanov M.G. *Kak ponimat' kvantovuyu mekhaniku* (How to Understand Quantum Mechanics) (Moscow–Izhevsk: NITs 'Regular and chaotic dynamics', 2012).