Dmytro HONCHAR[1]

Scientific supervisor: Yevhen VASILIU[2]

DOI: https://doi.org/10.53052/9788366249868.05

PRZEGLĄD AKTUALNEGO STANU TECHNOLOGII KWANTOWEGO BEZPIECZEŃSTWA INFORMACJI

Streszczenie: W artykule rozważane są podstawowe zasady fizyczne leżące u podstaw technologii kwantowych bezpieczeństwa informacji, aktualny stan ich rozwoju i perspektywy implementacji nowych kwantowych krypto-prymitywów, a także zastosowania technologii kwantowej dystrybucji klucza w pasywnych sieciach optycznych.

Słowa kluczowe: kryptografia kwantowa, dystrybucja klucza kwantowego, BB84, SARG04, wabikowa dystrybucja klucza kwantowego, bezpieczna bezpośrednia komunikacja kwantowa

OVERVIEW OF THE CURRENT STATE OF QUANTUM INFORMATION SECURITY TECHNOLOGIES

Summary: In this paper are considered the basic physical principles underlying quantum technologies of information security, the current state of their development and prospects for the implementation of new quantum crypto-primitives, as well as application of quantum key distribution technology in passive optical networks.

Keywords: quantum cryptography, quantum key distribution, BB84, SARG04, decoy quantum key distribution, quantum secure direct communication

1. Introduction

Today, the issue of information security is especially relevant in view of the almost complete transition to digital technologies and the creation of the Internet of Things. The main encryption methods currently used are based on one very vulnerable assumption - all the security (secrecy) of these methods is based on the complexity of

[1] State University of Intelligent Technologies and Telecommunications · Information Technologies and Cybersecurity: dmytro.honchar972@gmail.com

[2] profesor State University of Intelligent Technologies and Telecommunications · Information Technologies and Cybersecurity: email

the computational algorithms used to decrypt the message, or in other words, the limited computing power of the attacker. This applies to both symmetric encryption and asymmetric encryption. The fundamental task in terms of encryption is the need to distribute keys. This is the main difference between encryption methods. The main principle in symmetric encryption systems is the condition that the transmitter and receiver know in advance the encryption algorithm, as well as the key to the message, without which the information is just a set of characters that do not make sense. This raises the issue of allocating encryption keys. There are two possible options for this: to encrypt the keys themselves, or to transmit the keys with the help of messengers (and hope that no one will intercept them on the way). Both key distribution options cannot be considered to fully meet future confidentiality requirements, but are widely used in engineering. In the case of a universal quantum computer, it is potentially possible to hack all modern cryptosystems.

The idea of open-key cryptography (asymmetric encryption) is closely related to the idea of one-sided functions, that is, such functions $f\ (x)$ that the known x is quite simple to find the value of $f\ (x)$, while the definition of x from $f\ (x)$ is impossible for a reasonable term. But the one-way function itself is useless: it can be used to encrypt a message, but it cannot be decrypted. Therefore, public key cryptography uses one-way functions with a loophole. A loophole is a secret that helps decipher a message. That is, there exists a y such that knowing $f\ (x)$ and y, we can compute f. For example, to disassemble any device is quite simple, but to assemble it back is a much more time-consuming task, but it can be facilitated by the instructions. It is worth noting that it is still possible to assemble this device quickly enough. This variant is the emergence of a quantum computer that is able to quickly find x, knowing only $f\ (x)$. In connection with the above problems, it is necessary to move to a completely new paradigm of key distribution, which will not be so vulnerable to an increase in the computing power of an attacker, but will be based on the fundamental laws of physics. Quantum Key Distribution (QKD) systems ensure no eavesdropping in the channel and are used to generate random binary sequences known only to the sender and receiver [1-13]. These sequences can be used to obtain symmetric keys that cannot be compare even on a quantum computer. Thus, in contrast to classical methods of data protection, the stability of quantum communication systems does not depend on the time and computing power of the intruder. Quantum communication can be carried out on any optical channel: fiber or open space.

Currently, the transition to technologies based on the use of quantum effects is one of the main trends in modern communications and high performance computing. All over the world, great resources are being invested in the development of quantum methods of information transmission. This interest is due to the fact that even a partial transition to quantum technologies will make it possible to achieve fundamentally new qualities that are inaccessible when using classical approaches. Achievement of qualitatively new opportunities using the technology of quantum transmission and information processing is based on the laws of quantum physics that underlie them. Examples include “instantaneous” transmission of a quantum state at a distance based on the entanglement principle (quantum teleportation), acceleration of quantum computations due to their non-classical parallelism, and ensuring data confidentiality in quantum key distribution systems based on the indivisibility of quantum objects and the impossibility of their cloning. Devices for quantum transmission and processing of information use quantum units of information - qubits, which, unlike the classical analogue (bit), can be in a superposition of two states, i.e. when measured, are found in any of these states. The material embodiment of a qubit can be any microscopic physical system with two states.

The general principle of operation of quantum cryptography protocols can be described as follows: the transmitting side (Alice) at each step sends one of the states from their non-orthogonal set, the receiving side (Bob) makes such a measurement that after additional exchange of classical information between them, they must have bit lines that completely coincide in the case of an ideal channel and no interceptor. Errors in these lines can indicate both the imperfection of the channel and the actions of the eavesdropper. If the error exceeds a certain limit, the protocol is interrupted, otherwise legitimate users can extract the fully secret key from their (overlapping) bit strings. Based on the measurement postulate of quantum mechanics, it is impossible to measure an unknown quantum state without introducing a perturbation, unless that state is the eigenstate of the observable being measured. This means that Eve cannot perform a measurement of an unknown quantum state without introducing a disturbance that can be detected by Alice and Bob.

The uncertainty principle states that measuring one quantum observable, in fact, creates uncertainty in other properties of the system. This means that it is impossible to measure the simultaneous values of non-commutated observables on a single copy of a quantum state. This ensures that the interceptor cannot perform measurements that do not violate the quantum state. This automatic eavesdropping is not possible in classical cryptography. In quantum mechanics, it is impossible to make a perfect copy of an unknown state with perfect precision. This is called the no-cloning theorem. This prevents an attacker from simply intercepting the communication channel and making copies (in order to subsequently measure) the transferred quantum states, while transferring the unperturbed quantum state to Bob. Thus, the cloning prohibition theorem forms an important security property of QKD protocols.

In addition to quantum key distribution, quantum cryptography includes a number of other crypto-primitives, including quantum secret sharing, quantum digital signature, quantum secure direct communication, quantum bit commitment, quantum steganography, etc., which have not yet reached the level of industrial use [14-19].

The aim of the paper is a brief overview of the current state of achievements in the field of quantum methods of information protection, as well as prospects for their development and implementation.

2. Quantum key distribution schemes

There are two main types of QKD schemes, namely preparation and measurement (PM) schemes and entanglement-based (EB) schemes. The PM scheme is based on individual qubits, and the EB scheme is based on entangled qubits. Any of these schemes can be used by two parties to obtain a shared secret. However, the PM circuit can be immediately converted into an EB circuit. In prepare and measure scheme Alice encodes some common information into a set of quantum states and sends them to Bob through an insecure quantum channel. Bob then takes measurements of the resulting quantum states. This leads to the fact that the usual data generated by quantum tools are shared by Alice and Bob. Examples of protocols using this scheme are BB84, B92, Six states, and SARG04. In an entanglement-based scheme, the source prepares and distributes the most entangled quantum state, where one system is sent to Alice and the other to Bob. Then Alice and Bob take measurements in two mutually unbiased bases in their system, respectively. Once measured, they get perfectly matched results that are completely random. Since the source prepares a pure state, this means that this state cannot be reconciled by an attacker. This implies the secrecy of the key. An example of a protocol using this scheme is the E91 protocol [8].

2.1. BB84 protocol

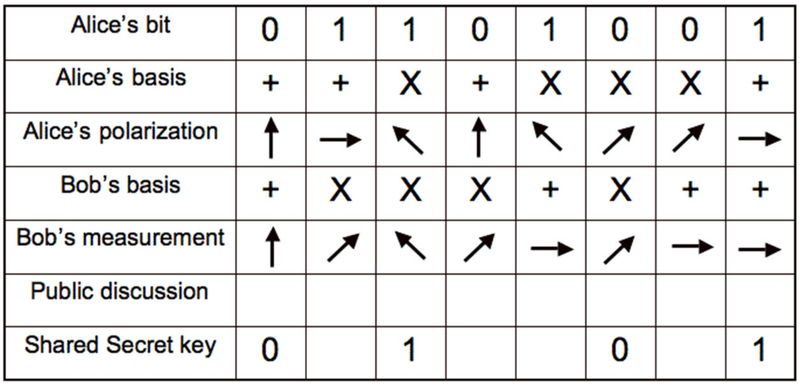
Suppose we have quantum states $|0\rangle$ that are not orthogonal, then we can prove that there is no quantum measurement that could distinguish between the states. In this case, the nonzero component of the state $|1\rangle$, parallel to the state $|0\rangle$ always gives a nonzero probability of the measurement result associated with the state $|1\rangle$, which also occurs when a measurement is applied to a state $|0\rangle$. This is because $|0\rangle$ can be decomposed into a nonzero component parallel to $|1\rangle$, And a component orthogonal to $|1\rangle$. Then there is no measurement that can reliably determine which of the two non-orthogonal quantum states has been measured. This feature is very useful for cryptographic applications like QKD. Alice and Bob are connected by two communication channels, namely an insecure quantum channel and an authenticated classical channel. The quantum channel is used to transmit qubits and is controlled by an interceptor. The classic channel is authenticated so that the interceptor can only listen to the message, but cannot modify the transmitted messages. This ensures that Alice and Bob can prove that they are communicating with each other. Otherwise, the interceptor could simply block all quantum and classical communication between Alice and Bob and perform QKD with Alice, taking on the role of Bob, and vice versa. Therefore, Alice and Bob must identify each message they send as originating from themselves before post-processing can begin.

In the quantum phase, Alice and Bob are using the quantum channel. They use quantum mechanical signals (i.e., qubits) and also take measurements. There are three sub-protocols, namely:

- Signal preparation: Alice prepares a random sequence of strings, which are extracted from a set of four signal states, and encodes each bit value into a state of the quantum system. Basic states are horizontal, vertical, diagonal, and antidiagonal.
- Send: The encoded quantum system is sent to Bob via the quantum channel.
- Measurement: Bob applies a quantum measurement to the quantum system to decode the bit value. The signals are measured in a random sequence of polarization bases, either in horizontal / vertical or diagonal / antidiagonal bases. Alice then keeps track of the choice of signals; Bob writes down his main choices and their corresponding measurements.

In the next step, Alice and Bob use some classic communication protocol to extract the secret key from their negotiated data. They do this by negotiating through an authenticated classic channel. The key retrieval procedure is described as follows:

- Parameter estimation: Alice randomly selects some part of her beacon intervals and tells Bob what signal she sent for these intervals. Bob transmits the measurement performed and the result he received. Depending on the number of errors they get when comparing, they can also decide whether to continue or abort the protocol execution.
- Sifting: In the sifting protocol, Alice and Bob transmit the polarization bases they used to prepare the signals and which bits are discarded. To prevent Eve from changing the transmitted messages, Alice and Bob use an authentication scheme. The rest of the data is called sifted data. Alice and Bob proceed to the negotiation or error correction phase.
- Key converting: Alice and Bob discard the base they used so that Eve cannot learn any encoding information. During key conversion, Alice and Bob convert their sifted data value records to a new key. This step is used to prepare and measure the protocol.
- Error correction: The sifted data may still contain some errors; therefore, Alice and Bob follow the classic error correction protocol to reconcile their data. They need to exchange additional information about their data over a public channel. In addition, they need to authenticate at this stage, as Eve can still modify messages at this stage. As a result of this protocol, Alice and Bob now agree on a key that is identical with a very high probability, but Eve may still have a little additional information about the key. After this stage, confidentiality is enhanced.
- Privacy amplification: After Alice and Bob agree on their key, they can shorten the relationship between their key and Eve using what is called confidentiality hardening. At this point, Alice and Bob transform their string, through a special family of functions called universal hash functions, to a shorter final key.



Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Figure 1. Principle of the BB84 protocol [12]

In practice many implementations use laser pulses attenuated to a very low level to send the quantum states. These laser pulses contain a very small number of photons, for example 0.2 photons per pulse, which are distributed according to a Poisson distribution. This means most pulses actually contain no photons (no pulse is sent), some pulses contain 1 photon (which is desired) and a few pulses contain 2 or more photons. If the pulse contains more than one photon, then Eve can split off the extra photons and transmit the remaining single photon to Bob. This is the basis of the photon number splitting attack, where Eve stores these extra photons in a quantum memory until Bob detects the remaining single photon and Alice reveals the encoding basis. Eve can then measure her photons in the correct basis and obtain information on the key without introducing detectable errors. Even with the possibility of a PNS attack a secure key can still be generated, as shown in the GLLP security proof; however, a much higher amount of privacy amplification is needed reducing the secure key rate significantly. There are several solutions to this problem. The most obvious is to use a true single photon source instead of an attenuated laser. While such sources are still in development QKD is successfully used in practice. However, as current sources operate at a low efficiency and frequency key rates and transmission distances are limited. Another solution is to modify the BB84 protocol, as is done for example in the SARG04 protocol, in which the secure key rate scales as $t^{3/2}$. The most promising solution is the decoy states in which Alice randomly sends some of her laser pulses with a lower average photon number. These decoy states can be used to detect a PNS attack, as Eve has no way to tell which pulses are signal and which decoy. Using this idea the secure key rate scales as t, the same as for a single photon source.

2.2 SARG04 protocol

In fact, the quantum phase of SARG04 is the same as that of BB84 [8,13].
The steps for the SARG04 protocol with a ν-photon source (ν = 1, 2) and one-way communications are as follows:

- Alice sends a sequence of N signals to Bob. For each signal, Alice randomly chooses one of the four sets and sends one of the two states in the set to Bob.
- For each signal, Bob performs the polarization measurement using one of the two bases randomly. If his detector fails to click, then he broadcasts this fact, and Alice and Bob discard all the corresponding data.
- For each signal, Alice publicly announces the choice of the set from which the state was selected.
- For each signal, Bob compares his measurement outcome to the two states in the set. If his measurement outcome is orthogonal to one of the states in the set, then he concludes that the other state has been sent, which is a conclusive result. On the other hand, if his measurement outcome is not orthogonal to either of the states in the set, he concludes that it is an inconclusive result. He broadcasts if he got the conclusive result or not for each signal.
- Alice randomly chooses some bits as test bits and announces their locations. Bob estimates the bit error rate e_ν from the test bits by taking the ratio of the number of incorrect conclusive test bits to the total number of conclusive test bits. If e_ν is too high, they abort the protocol.
- Alice and Bob retain only the conclusive untested bits.
- They perform bit error correction and privacy amplification on the remaining bit string.

2.3 Decoy quantum key distribution

One of the most promissory alternatives of SARG04 is the decoy QKD [8]. In this protocol Alice prepares a set of quantum states in addition to the typical states of the BB84 protocol. These extra states are called decoy states. Decoy states are used only with the purpose to detect the eavesdropping activity, rather than establishing the key. In order to produce the decoy states, Alice randomly uses different mean photon numbers on the photonic source. For example, she could send the first pulse with a mean photonic pulse of μ=0.1, the second pulse with μ=0.4, the third pulse with μ=0.05, and so on. To each mean photon number a different probability of producing more than one photon in the correlated pulse corresponds. The difference between the standards BB84 states and the decoy states is the mean photon numbers. Given this, Eve is not able to distinguish a decoy state from a quantum key related state and the only information she gets is the number of photons in a pulse. Thus, decoy states can be introduced to secure the BB84 protocol from PNS attacks, allowing at the same time high key rates. In both, BB84 and decoy QKD protocols, a single photonic gain in the quantum channel is established. Lamentably, Eve can set successful attacks to the decoy QKD if it is able to set the QBER to zero by adjusting the gain of the quantum channel.

3. Quantum secure direct communication

One of the possible solutions to extend quantum cryptography beyond the key distribution problem was found in the late 90's - early 2000's, when the so-called quantum secure direct communication protocols were proposed, in particular, a simpler version of the ping-pong protocol [14]. These protocols transmit sensitive data without performing any encryption procedure. Secrecy in data transmission is provided by the same advantage of quantum cryptography: the ability to detect in real time the fact of listening to the communication channel. Even if an attacker manages to intercept a certain amount of information in a short period of time, the damage to legitimate users of the communication channel can be minimized to the required level through additional data processing procedures. Because channel users can determine the maximum amount of information that reaches the attacker, when eavesdropping is detected, the situation is completely under control. Technically, such a solution is implemented, as a rule, by periodic switching between the modes of information transmission and interception control in the quantum communication channel. The frequency of such switching is determined by the required level of security. Also, to date, developed additional, including non-quantum methods to increase the security of quantum direct secure communication protocols [4].

4. Quantum secret sharing and quantum bit commitment

Further development of quantum cryptography followed the path of improving the above protocols, as well as the creation of a number of other quantum cryptographic primitives. Thus, in particular, a large number of works refer to the problem of quantum secret sharing, first solved in the HBB99 protocol [15]. This task is of great practical importance, for example, in banking: general mutually controlled access to the storage, the presence of more than one electronic digital signature in interbank payment procedures and payments at the client-bank level using telecommunication systems, etc. To date, a significant number of quantum secret sharing schemes have been proposed that differ from each other: some are based on quantum entanglement, others on the use of squeezed light to realize quantum phenomena with continuous states, etc. [16-19]. A significant number of secret sharing protocols have been successfully implemented today in the laboratories of renowned universities and research centers.

Unlike the classical (non-quantum) schemes of secret sharing, the quantum protocols allow to uncover eavesdropping of communication channels between the remote participants of the procedure. In addition, quantum secret sharing protocols are protected from dishonest actions of the legal participants.

Quite a long history has a solution to the problem of a quantum bit commitment – transferring to a partner closed information, which, according to the conditions, cannot be disclosed prematurely, but the sender, in turn, has no right to refuse its content and authorship. This protocol took the form of an acceptable solution only two decades after the problem was formulated within the framework of quantum cryptography [19]. The problem of bit commitment, which easily found its solution in classical cryptography, for a long time ran into insurmountable difficulties when trying to implement this kind of scheme in the framework of quantum cryptosystems. Ultimately, the researchers managed to create both a theoretical scheme of such a quantum cryptographic primitive and its experimental embodiment, using additionally the property of the finiteness of the speed of light. The practical use of bit commitment in general and quantum in particular is due to the requirements for electronic voting systems, electronic auctions, and some other applications.

5. Discusion and conclusion

Taking into account the fact that, in addition to the one-time pad cipher, in classical cryptography there are no ciphers suitable for practical use that have unconditional security, and research on the creation of quantum computers is being carried out quite intensively, quantum cryptography is a rather promising field of cryptology. Today, devices for quantum key distribution are used in areas where a high level of security is required. Work is underway to create networks of trusted servers for quantum key distribution.

Despite the unconditional strength of the theory of quantum key distribution, it has a number of disadvantages. One of the key issues is the range and data rate of quantum communications. The fact is that the transmitted data is encoded in the states of single photons; at this stage, quantum communication lines are very vulnerable to interference and noise, therefore, in practice, in backbone networks, the quantum key is transmitted over distances of up to 100 km. At larger distances, the key generation rate becomes too low, in fact, the achieved key distribution rate in a fiber-optic communication line (FOCL) with a length of up to 50 km is ~ 1 Mbit/s, a FOCL length of more than 80-100 km leads reducing the QKD speed to a level of ~ 1 kbit/s, which limits practical applications. The high requirements of QKD schemes to the level of optical losses sharply limit the number of welded and detachable optical fiber connections. The presence of the above unsolved problems and the high cost of equipment is the reason for the development of combined network schemes that combine sophisticated computer processing methods with QKD schemes. Such network schemes demonstrate the forced convergence of quantum optics and computer methods to solve increasingly complex information security problems. Of course, the quantum direction of cryptographic information protection is very promising, since quantum laws make it possible to bring information protection methods to a qualitatively new level. To date, there is already experience in the creation and testing of a computer network protected by quantum-cryptographic methods - the only network in the world that is theoretically impossible to hack. Note that one of the longest quantum key distribution lines (more than 2000 km), containing 32 intermediate trusted servers, was built in China.

As for other areas of quantum cryptography, including quantum secure direct communication and quantum secret sharing, they have not yet reached the level of practical use due to a number of reasons, which include the low speed of information transfer by individual photons, high complexity and, accordingly, cost appropriate technical solutions, the lack of large-volume quantum memory devices required for the implementation of many protocols, etc. However, at the level of theoretical research, as well as at the level of laboratory experiments, all areas of quantum cryptography are rapidly developing, and their practical implementation in the field of information security is probably a matter of one or two next decades.

The work has been done with the supporting by The Ministry of Education and Science of Ukraine as part of the joint Ukrainian-Belarusian research project "Secret key transmission system based on quantum cryptography protocols".

LITERATURE

1. BENNETT C.H., BRASSARD G.: Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, (Bangalore, India, December 10-12, 1984). – New York, 75, pp. 175–179, 1984.
2. SHOR P., PRESKILL J.: Simple proof of security of the BB84 quantum key distribution protocol // Phys. Rev. Lett., 85, p. 441, 2000.
3. LIZAMA-PEREZ L.A., MAURICIO LOPEZ J., DE CARLOS LOPEZ E.: Quantum Flows for Secret Key Distribution // Advances Technologies in Quantum Key Distribution. – InTech, pp. 37–62, 2018.
4. KORCHENKO O., VOROBIYENKO P., LUTSKIY M., VASILIU YE., GNATYUK S.: Quantum Secure Telecommunication Systems // Telecommunications Networks – Current Status and Future Trends (Edited by JH Ortiz). – InTech, pp. 211–236, 2012.
5. LUCAMARINI M., CHOI I., WARD M.B., DYNES J.F., YUAN Z.L., SHIELDS A.J.: Practical Security Bounds Against the Trojan-Horse Attack in Quantum Key Distribution // Physical Review A, 5, 031030, 2015.

6. LYDERSEN L., WIECHERS C., WITTMANN C., ELSER D., SKAAR J., MAKAROV V.: Hacking commercial quantum cryptography systems by tailored bright illumination / // Nature Photonics, 4, pp. 686-689, 2010.
7. BARANOVSKY O., GORBADEY O., ZENEVICH A., VASILIU YE.: Quantum Method of Secure Key Distribution in Optical Fiber Communication Lines // The Second International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo'2017), IEEE Xplore Digital Library: *http://ieeexplore.ieee.org/document/8095366/*
8. PIRANDOLA S., ANDERSEN U. L., BANCHI L., et al.: Advances in Quantum Cryptography // Adv. Opt. Photon., 12, 1012-1236, 2020.
9. BEDINGTON R. ARRAZOLA J. M., LING A.: Progress in satellite quantum key distribution // Quantum Information, 3.1, p. 1-13, 2017.
10. GRAHAM-ROWE D.: *https://www.technologyreview.com/s/415073/ quantum-cryptography-for-the-masses/* 11.11.2021
11. *https://www.ncsc.gov.uk/whitepaper/quantum-key-distribution 11.11.2021*
12. AGGARWAL R., SHARMA H., GUPTA D.: Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol // International Journal of Computer Applications, 20, pp. 28-31, 2011.
13. *SCARANI V., ACIN A., RIBORDY G., GISIN N.*: Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations // Phys. Rev. Lett., 92, 057901, 2004.
14. BOSTROM K., FELBINGER T.: Deterministic secure direct communication using entanglement // Physical Review Letters, 89, 187902, 2002.
15. HILLERY M., BUZEK V., BERTHIAUME A.: Quantum Secret Sharing // Physical Review A, pp. 1829-1834, 1999.
16. DU YU-TAO, BAO WAN-SU.: Multiparty quantum secret sharing scheme based on the phase shift operations // Opt. Commun., 308, pp. 159-163, 2013.
17. BELL B.A., MARKHAM D., HERRERA-MARTÍ D.A., MARIN A., WADSWORTH W.J., RARITY J.G., TAME M.S.: Experimental demonstration of graph-state quantum secret sharing // Nature Communications, 5, p. 5480, 2014.
18. LAU H.K, WEEDBROOK C.: Quantum secret sharing with continuous-variable cluster states // Physical Review A, 88, 042313, 2013.
19. KENT A.: Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes // Physical Review Letters, 109, 130501, 2012.