FULLY OPTICAL NETWORKS FOR QUANTUM ENCRYPTION KEY TRANSMISSION SYSTEMS

Maharramov Vagif Ali
Azerbaijan Technical University, Baku, Azerbaijan
mvg476@mail.ru

Mansurov Tofig Magomed ogly
Azerbaijan Technical University, Baku, Azerbaijan
tofiq-mansurov@rambler.ru

DOI: 10.36724/2664-066X-2022-8-4-14-17

ABSTRACT

The development of experimental quantum physics in recent years has led to the fact that the abstract ideas of quantum mechanics began to find practical application for the protection of information in a rapidly developing field such as fiber-optic communication lines (FOCL). On the basis of (smart) translucent SMART mirrors, optical splitters, switches, schemes of unidirectional, counter, bidirectional and universal multiplexers and demultiplexers, and the principle of distributing quantum encryption keys between authorized users have been developed. It is shown that it is possible to improve the speed of the process of switching and multiplexing of information flows in comparison with traditional mechanical switches. The paper proposes a circuit solution for an all-optical network (All-Optical Networks - AON) with the possibility of generating and distributing quantum encryption keys between authorized users. The aim of this work is to develop a principle for constructing quantum systems for the secure distribution of encryption keys on all-optical networks between selected (4 or more) users, as well as methods for generating, transmitting and receiving these keys in real time. In this regard, there is a need to develop a switch and a multiplexer of information flows.

KEYWORDS: *Quantum entanglement, switching, multiplexing, mirror, optical splitter, commutator, multiplexer, demultiplexer, information flow.*

Information about authors:
Maharramov Vagif Ali
Azerbaijan Technical University, Professor, Doctor of Physical and Mathematical Sciences, Baku, Azerbaijan

Mansurov Tofig Magomed ogly
Azerbaijan Technical University, Professor, Doctor of Technical Sciences, Baku, Azerbaijan

INTRODUCTION

In 2022, Frenchman Alain Aspe, American John Clauser and Austrian Anton Zeilinger were announced as winners of the Nobel Prize in Physics. The wording of the Nobel Committee states that these scientists are noted "for experiments with entangled photons, which demonstrated the violation of Bell's inequalities and gave rise to quantum computer science." Scientists have described the effect of "quantum entanglement", when the particles that were part of the same system continue to "feel" each other's state changes even at a distance of several kilometers.

The history of these studies began back in the mid-1930s with an article by Albert Einstein, Boris Podolsky and Nathan Rosen, in which a paradox was formulated by which the authors tried to show the incompleteness of quantum mechanics. Attempts to comprehend this paradox, to which the laureates made an important contribution, ultimately made it possible to better understand the quantum basis of our world.

The idea of protecting information using quantum objects was first proposed by Stefan Weisner in 1970. Decades later, C. Bennett and J. Brassard, having familiarized themselves with the work of S. Weissner, proposed to transmit a secret key using quantum objects and in 1984 proposed the possibility of creating a fundamentally secure channel using quantum states [1]. A detailed analysis of theoretical and experimental works in this direction was made in [2].

The development of experimental quantum physics in recent years has led to the fact that the abstract ideas of quantum mechanics began to find practical application for the protection of information in a rapidly developing field such as fiber-optic communication lines (FOCL). Experimental research in the field of quantum cryptography and currently proposed protocols for data transmission and encryption key can only involve two authorized users. With a larger number of users, it is very difficult to ensure the integrity of the encryption keys or its confidentiality. This problem was first considered in [3] and a new approach was proposed, the essence of which is that when transmitting confidential information over FOCL, the encryption key is transmitted after authorized users make sure that there are no unauthorized connections to FOCL. At the same time, the detection of unauthorized users is carried out by controlling the parameters of optical noise with a given photon statistics, known only to authorized users.

The main task of quantum cryptography is the search for efficient algorithms and the development of schemes for the practical implementation of the transfer of confidential information using quantum objects, i.e. single photons [2, 4]. The modern data coding system in telecommunication systems (classical cryptography) is based on the use of ciphers (keys), for deciphering which it is necessary to be able to factorize (decompose into prime factors) large numbers. Since there are no fast algorithms for factorization of large numbers for modern computers (although they have already been developed for quantum computers), which makes it possible to ensure secrecy. However, it can be expected that in the near future such algorithms will be found and the entire security system may be destroyed.

Therefore, to fully protect the transmitted data, it is necessary to use absolutely random sequences of numbers as encryption keys (used only once, to transmit one message from the sender Alice to the recipient Bob), which cannot be reliably determined by the spy Eve. According to Shannon's mathematically proven statement [5], a data transmission cannot be decrypted if the message is encrypted with a one-time random key, the length of the key is equal to the length of the message, and this key is known only to authorized users.

The aim of this work is to develop a principle for constructing quantum systems for the secure distribution of encryption keys on all-optical networks between selected (4 or more) users, as well as methods for generating, transmitting and receiving these keys in real time. In this regard, there is a need to develop a switch and a multiplexer of information flows.

A NEW APPROACH TO SWITCHING AND MULTIPLEXING INFORMATION FLOWS

In the process of developing fiber-optic networks, one has to face a number of complex scientific and technical problems. One of them is the creation of high-speed splitters of information optical streams that perform the functions of both an optical switch and a multiplexer, providing the required accuracy of spatial modulation or spectral selection of the stream and thereby stabilizing the position of the optical stream in the focal surface of the receiver or transmitter of optical information [6, 7].

The main advantage of all-optical networks is their virtually unlimited bandwidth. The practical value of this property lies in the possibility of multiplying the speed of information transmission over fiber optic communication channels on a global scale. This task of research in the field of all-optical networks is a very relevant and promising task of a theoretical and practical nature.

In addition to the important task of improving the parameters and designs of backbone optical cables, the issue of creating reliable and affordable optical signal switches is no less acute, without which it is impossible to build branched optical networks [8].

Switches are one of the most important units of optical information transmission systems built on the basis of standard hierarchical structures. Without them, it is practically impossible to carry out automatic control of the movement of data flows and monitoring issues over an extensive network. A huge variety of devices used in technology that perform the function of switching optical signals is determined by the particular features of their use in a particular type of network [9].

One of such technologies proposed by us, as the principle of key distribution, based on bidirectional multiplexing of information flows, is considered in [7, 8].

As you know, the basis for building all-optical networks is the creation of fundamentally new circuit solutions for switching and multiplexing information flows. On fig. 1 shows variants of circuit solutions for switching and multiplexing information flows based on moving Smart mirrors.

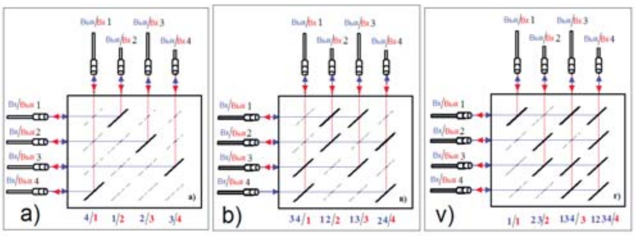

Figure 1. Options for switching and multiplexing information flows based on moving Smart mirrors

Similar switches and multiplexers can be created from a set of optical lenses in the form shown in Figure 2.

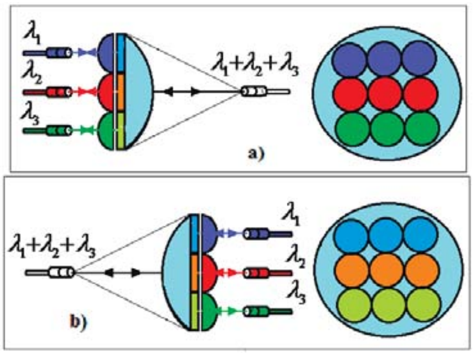

Figure 2. Technology of switching and multiplexing optical flows based on focusing lenses

All optical filters are designed as semitransparent dichroic mirrors operating at a selected wavelength [8, 9]. A dichroic mirror is an optical element that reflects radiation of only one wavelength and freely transmits other wavelengths. Such mirrors are a glass substrate with a deposited multilayer dielectric structure, which reflects only one wavelength due to the interference effect.

The principle of quantum keys distribution built on the basis of translucent mirrors

One of the problems of cryptography has always been the problem of key distribution, which is currently successfully solved using asymmetric encryption algorithms with a private key that does not leave its owner.

Currently, there are several protocols used in quantum cryptography to distribute encryption keys. Historically, the first implementation of a quantum key distribution system was a polarization coding scheme operating according to the BB84 protocol [10].

However, the strength of this and many other encryption algorithms is ensured by the current lack of computing power in the world for the possibility of successful cryptanalysis, so it is worth looking for new methods and technologies for key distribution.

One of such technologies with polarization coding was proposed in [6], where the principle of quantum key distribution was created on the basis of bidirectional multiplexing of information flows using the features of an optical splitter and a semitransparent mirror. The proposed scheme of a quantum cryptographic installation with polarization coding is shown in Figure 3.

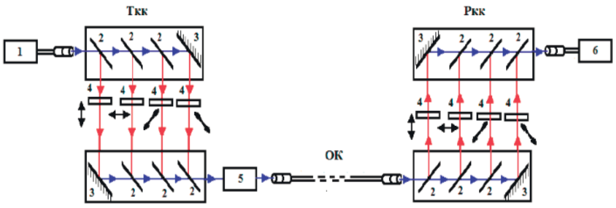

Figure 3. The proposed principle of quantum key distribution based on bidirectional multiplexing of information flows:
Tkk – quantum key transmitter or station Alice; Rkk – quantum key receiver or station Bob; OK - optical cable; 1 – semiconductor laser; 2 – translucent mirrors operating in the optical splitter (OR) mode; 3 – reflective mirrors; 4 – polarizers; 5 – absorbing filter; 6 – single-photon detector of photons from an avalanche photodiode

A semiconductor laser quantum encryption key transmitter emits short light pulses (eg, 1.0 ns duration). In principle, a semiconductor laser can operate in a continuous mode, and the formation of a short pulse (for example, 1.0 ns duration) can be formed by the OR, depending on the required polarization plane, turning the CCD into an active position. The polarization planes of photons can be -45°, 0°, +45°, and 90°. In other words, in order to transmit one bit from the required plane of polarization of a photon, it is activated according to this degree of polarization, chosen by smart translucent mirrors (SMI) in Tkk. In principle, all four types of polarization can be transmitted simultaneously. Then the pulses are attenuated by absorbing filters 5 to ensure the single-photon condition, i.e. the average number of photons per pulse is chosen to be less than one. After that, the photon is emitted in the direction of the quantum key receiver or station Bob. As is known, an important condition for the correct detection of information by station Bob is the preservation of the polarization of photons in the optical fiber.

The pulses arriving at the input of the receiver of the quantum encryption key or the Bob station pass through the CPL set and the initial polarization state is automatically determined. After that, coming from the avalanche photodiode to the input of a single-photon detector, photons are detected in the corresponding status codes. It is very important to note here that if an external intruder on the way from Alice to Bob is noticed by the transmitter or receiver of information, then they, for their part, can automatically change the direction of information transfer to the optical splitter with smart translucent mirrors, noted in [6, 7, 11, 12].

The proposed scheme of a quantum cryptographic setup with polarization coding is characterized by ease of implementation, fast detection, and high reliability. After creating SMART optical separators, multiplexing (MUX), demultiplexing (DMUX) and the principle of quantum key distribution (QKKD), we will start creating an optical network with the possibility of generating and distributing quantum encryption keys.

ALL-OPTICAL NETWORK WITH THE ABILITY TO GENERATE AND DISTRIBUTE QUANTUM ENCRYPTION KEYS BETWEEN AUTHORIZED SUBSCRIBERS

As noted in [3], the most effective ways to protect information transmitted over FOCL are quantum cryptography methods, however, according to this scheme, it is impossible to create systems for generating and distributing encryption keys for more than two authorized users. Therefore, for the first time in [9], a new approach was proposed for creating a system for generating and distributing encryption keys between several authorized users for transmitting confidential information over FOCL.

Subsequently, expanding this idea, Figure 4 proposes the principle of constructed AON networks, where the formation and distribution of quantum encryption keys between authorized subscribers is carried out [13].

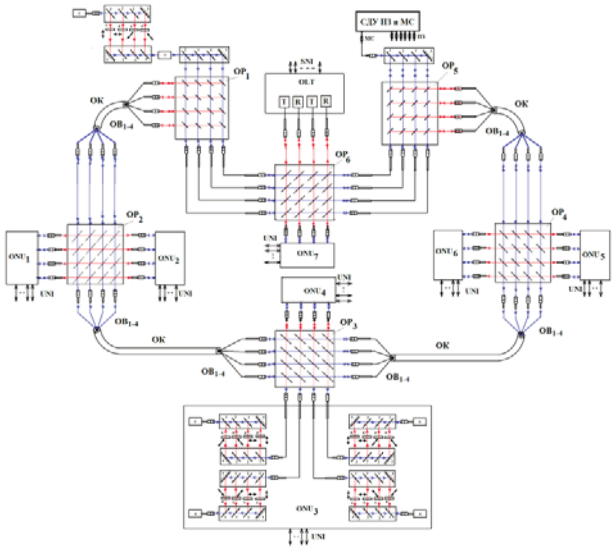

Figure 4. Scheme of an all-optical network based on optical splitters with CCD:
SNI – trunk connection interfaces; OLT – central node; ONU1-ONU7 – subscriber nodes, UNI – subscriber connection interfaces; m - main and backup transmitters; R – main and backup receivers; SDU PZ and MS – remote control system for translucent mirrors and network monitoring; OK – optical cable; OV1÷4 – optical fibers; OP1÷OP7 – optical splitters; 1 – semiconductor laser; 2 – translucent mirror; 3 – reflective mirror; 4 – polarizer (Glan prism); 5 – absorbing filter; 6 – avalanche photodiode

Here, the AON network is based on the principle of building AON networks based on OR with VMI, considered in [7].

The operation of the network is similar to the principle of operation described in Figure 3, as well as the operation of the networks described in [3, 9, 13]. On the other hand, if unauthorized users are detected, depending on the location of Eva penetration, the subscriber of this subscriber node can turn off the information receipt network or change the route using the capabilities of a universal optical splitter [6, 7].

CONCLUSION

Taking into account the proposed principle of constructing translucent and smart translucent mirrors, optical splitters, the scheme of unidirectional, counter, bidirectional and universal multiplexers (MUX) and demultiplexers (DMUX), the option of building an all-optical network based on an OR with an SPL, the principle of distributing quantum keys based on bidirectional multiplexing information flows made it possible to create an AON network with the ability to generate and distribute quantum encryption keys between authorized subscribers. On the other hand, the advantage of the network lies in the fact that, firstly, all ORs and CCDs are remotely controlled and, secondly, all optical fibers are under continuous monitoring at a wavelength that does not interfere with the normal functioning of the network built for its intended purpose.

REFERENCES

[1] Bennet C.H., Brassard G. Proc. *IEEE Intern. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore (India), 1984, pp. 175-179.

[2] Gisin N., Ribordy G., Titlel W. et al. Quantum cryptography. *Rev. Mod. Phys*. 2002. Vol. 4, pp. 145-175.

[3] A.O. Zenevich. Quantum systems for transmitting encryption keys over fiber-optic communication lines. *International conference "Innovative technologies in telecommunications"*. Baku, December 4-6, 2019, pp. 13-15.

[4] I.I. Ryabtsev, I.I. Beterov, D.B. Tretyakov et al. Experimental quantum informatics with single atoms and photons. *Bulletin of the Russian Academy of Sciences*. 2013. Vol. 83. No. 7. P. 606.

[5] Shannon, C.E. Communication Theory of Secret Systems. *Bell Syst. Tech. Jour*. 1949. Vol. 28. P. 658.

[6] V.A. Maharramov. The principle of an optical splitter. *International conference "Innovative technologies in the shopping mall"*. Baku December 4-6, 2019. P. 155-158.

[7] V.A. Maharramov. Fully optical networks based on Smart mirrors. *Problems of infocommunication*. No. 1(11), Minsk, Belarus, 2020, pp. 19-26.

[8] V.A. Maharramov, T.M. Mansurov. About one technology of switching and multiplexing of information flows. *XXVII International Conference "Modern means of communication"*. Minsk, October 27-28, 2022, pp. 184-186.

[9] V.A. Maharramov. All optical networks based on translucent mirrors. *"Machine-building and Energy: New Concepts and Technologies" International Scientific-practical Conference*, December 2-3, 2021, AzTU, Baku, Azerbaijan.

[10] V.L. Kurochkin, I.I. Ryabtsev, I.G. Neizvestnyy. Experimental setup for quantum cryptography with single polarized photons. *JTF*. 2005. Vol. 75. no. 6, pp. 54-58.

[11] I.R. Gulakov, A.O. Zenevich, T.M. Mansurov. Components of fiber-optic communication lines. Minsk, BGAS, 2020. 336 p.

[12] T.M. Mansurov, A.O. Zenevich, I.A. Mammadov. Fiber optic coupler/optical power switch. *REDS: Telecommunication devices and systems*. 2021. No.2, pp. 29-36.

[13] V.A. Maharramov, T.M. Mansurov. A new approach to building all-optical networks for a quantum encryption key transmission system. *XXVI International Conference "Modern means of communication"*. October 21-22, 2021, pp. 128-131. Minsk, Belarus.