Omega Journal of Linguistics and Language Studies
ISSN: 3072-4678
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

PROSPECTS FOR THE APPLICATION OF QUANTUM CRYPTOGRAPHY IN MODERN INFORMATION AND COMMUNICATION

Shafeyev A. N.
Institute of Information Communication Technologies and Military Signals

Abstract
This article examines quantum-based encryption algorithms from the perspective of physical phenomena. Methods of practical application of the technology and means of its implementation are presented. In addition, current problems and advantages of quantum cryptography are analyzed. A method for increasing the speed of quantum-based encryption is proposed.

Keywords: Information, security, information protection, quantum cryptography.

Introduction

Annotatsiya
Ushbu maqolada axborotni kvantlar yordamida shifrlash algoritmi fizik hodisalar nuqtai nazaridan ko‘rib chiqiladi. Texnologiyaning amaliy qo‘llanilish usullari va uni amalga oshirish vositalari taqdim etiladi. Shuningdek, kvant kriptografiyaning dolzarb muammolari va afzalliklari tahlil qilingan. Kvantlarga asoslangan shifrlash tezligini oshiruvchi usul taklif etiladi.

Kalit so‘zlar. Axborot, xavfsizlik, axborotni himoya qilish, kvant kriptografiya.

Аннотация
В данной статье рассматриваются алгоритмы шифрования на основе квантовых технологий с точки зрения физических явлений. Представлены методы практического применения данной технологии и средства её реализации. Также анализируются актуальные проблемы и преимущества квантовой криптографии. Предлагается метод повышения скорости квантового шифрования.

Omega Journal of Linguistics and Language Studies
ISSN: 3072-4678
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

Ключевые слова: Информация, безопасность, защита информации, квантовая криптография.

Quantum cryptography is becoming increasingly important over time. Currently, most information is encrypted in such a way that the key can be decrypted by trying all possible options. The power of modern computers is not enough to crack long passwords. However, with the advent of quantum computers, this encryption system has become a threat, because they can solve such problems much faster than ordinary computers.

Quantum cryptography is a method of protecting communication systems based on the laws of quantum physics. With the development of quantum computers, the threat of cracking passwords for all types of information processing systems is increasing. Protection against such threats can be achieved through quantum-based encryption.

The key concept for quantum encryption is quantum superposition. This phenomenon can be explained by the example of the polarization of light. Since light is a transverse wave, it has a polarization property, which describes the direction of vibration. The polarization state of a single photon is called the quantum polarization state and can be vertical, horizontal, diagonal, and antidiagonal.

Let's consider an experiment with a polarizing beam splitter. A filter is placed in the path of light that passes photons with horizontal polarization and reflects photons with vertical polarization.

When a photon with diagonal polarization is sent, it will either pass through or return at the exit with a random probability. If it passes through a horizontal polarization path, its state will change to horizontal polarization. Similarly, in the vertical direction, the photon will assume the appropriate polarization state.

We will conduct a more complex experiment on a diagonally polarized photon, using the device shown in Figure 1. This device works on the principle of a Mach–Zehnder interferometer.

Omega Journal of Linguistics and Language Studies
ISSN: 3072-4678
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

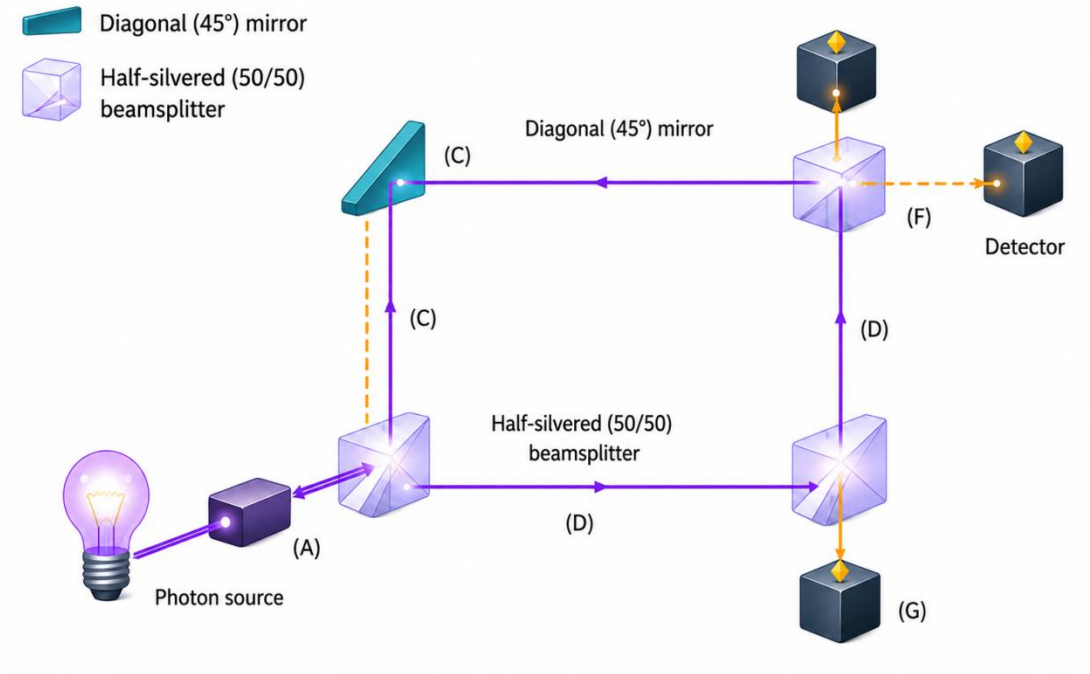

Figure 1. Mach-Zehnder interferometer.

Let the photon source be in state |A⟩ When it passes through the first semi-transparent window, it splits into two paths - |C⟩ va |D⟩. This process is expressed in terms of quantum amplitudes:

$$|A\rangle \rightarrow \frac{1}{2}(|C\rangle + i|D\rangle) \quad (1)$$

Here i denotes the phase shift (due to reflection).

Each path then reflects from its own mirror and recombines at the second semi-transparent mirror. The final output states are |F⟩ and |G⟩:

$$|C\rangle \rightarrow \frac{1}{2}(|F\rangle + i|G\rangle) \quad (2)$$

$$|D\rangle \rightarrow \frac{1}{2}(i|F\rangle + |G\rangle) \quad (3)$$

Now we find the general output state:

$$|A\rangle \rightarrow \frac{1}{2}[(1-1)|F\rangle + i(1+1)|G\rangle] = i|G\rangle \quad (4)$$

This result shows that if the phases match, all photons will fall on detector G, while nothing will be observed on detector F - this is the result of interference.

If one of the paths has a phase shift of ϕ, the general expression is:

Omega Journal of Linguistics and Language Studies
ISSN: 3072-4678
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

$$|A\rangle \rightarrow \frac{1}{2}\left[\left(e^{i\phi}-1\right)|F\rangle + i\left(e^{i\phi}+1\right)|G\rangle\right] \quad (5)$$

The output intensities from this formula are:

$$I_F \propto \sin^2\left(\frac{\phi}{2}\right), \quad I_G \propto \cos^2\left(\frac{\phi}{2}\right) \quad (6)$$

Although the diagonal photon has two paths - horizontally polarized and vertically polarized components - after the measurement, the photon returns with diagonal polarization at the output. Until the measurement is performed and it is determined which path the quantum of light has traveled, it is in a superposition of the horizontal and vertical polarization states [1].

In quantum cryptography, this quantum superposition phenomenon is used to encrypt information. The transmission process is carried out by encoding the polarization states of single photons emitted by pulsed semiconductor lasers in two alternative, mutually non-orthogonal bases.

The sender and receiver agree in advance on the values 0 and 1 for each polarization state. During transmission, the source sends a sequence of photons, and their polarization is chosen randomly. The receiver records the incoming photons and randomly chooses a measurement basis for each.

Through an open additional communication channel, the receiver tells the sender in which basis the measurement was made, but does not reveal the result. Since a photon can represent the value 0 or 1, transmitting only the measurement information over an open channel does not provide any useful information to a potential eavesdropper.

The sender, in turn, informs the receiver whether the correct basis has been chosen for each photon. Only measurements made in the correct basis are stored, and on this basis the parties generate a sequence of common random 0s and 1s, which is formed as a private key [2].

In practice, a quantum key distribution system consists of the following components: a laser as a source of single photons on one side, and a calcite prism as a receiving device on the other. This prism splits the light flux into two components, which are recorded by two photodetectors. The photodetectors, in turn, measure the orthogonal components of the polarization. An optical fiber communication line is used as the information transmission medium.

Omega Journal of Linguistics and Language Studies
ISSN: 3072-4678
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

If there are 1000 quanta in a pulse, there is a chance that 100 of them will be directed by the cryptanalyst to his receiver. After analyzing the open exchange (negotiations carried out over an open channel), he will be able to obtain all the necessary information. It follows that the most ideal situation is that the number of quanta in the pulse converges, that is, only one photon is transmitted per pulse. In such conditions, any attempt to eavesdrop will change the state of the entire system and lead to an increase in the number of errors on the receiving side.

In this situation, it is necessary to retransmit the received information rather than directly decoding it. However, attempts to increase channel reliability maximize the sensitivity of the receiving device, which introduces the problem of "dark noise." This means that the receiver may receive a signal that was not actually sent.

To ensure the reliability of data transmission, each logical value in the binary system (0 and 1) is encoded not as a single state, but as a sequence of states. This allows for error detection and correction even for multiple failures [3].

As photons travel through an optical channel, their effective range is limited by their attenuation. Quantum repeaters are proposed as a solution to this problem - devices that can reconstruct quantum information without loss.

In addition, the Micius satellite, developed by Chinese scientists in 2016, was a significant technological breakthrough aimed at solving the problem of quantum information transmission over long distances. In 2017, it became fully operational and carried out experiments on the transmission of photons from Earth orbit to Earth using quantum teleportation [4].

The satellite transmits encrypted messages based on quantum teleportation, as well as receiving and transmitting quantum entangled particles. The quantum states of these particles are used as an encryption key at a certain moment in time. The system is equipped with special devices designed for quantum communication - a quantum key communicator, a quantum entanglement source, a control processor and a high-speed laser communication system [5].

In 2019, IBM introduced the first commercial quantum computer model. This technology has already gained practical application and is expected to develop further in the future. Quantum computers can also increase the possibility of unauthorized access to information in some cases [6]. Nevertheless, quantum cryptography is a system that can detect any external interference. Direct

Omega Journal of Linguistics and Language Studies
ISSN: 3072-4678
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

eavesdropping on communication channels based on individual microparticles is impossible, since according to the laws of quantum physics, the measurement process changes the state of the particle. This is confirmed by the theorem on the prohibition of cloning quantum states. Therefore, a significant increase in the error rate in the communication channel indicates the presence of external interference in the system, and the generated key in such a case cannot be used. Important information is transmitted only after the successful distribution of the quantum key. Any eavesdropping or interference attempts are immediately detected, and if necessary, the possibility of identifying the source of the attack becomes apparent.

Despite the high level of protection offered by quantum cryptography, quantum encryption based on polarization coding has a number of drawbacks that prevent this technology from being widely implemented at the current stage. These drawbacks include:

complex methods for controlling polarization do not always work, which leads to an increase in the number of errors in the key;

there is instability of single photon polarization, and the main errors occur due to the loss of the polarization state of the photon during its passage through the information channel;

the greater the transmission distance, the greater the probability of information loss and the lower the transmission speed;

the process of correcting errors in polarization detection complicates the system and reduces its performance;

compared to traditional encryption methods, the data transfer rate in terrestrial quantum communication systems is low and the error rate is relatively high [7].

Since the quantum key transmission speed is limited, our team proposes a combination of encryption methods to transmit long keys in a short time. According to this idea, the key is divided into two parts: one part is encrypted using quantum cryptography, and the second part is transmitted using other classical cryptographic methods. This approach significantly increases the transmission speed, while maintaining the level of security. The part encrypted using quantum methods remains unbreakable for a potential attacker. Even if an attacker obtains part of the key, it will not have any practical value, since the

Omega Journal of Linguistics and Language Studies
ISSN: 3072-4678
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

second part is not available. In the event of an attempt to fully penetrate, the system will detect a violation and stop the transmission process.

In conclusion, the use of quantum technologies in the field of information encryption can significantly facilitate the work of specialists in ensuring information security. This is especially important in the context of the rapid development of modern computing power and the emergence of technologies that threaten information. Quantum cryptography is an effective tool for reducing the threat posed by quantum computers to traditional cryptosystems. However, since these technologies are relatively new, there are a number of problems that need to be solved before they can be widely implemented.

REFERENCES

1. Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shaari, J. S., Tomamichel, M., & Usenko, V. C.*"Advances in quantum cryptography"*Nature Photonics, 12(10), 2019. –641–652 bet .DOI: 10.1038/s41566-019-0401-9

2. Nielsen, M. A., & Chuang, I. L.*"Quantum Computation and Quantum Information"* (10th Anniversary Edition) Cambridge University Press, 2010. 1–702 bet. ISBN: 978-1-107-00217-3

3. И. Ферапонтов Квантовая криптография: что это такое? [Элек-тронный ресурс]: Электронный журнал Популярная механика, 29 мая 2018. URL:https://www.popmech.ru/technologies/235655-kvantovaya-kriptografiyachto-eto-takoe/#part2.

4. М. Агаджанов Китайский спутник использовал квантовую крип-тографию для проведения защищенной межконтинентальной видеоконфе-ренции [Электронный ресурс]: портал Habr, 1 февраля 2018. URL: https://habr.com/ru/post/410071.

5. BergerReleaseoffirstquantumcomputer [Электронный ресурс]: официальный сайт IBM, 9 января 2019. URL: https://www.ibm.com/quantumcomputing/.

6. П. Громов Китайский спутник квантовой связи прошел испытания и готов к работе [Электронный ресурс]: Электронный журнал ХАЙТЕК, 19 января 2017. URL: https://hightech.fm/2017/01/19/micius-ready.

7. А.С. Альбов «Квантовая криптография»: Санкт-Петербург – изд. Страта, 2015. – 132-176 bet. – ISBN: 978-5-906150-35-6.