UDC 004.056.55:003.26
DOI: 10.24025/2306-4412.3.2023.288020

A BASIC QUANTUM KEY DISTRIBUTION PROTOCOL

Serhiy Dorozhynskyi
Assistant Professor of the Department of Computer Information Technologies
of the Faculty of Computer Sciences and Technologies of the NAU,
Junior Researcher of the National Research Institute for Combating Cyber Threats
in the Aviation Industry
National Aviation University, 1, Liubomyra Huzara Ave., Kyiv, Ukraine
https://orcid.org/0000-0002-5395-6423, e-mail: dorozhynskyi.serhii@npp.nau.edu.ua

Abstract. Over time, the complexity of threats that can be perpetrated against critical infrastructure is increasing, including cyberattacks, large-scale failures, terrorist attacks, etc. The confidentiality of data processed and transmitted within critical infrastructure is a key aspect of its security. Traditional cryptography methods, although reliable, are becoming vulnerable to advanced computing and quantum capabilities of attackers. For this reason, the relevance of studying and applying quantum cryptography in critical infrastructure is becoming increasingly important. They are highly resistant to attacks related to computational aspects and provide untraceability of keys and data due to the principles of uncertainty. However, they also require complex technical implementation and further research for widespread implementation. Quantum cryptography can provide reliable protection against current and future attacks while maintaining data confidentiality and user identification. However, it is important to choose the right methods and tools to ensure the maximum level of data confidentiality, taking into account the characteristics of the network.
The article describes in detail the processes of improving the quantum key distribution protocol using quantum identification and quantum channel multiplexing methods, describes the mathematical apparatus of the improved method, and defines the stages of forming the key distribution protocol stack. The proposed improved method of quantum key distribution creates the possibility of its universal application under conditions of uncertainty, providing fast operation speed and a higher level of data security.

Keywords: Twin Field protocol, quantum channel multiplexing, quantum identification, quantum channels, quantum cryptography, key distribution protocol stack.

Introduction

Today, one of the newest quantum key distribution protocols is the Twin Field QKD protocol (Sun *et al*., 2022; Meda *et al*., 2022; Chan *et al*., 2021). It uses the concept of two polarized quantum channels and quantum interference between two polarized photon states to ensure secure key exchange between two parties. Due to its characteristics, it is considered the most promising of all known protocols, if the type of attack is not taken into account. However, it can also be improved. In particular, it is possible to improve the efficiency of the protocol by reducing the number of errors and increasing the data transfer rate. New technologies can be used for this purpose, for example, the use of quantum channel multiplexing, which allows more information to be transmitted simultaneously, as well as the use of new methods of data processing and verification. It is also possible to use more sophisticated encryption techniques that allow for a higher level of security for the transmission of quantum information. In particular, there is the "quantum identification" technique, where information is transmitted between the parties using a quantum system that provides mutual authentication of the parties. Twin Field QKD (TF-QKD) (Park & Heo, 2021) is a quantum key distribution protocol that uses

DOI: 10.24025/2306-4412.3.2023.288020

two synchronized emitting circuits that generate pairs of photons in a spin state. Thus, quantum channels in TF-QKD are channels that transmit quantum bits based on photon emission.

The purpose of the article is to reveal the principles of quantum key distribution, to identify its role in ensuring the security of communications and information exchange, and to consider the possibilities of applying this protocol in various fields, including cryptography and network security.

The main objectives of the research are:

1. Consider the principles and functionality of the Twin Field QKD protocol, including its main components and stages of operation.
2. Analyze the multiplexing methods used to simultaneously transmit multiple quantum channels and determine their efficiency and advantages.
3. Present specific improvements to the Twin Field protocol, including multiplexing techniques and quantization, and justify their importance.
4. Consider the practical aspects of implementing the Twin Field QKD protocol and new methods of multiplexing and quantization.
5. Identify opportunities for further research in the field of quantum key distribution and development of the Twin Field protocol.

Development of a basic QKD protocol. Quantum channel multiplexing can be applied to TF-QKD in order to increase the bandwidth and efficiency of quantum key distribution. Quantum channel multiplexing (Woo et al., 2020; Wengerowsky *et al*., 2019) allows more information to be transmitted over a quantum channel at one time by dividing it into multiple physical channels. However, when applying quantum channel multiplexing to TF-QKD, some technical difficulties must be taken into account due to the increasing number of photons to be transmitted through quantum channels. As the number of photons increases, the noise in the channel increases and can degrade the transmission quality.

To avoid the deterioration in transmission quality associated with the increase in the number of photons to be transmitted through quantum channels when multiplexing quantum channels in the Twin Field QKD protocol, additional techniques can be used to reduce channel noise. One such technique is to reduce the impact of channel noise by filtering the signal. Filtering can reduce channel noise by eliminating some of the noise that affects signal transmission.

Materials and methods

Multiplexing of quantum channels (Lin *et al*., 2020) in the Twin Field QKD protocol can lead to an increase in the number of transmitted photons and the time required for data transmission. The quantitative indicators that may increase with quantum channel multiplexing may include:

1. The number of photons required to transmit data may increase depending on how many channels are to be multiplexed.
2. The data transmission time may increase due to the need to transmit more photons and depending on the photon transmission rate through the quantum channels.
3. Energy consumption for data transmission may increase due to the need to use additional equipment to multiplex the channels and signal amplifiers to transmit the photons.
4. The complexity of the system may increase due to the need to use additional equipment and software for multiplexing quantum channels.
5. The cost of the system may increase due to the need to use additional hardware and software for quantum channel multiplexing.

DOI: 10.24025/2306-4412.3.2023.288020

Wavelength Division Multiplexing (Haigh *et al*., 2020; Wang *et al*., 2022; Yousefi, & Yangzhang, 2020) is a technology used in fiber optic communications where multiple signals of different wavelengths are combined in the same medium (i.e., optical fiber) through superposition. Thanks to multiplexing, the sending and receiving parties can transmit large amounts of information to each other over a single channel, thus making more efficient use of the available optical fiber bandwidth. When integrating a QKD system with an existing fiber infrastructure, multiplexing allows quantum and classical signals used for key generation, synchronization, error correction, and privacy enhancement to coexist with data signals carrying other information for bidirectional communication between parties over the same fiber line. Consequently, multiplexing makes the QKD process less resource-intensive, as a single fiber can be used to transmit all the information between the transmitter and receiver, instead of using separate fibers for each of the quantum and classical signals.

The process of quantum channel multiplexing for the TF-QKD protocol can be described as follows:

1. Preparation of quantum groups: Quantum groups are prepared at the transmitter (Alice) and receiver (Bob). Each quantum group is composed of light pulses that correspond to quantum bits (qubits) using, for example, photon polarization. The formula for preparing quantum groups during quantum channel multiplexing for the Twin Field QKD protocol can be given as follows:

Suppose we have N quantum channels, then each channel must use M quantum states to transmit data. At the same time, according to the Twin Field QKD protocol, each of the channels must use L quantum states to measure in the correct basis. Therefore, the total number of quantum states required to prepare quantum groups for N channels can be calculated by the formula:

$$N_g = N(M+L), \tag{1}$$

where N_g is the total number of quantum states required to prepare quantum groups for all N channels.

2. Multiplexing of quantum channels: The quantum groups are transmitted over a single channel that multiplexes the quantum channels using, for example, frequency division multiplexing. The formula for multiplexing quantum channels for the Twin Field QKD protocol can be given as follows:

Suppose we have N quantum channels that we want to multiplex, and for each of them we use two phase-shifted light modulators to transmit two quantum states. Each channel transmits M quantum states for data transmission and L quantum states for measurement in the correct basis. The total number of quantum states required to multiplex N channels can be calculated by the formula:

$$N_t = 2N(M + L), \tag{2}$$

where N_t is the total number of quantum states required to multiplex all N channels.

3. Transmission of quantum groups: Quantum groups are transmitted from the transmitter to the receiver. The quantum groups passing through the channel can be labeled with indices, allowing them to be separated at the receiver. The quantum group transmission formula for quantum channel multiplexing in the Twin Field QKD protocol can be written as follows:

Suppose we have N quantum channels that we want to multiplex, and for each of them we use two phase-shifted light modulators to transmit two quantum states. To multiplex the quantum states from different channels, two different quantum channels are used - channel Z and channel X - which transmit information using vertical and horizontal polarization, respectively.

DOI: 10.24025/2306-4412.3.2023.288020

When multiplexing quantum states from N channels, the total quantum state is transmitted to channel Z:

$$\left|\varphi_Z\right\rangle = \bigotimes_{j=1}^{N} \left|\varphi_j^{(Z)}\right\rangle, \tag{3}$$

where $\varphi_j^{(Z)}$ is the quantum state transmitted in the j-th quantum channel using channel Z. Similarly, the total quantum state is transmitted for channel X:

$$\left|\varphi_X\right\rangle = \bigotimes_{j=1}^{N} \left|\varphi_j^{(X)}\right\rangle, \tag{4}$$

where $\varphi_j^{(X)}$ is the quantum state transmitted in the j-th quantum channel via channel X.

In both cases, we multiply quantum states from different channels because they are transmitted through different quantum channels (channel Z and channel X).

4. Measurement of quantum groups: At the receiver, each quantum group is measured separately to obtain quantum bit values. The results are then used to calculate the key.

After the total quantum states have been transmitted over the Z and X channels, respectively, they arrive at the receiver. To measure each quantum state from each channel, the receiver uses two phase-shifted light modulators that measure the vertical and horizontal polarization. After measuring the quantum state in the j-th channel using the Z channel, the measurement operator for the vertical polarization is as follows:

$$M_J^{(Z,0)} = \left|0\right\rangle\left\langle 0\right|, \tag{5}$$

and for horizontal polarization:

$$M_J^{(Z,1)} = \left|1\right\rangle\left\langle 1\right|. \tag{6}$$

Similarly, after measuring the quantum state in the j-th channel using channel X, the measurement operator for the vertical polarization is as follows:

$$M_J^{(X,0)} = \frac{1}{2}\left(\left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|\right), \tag{7}$$

and for horizontal polarization:

$$M_J^{(X,1)} = \frac{1}{2}\left(\left|0\right\rangle\left\langle 0\right| - \left|1\right\rangle\left\langle 1\right|\right). \tag{8}$$

As a result of measuring the vertical and horizontal polarization for each channel, the receiver receives two-bit sequences: *bj(Z)* and *bj(X)*, which correspond to the results of measuring the quantum state in the j-th channel using channel Z and channel X, respectively.

In the process of measurement, a projection onto the corresponding basis occurs. Thus, the output state will be equal to the projection of the input state onto the corresponding basis:

$$\left|\varphi_{Z,out}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle\left\langle 0\right| + \left|1\right\rangle\left\langle 1\right|\right)\left|\varphi_Z\right\rangle, \tag{9}$$

$$\left|\varphi_{X,out}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+\right\rangle\left\langle +\right| + \left|-\right\rangle\left\langle -\right|\right)\left|\varphi_X\right\rangle, \tag{10}$$

$$\left|\varphi_{Y,out}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+i\right\rangle\left\langle +i\right| + \left|-i\right\rangle\left\langle -i\right|\right)\left|\varphi_Y\right\rangle, \tag{11}$$

where $\left|\varphi_{Z,out}\right\rangle$, $\left|\varphi_{X,out}\right\rangle$, $\left|\varphi_{Y,out}\right\rangle$ are the input quantum states, and $\left|\varphi_Z\right\rangle$, $\left|\varphi_X\right\rangle$, $\left|\varphi_Y\right\rangle$ are the output quantum states after projection to the corresponding basis. These output states are transmitted through the appropriate channels on the receiver side, which decompresses them and performs measurements as in the opposite direction, which allows to obtain a bit sequence in which information is stored according to the basis in which the states were measured.

DOI: 10.24025/2306-4412.3.2023.288020

5. Error correction: If errors occur during the measurement process, a feedback channel can be used to correct the errors, as is commonly done in quantum key distribution protocols. The feedback channel allows you to eliminate erroneous bits and improve the quality of information transmission.

The error correction formula in the quantum channel multiplexing protocol for TF-QKD uses the least squares principle and consists in finding the optimal error vector e for each channel by means of measurements in the *Z*-base and using the inverse propagation matrix:

$$e = S^{-1}(X - Y), \tag{12}$$

where X is Alice's measurement, Y is Bob's measurement, and S is the propagation matrix representing the relationship between the number of transmitted and received quantum bits.

The resulting error vector e is then used to correct the output keys received from each channel by eliminating the bits that cause errors.

In the TF-QKD protocol, quantum channel multiplexing allows to increase the number of transmitted quantum bits per unit time. This improves the efficiency of the protocol and reduces the time it takes to transmit keys between Alice and Bob. However, multiplexing quantum channels can lead to some problems, such as increased channel noise and the need to use more complex error correction methods. In general, quantum channel multiplexing is an important element in quantum key distribution protocols, which allows to increase the efficiency and speed of information transmission. However, when using this technology, it is necessary to take into account some technical difficulties and problems that may affect the quality of data transmission.

The Twin Field protocol is one of the quantum key distribution protocols to which quantum identification (QID) can be applied to identify trusted devices and ensure the security of the key distribution process.

The process of applying quantum identification in TF-QKD includes the following steps:

1. Physical channel verification: Before starting the identification process, each device verifies the physical channel to ensure that it is not subject to interception or data modification. The process of verifying physical communication channels with quantum identification includes the following steps:

- Quantum state generation: The sender and receiver generate quantum states to be used during verification.
- Sending and receiving quantum states: the sender sends quantum states to the receiver through a physical communication channel. The receiver receives the quantum states and stores them for further processing.
- Measurement of states: the receiver measures the quantum states that have come to it. The measurement is performed in a random base, which is determined randomly for each state.
- Sending the measurement results: the receiver sends the measurement results to the sender via an unsecured communication channel.
- Comparison of results: the sender compares the receiver's measurement results with its own results. If the results match, the communication channel is considered secure. If the results do not match, it may indicate that the communication channel has been compromised.
- Repeat the procedure: If the results do not match, the process is repeated several times. If the results still do not match, the channel is secure.

2. Sending test signals: During the identification process, each device sends test quantum signals to the other device.

DOI: 10.24025/2306-4412.3.2023.288020

3. Measuring the received signals: after receiving the quantum signals, each device measures them to obtain information about the states in which they were sent.

4. Comparing the results: each device compares the measurement results to make sure that the test signals were received correctly.

5. Reliable identification: If the comparison results match expectations, the devices can identify each other as trusted. If the results do not match, the process is repeated until the devices are reliably identified.

6. Transition to the key distribution phase: after successful identification, the devices move to the key distribution phase, in which they perform quantum signals to create a shared encryption key that will be used to securely exchange information between the trusted devices.

In the key distribution process, quantum signals are sent by the sender and then received by the receiver. The sender and receiver compare the results of their measurements to determine whether the data was transmitted without interference. If the results match, then they can use a shared key to securely encrypt and decrypt messages. If the results do not match, it indicates an interception attempt, and the process repeats.

Formation of a key distribution protocol stack. The quantum protocol stack (Zhao, & Qiao, 2023) is a set of different stages and procedures used in quantum protocols to ensure the security of information transmission. Building a stack is an important component of a quantum protocol and helps ensure its security and reliability. The stack is used to store intermediate results during the execution of a quantum protocol. When two parties to the protocol interact, each of them saves its own parts of the stack. Saving this data allows you to preserve the order of interaction between the parties to the protocol and ensure the correct execution of its steps. The Twin Field QKD protocol is one of the quantum protocols used to securely exchange keys between two parties. The following stack can be created for it:

1. Quantum source – generates pairs of quantum bits (qubits) that are transmitted through different channels.

2. Quantum multiplexer – combines quantum bits from different channels into one quantum stream.

3. Quantum channel – transmits quantum bits between remote parties to the protocol.

4. Quantum demultiplexer – breaks the quantum stream into separate quantum bits, which are then sent to the receivers.

5. Quantum receiver – receives the quantum bits and performs measurements of the corresponding states to obtain keys.

6. Classical channel – transmits classical bits (e.g., to preserve the parameters of quantum bit transmission) between remote parties to the protocol.

7. Quantum identifier – used to verify that the receivers are the true receivers of the corresponding quantum bits. This is achieved by sending additional quantum bits that are used to measure identical states between remote parties.

8. Classical identifier – used to transmit information about the confirmation of successful quantum identification and other classical messages used to control the protocol.

The Twin Field QKD protocol uses two quantum channels to transmit quantum bits, and quantum sources are used to generate pairs of quantum bits per channel. To multiplex the quantum channels, different frequencies of light are used for each channel, which can be separated by using appropriate filters. For example, you can use filters with an opaque band for one channel at one light frequency, and filters with an opaque band for another channel at

DOI: 10.24025/2306-4412.3.2023.288020

another light frequency. In this case, quantum sources generate pairs of quantum bits on each channel at the corresponding light frequency.

In addition, the Twin Field QKD protocol uses quantum identification to provide an additional level of security for the transmission of quantum bits. Quantum identification is based on the fact that the detector can measure the parameters of the photon's quantum state without changing this state. Quantum identification is used to verify that the correct quantum bits have been transmitted and to detect possible attempts to intercept quantum bits.

Quantum sources for the Twin Field QKD protocol generate pairs of quantum bits with the appropriate light frequencies for each channel, which are then transmitted through quantum channels. Quantum identification is used to verify the correctness of the transmission and provide an additional level of security for the transmission of quantum bits.

To realize this process, we obtain the following mathematical model:

1. Measurement of the energy state of an electron in an atom:

$$H_{at}\left|\psi_i\right\rangle = E_i\left|\psi_i\right\rangle. \tag{13}$$

2. Sending the generated photon to the generated detector:

$$\left|\psi_i\right\rangle \to \left|\psi_f\right\rangle. \tag{14}$$

3. Registering the generated photon:

$$\left|\psi_f\right\rangle \to \left|1\right\rangle \text{ with probability } P_1 \text{ or } \left|0\right\rangle \text{ with probability } P_0\ . \tag{15}$$

4. Mixing of generated photons using quantum channel multiplexing:

$$\left|\psi\right\rangle = \Sigma^{n}{}_{i=1}\alpha_i\left|1_i\right\rangle. \tag{16}$$

5. Using quantum identification to check the state of photons:

$$\left|\psi\right\rangle = \Sigma^{n}{}_{i=1}\alpha_i\left|1_i\right\rangle \to \left|\psi'\right\rangle = \Sigma^{n}{}_{i=1\beta i}\left|1_i\right\rangle або \left|\psi'\right\rangle = \left|0\right\rangle. \tag{17}$$

6. Transmission of a mixed signal to the receiver and the beginning of the process of quantum key exchange using the Twin Field QKD protocol:

$$\rho_{mix} = p_1\rho_1 + p_2\rho_2 + ... + p_n\rho_n, \tag{18}$$

where n is the number of channels through which quantum states are transmitted, p_i is the probability of sending a quantum state through channel i, and p_{mix} is the mixed quantum state received at the receiver after mixing signals from different channels.

A quantum multiplexer (Lu, & Qiu, 2020; Khan *et al*., 2016) for Twin Field QKD protocol is a device that allows multiplexing multiple quantum channels in a single fiber optic link. Using a quantum multiplexer, several independent quantum channels can be transmitted over a single fiber while maintaining their independence.

The quantum multiplexer in the Twin Field protocol also provides quantum identification (QID), which allows detection of any intermediate controlled cross-path emitters (CPEs) that can be used to study or steal quantum information. The QID is used to determine the individual state of each qubit that is transmitted through the quantum channel. This allows us to confirm that the qubits have not been tampered with during transmission and that the channel has not been compromised.

The following formulas are used for the quantum multiplexer in the Twin Field QKD protocol:

1. Formula for preparing quantum groups:

$$\left|\psi\right\rangle_{AB} = \frac{1}{\sqrt{2}}(\left|0\right\rangle_A\left|\psi_0\right\rangle_B + (\left|1\right\rangle_A\left|\psi_1\right\rangle_B, \tag{19}$$

DOI: 10.24025/2306-4412.3.2023.288020

where $|\psi_0\rangle_B$ and $|\psi_1\rangle_B$ are quantum states corresponding to different communication channels.

2. The formula for multiplexing quantum channels:

$$|\psi\rangle_{ABCD} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|\psi_0\rangle_B|\psi_0\rangle_C + |1\rangle_A|\psi_1\rangle_B|\psi_1\rangle_C\right), \tag{20}$$

where $|\psi_0\rangle_C$ and $|\psi_1\rangle_C$ are quantum states corresponding to different user IDs.

3. The formula for the transmission of quantum groups:

$$|\psi\rangle_{AB} \to \frac{1}{\sqrt{2}}(|0\rangle_A|\psi_0\rangle_B + |1\rangle_A|\psi_1\rangle_B). \tag{21}$$

4. Formula for measuring quantum groups:

$$M^Z{}_B(M^X{}_A \otimes I_{BC})|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|0\rangle_A|\psi_0\rangle_B|\psi_0\rangle_C - |1\rangle_A|\psi_1\rangle_B|\psi_1\rangle_C), \tag{22}$$

where $M^X{}_A$ and $M^Z{}_B$ are the measurement operators corresponding to the X and Z bases, respectively.

5. Error correction formula:

$$|\psi_{corr}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^A|0\rangle^B + e^{i\phi}|1\rangle^A|1\rangle^B) \otimes |\varphi\rangle_{AB}, \tag{23}$$

where $|\varphi\rangle_{AB}$ is the shared quantum state used for quantum identification.

A quantum channel for the Twin Field QKD protocol is a communication channel between two trusted parties (for example, Alice and Bob) that allows the transmission of quantum states using quantum channel multiplexing and quantum identification technologies. Such a channel ensures the security of information transmission through the use of the laws of quantum mechanics and quantum cryptography, which makes it reliable for protecting confidential information.

A quantum channel is formed according to the following scenario:

1. Encoding quantum bits of the transmitted message into quantum states:

$$|\psi_0\rangle = |0\rangle,\ |\psi_1\rangle = |1\rangle,\ |\psi_2\rangle = |+\rangle,\ |\psi_3\rangle = |-\rangle. \tag{24}$$

2. Base transformation operations on the side of Alice and Bob:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{(Adamar operation)}, \tag{25}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{(PaulSinger operation)}. \tag{26}$$

3. Multiplexing of two quantum channels transmitting quantum bits $|\psi_0\rangle$ and $|\psi_1\rangle$:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle_A|\psi_0\rangle_B + |\psi_1\rangle_A|\psi_1\rangle_B).$$

4. Multiplexing of two quantum channels transmitting quantum bits $|\psi_2\rangle$ and $|\psi_3\rangle$:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|\psi_2\rangle_A|\psi_2\rangle_B + |\psi_3\rangle_A|\psi_3\rangle_B). \tag{27}$$

5. Transmission of quantum channels from Alice to Bob.
6. Measurement of quantum channels using projectors on the ground states.
7. Error correction.

DOI: 10.24025/2306-4412.3.2023.288020

A quantum demultiplexer for the Twin Field QKD protocol is a device that separates a mixture of quantum signals that have been transmitted over a quantum channel using quantum channel multiplexing. The device distributes quantum signals to different receivers that receive these signals using quantum identification. The quantum demultiplexer is an important component of the Twin Field QKD protocol, as it allows for a continuous flow of quantum data between the parties involved in the quantum key exchange. The multiplexed quantum signals are separated in the following sequence:

1. Time slot division.

$$U\hat{}^{(t)}_{dmux} = \sum^{n}_{i=1} P\hat{}^{(t)}_{i} \otimes U\hat{}_{swap} \otimes P\hat{}^{(t)}_{i}, \tag{28}$$

where $P\hat{}^{(t)}_{i}$ is a projector to a quantum state in time slot t, $U\hat{}_{swap}$ is a SWAP gate that exchanges states of two qubits.

2. Separation of frequency channels:

$$U\hat{}^{(f)}_{dmux} = \sum^{n}_{i=1} P\hat{}^{(f)}_{i} \otimes U\hat{}_{swap} \otimes P\hat{}^{(f)}_{i}. \tag{29}$$

3. Separation of spins:

$$U\hat{}^{(s)}_{dmux} = \sum^{N}_{i=1} P\hat{}^{(s)}_{i} \otimes U\hat{}_{swap} \otimes P\hat{}^{(s)}_{i}. \tag{30}$$

A quantum receiver for the Twin Field QKD protocol is a device that is designed to receive quantum signals that have been transmitted over multiplexed channels within this protocol. The quantum receiver allows quantum identification and reading of the data transmitted by the sender.

In the Twin Field QKD protocol, the quantum receiver receives quantum signals containing photons that have been emitted by random polarizations from different channels. The receiver can measure the polarization of each photon and determine which channel it belongs to by means of multiplexing. In addition, the quantum receiver performs quantum identification, which allows you to verify that the data was transmitted without interception.

The formulas for the quantum receiver for the Twin Field QKD protocol are complex and depend on the specific implementation of the device. However, the general approach is to measure the quantum states containing photons from different channels and process this data to recover the transmitted information.

1. First, a measurement operation is performed in the basis corresponding to the transmitted bit:

$$M\hat{}_{j} = \int_{Bj} d\omega \left|\omega\right\rangle\left\langle\omega\right|, \tag{31}$$

where $j \in \{0,1\}$ is the transmitted bit, B_j is the basis corresponding to the transmitted bit, $|\omega\rangle$ is the state of the input quantum signal.

2. Probability of receiving the transmitted bit:

$$p_j = Tr\{\rho_j M\hat{}_{j}\}, \tag{32}$$

where ρ_j is the state density of the transmitted quantum signal.

3. The probability of error in the quantum channel:

$$e = \frac{1}{\sqrt{2}}(\sqrt{p_0} - \sqrt{p_1})^2. \tag{33}$$

4. Error correction:

$$E\hat{} = \frac{1}{\sqrt{p_0}}\left|0\right\rangle\left\langle 0\right| - \frac{1}{\sqrt{p_1}}\left|1\right\rangle\left\langle 1\right|. \tag{34}$$

5. The final state obtained after error correction:

$$\rho' = E\hat{}_{\rho j} E\hat{}^{\dagger}. \tag{35}$$

DOI: 10.24025/2306-4412.3.2023.288020

The quantum identifier is one of the elements of the Twin Field QKD protocol and is used to determine the identity of quantum channels between two interlocutors. Its main purpose is to prevent eavesdropping on quantum channels and message tampering. It can be implemented using quantum systems, such as photons or qubits, which are sent between the two parties to the protocol. In this case, the interaction between quantum systems allows the interlocutors to determine whether the channels are identical, i.e. whether they have not been altered or tampered with.

The quantum identifier in the Twin Field QKD protocol can be described by the following formulas:

1. Suppose Alice has a prepared state ρ_A and sends it over the channel to Bob. Bob can retrieve this state using the decomposition operator:

$$\left|\psi'_B\right\rangle = E\left(\rho_A\right)\left|\psi_A\right\rangle. \tag{36}$$

2. Bob can then verify that the state was sent by Alice using quantum identification:

$$P_{accept} = Tr(M\rho_A), \tag{37}$$

where M is the projection operator for recognizing the state, and T_r is the trace operator. If P_{accept} is high enough, Bob confirms that the state was sent from Alice.

The classic identifier for the Twin Field QKD protocol is an information exchange between the parties to the protocol used to confirm mutual authenticity and establish the secret key. It includes identification information about each user, such as name, device number, public key, etc., as well as information about the protocol parameters used to generate quantum keys. In addition, the classical identifier may also include information about the state of the communication channel, such as the noise level, which may affect the quality of quantum data transmission.

The formula for the classical identifier in the Twin Field QKD protocol can be written as:

$$c = H\left(x\right), \tag{38}$$

where H is a hashing function that converts a random vector x into a random number c of fixed length. The value of c is sent to the sender and receiver so that they can compare their identities and make sure they are using the correct quantum channels and quantum bits to exchange keys.

Also, to make the protocol more secure, a hash function with a key k can be used, which is added to the formula:

$$c = Hk\left(x\right). \tag{39}$$

Results and discussion

The principles and main components of the Twin Field QKD protocol were considered in detail during the study. The results presented on quantum channel multiplexing methods that can be used to simultaneously transmit more than one quantum stream. It was shown how these methods can improve the performance and efficiency of the Twin Field QKD protocol. This paper explores the possibilities and advantages of quantum identification in the context of quantum key distribution and shows how this aspect can improve the security and robustness of the protocol. It follows from the research that the use of quantum channel multiplexing and quantum identification methods can significantly improve the efficiency of the Twin Field QKD protocol. This opens up new opportunities for secure and efficient quantum key distribution.

DOI: 10.24025/2306-4412.3.2023.288020

Conclusions

This paper presents the development of a quantum key distribution protocol based on the improved Twin Field QKD protocol. One of the key achievements is the use of quantum signal multiplexing methods, which made it possible to bring the protocol to a new level of efficiency and speed of quantum key transmission. This opens up a wide range of opportunities for the development of quantum communications and ensuring their operation in real-world conditions. Additionally, the article discusses the introduction of quantum identification methods that provide a high level of security in the distribution of quantum keys. This is becoming an important factor, especially in the context of modern cybersecurity threats. In addition, the article demonstrates the developed concept of a key distribution protocol stack that allows choosing the optimal protocol depending on specific scenarios and communication requirements. This makes the system flexible and adaptive to different conditions. In summary, this paper opens up new application perspectives for quantum communication by enhancing the security and efficiency of the key distribution process. This helps to create a solid foundation for the development of quantum networks and expands the possibilities of applying quantum technology in the modern world, including the areas of cybersecurity, communications, and computing.

Acknowledgments

I would like to express special gratitude to the NAU Cybersecurity R&D Lab and its scientific advisor, doctor of technical sciences, professor Sergiy Gnatyuk, for the research assistance and technical support.

Conflict of Interest

There is no conflict of interest.

References

Chan, A., Khalil, M., Shahriar, K.A., Chen, L.R., Plant D.V., & Kuang, R. (2021). Security analysis of a next generation TF-QKD for secure public key distribution with coherent detection over classical optical fiber networks. In *7th International Conference on Computer and Communications (ICCC)* (pp. 416-420). Chengdu, China. doi: 10.1109/ICCC54389.2021.9674320.

Haigh, P.A., Burton, A., Chvojka, P., Zvanovec, S., Ghassemlooy, Z. & Darwazeh, I. (2020). Visible light communications: Filterless wavelength division multiplexing. In *12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)* (pp. 1-5). Porto, Portugal. doi: 10.1109/CSNDSP49049.2020.9249495.

Joshi, S.K. et al. (2021). Entanglement based quantum networks: Protocols, AI control plane & coexistence with classical communication. In *Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC)* (pp. 1-1). Munich, Germany. doi: 10.1109/CLEO/Europe-EQEC52157.2021.9542689.

Khan, A., Mandal, S., Nag S. & Chakrabarty, R. (2016). Efficient multiplexer design and analysis using quantum dot cellular automata. *Conference: 2016 IEEE Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)* (pp. 163-168). Mangalore, India. doi: 10.1109/DISCOVER.2016.7806233.

Lin, R. et al. (2020). Telecommunication compatibility evaluation for co-existing quantum key distribution in homogenous multicore fiber. *IEEE Access,* 8, 78836-78846. doi: 10.1109/ACCESS.2020.2990186.

DOI: 10.24025/2306-4412.3.2023.288020

Lu, W. & Qiu, J. (2020). Coherent polarization states multiplexer and its feasibility in quantum communication. *IEEE Access,* 8, 114354-114360. doi: 10.1109/ ACCESS.2020.3004154.

Meda, A. et al. (2022). QKD and frequency distribution cooperation: The Twin-Field QKD case. In *IEEE 15th Workshop on Low Temperature Electronics (WOLTE)* (pp. 1-4). Matera, Italy. doi: 10.1109/WOLTE55422.2022.9882601.

Padamvathi, V., Vardhan, B.V., & Krishna, A.V.N. (2016). Quantum cryptography and quantum key distribution protocols: A survey. In *IEEE 6th International Conference on Advanced Computing (IACC)* (pp. 556-562). Bhimavaram, India. doi: 10.1109/ IACC.2016.109.

Park, J., & Heo, J. (2021). Finite-key-size effect in asymmetric Twin-Field quantum key distribution. In *International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 265-267). Jeju Island, Korea. doi: 10.1109/ICTC52510.2021.9620743.

Sun, M.-S., Zhang, C.-H., Ma, X., Zhou, X.-Y., & Wang, Q. (2022). Sending-or-not-sending Twin-Field quantum key distribution with measurement imperfections. *IEEE Communications Letters,* 26(9), Sept., 2004-2008. doi: 10.1109/LCOMM.2022.3181984.

Wang, S., Yang, H., Qin, Y., Peng, D., & Fu, S. (2022). Power-over-fiber in support of 5G NR fronthaul: Space division multiplexing versus wavelength division multiplexing. *Journal of Lightwave Technology*, 40(13), 1, July 1, 4169-4177. doi: 10.1109/JLT.2022.3159540.

Wengerowsky, S., Joshi, S.K., Steinlechner, F., Hübel, H., & Ursin, R. (2019). An entanglement-based wavelength multiplexed quantum communication network. In *Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC)* (pp. 1-1). Munich, Germany. doi: 10.1109/CLEOE-EQEC.2019.8872932.

Woo, M.K. et al. (2020). One to many QKD network system using polarization-wavelength division multiplexing. *IEEE Access,* 8, 194007-194014. doi: 10.1109/ACCESS.2020.3032992.

Yousefi, M. & Yangzhang, X. (2020). Linear and nonlinear frequency-division multiplexing. *IEEE Transactions on Information Theory*, 66(1), Jan., 478-495. doi: 10.1109/TIT.2019.2941479.

Zhao, Y. & Qiao, C. (2023). Distributed transport protocols for quantum data networks. *IEEE/ACM Transactions on Networking*. doi: 10.1109/TNET.2023.3262547.

DOI: 10.24025/2306-4412.3.2023.288020

ISSN 2306-4412 (Print), ISSN 2306-4455 (CD-ROM), ISSN 2708-6070 (Online)

БАЗОВИЙ ПРОТОКОЛ РОЗПОДІЛУ КВАНТОВОГО КЛЮЧА

С. А. Дорожинський
Асистент кафедри комп'ютерних інформаційних технологій
факультету комп'ютерних наук та технологій НАУ,
молодший науковий співробітник НДЛ протидії кіберзагрозам в авіаційній галузі,
Національний авіаційний інститут, м. Київ, Україна
https://orcid.org/0000-0002-5395-6423, e-mail: dorozhynskyi.serhii@npp.nau.edu.ua

Анотація. З плином часу зростає комплексність загроз, які можуть здійснюватись проти критичної інфраструктури, включаючи кібератаки, великомасштабні відмови, терористичні акти тощо. Конфіденційність даних, які обробляються і передаються в межах критичної інфраструктури, є основним аспектом її безпеки. Традиційні методи криптографії, хоча й надійні, стають уразливими перед сучасними обчислювальними та квантовими здатностями атакуючих. Через це актуальність вивчення та застосування квантової криптографії в критичній інфраструктурі набуває все більшого значення. Вони мають високу стійкість до атак, пов'язаних з обчислювальними аспектами, і забезпечують невідслідковуваність ключів і даних завдяки принципам невизначеності. Однак вони також вимагають складної технічної реалізації та подальшого дослідження для широкого впровадження. Квантова криптографія може забезпечити надійний захист від сучасних та майбутніх атак, зберігаючи конфіденційність даних та ідентифікацію користувачів. Проте важливо правильно підібрати методи та засоби для забезпечення максимального рівня конфіденційності даних, зважаючи на особливості мережі.
У статті детально описано процеси вдосконалення протоколу квантового розподілу ключів за допомогою методів квантової ідентифікації та мультиплексування квантових каналів, описано математичний апарат вдосконаленого методу та визначено етапи формування стеку протоколу розподілу ключів. Запропонований вдосконалений метод квантового розподілу ключів формує можливість універсального його застосування в умовах невизначеності, забезпечуючи швидкодію виконання операцій та більший рівень захищеності даних.

Ключові слова: протокол Twin Field, мультиплексування квантового каналу, квантова ідентифікація, квантові канали, квантова криптографія, стек протоколу розподілу ключів.

Дата надходження: 25.08.2023
Прийнято: 15.09.2023

DOI: 10.24025/2306-4412.3.2023.288020