UDC 004
https://doi.org/10.31891/csit-2023-1-8

Tetiana OKHRIMENKO, Serhii DOROZHYNSKYI, Bohdan HORBAKHA
National aviation university, Kyiv, Ukraine

ANALYSIS OF QUANTUM SECURE DIRECT COMMUNICATION PROTOCOLS

The development of modern computer technologies endangers the confidentiality of information, which is usually ensured by traditional cryptographic means. This circumstance forces us to look for new methods of protection. In view of modern trends, quantum cryptography methods can become such alternatives, which allow solving a number of important cryptographic problems, for which the impossibility of solving using only classical (that is, non-quantum) communication has been proven. Quantum cryptography is a branch of quantum informatics that studies methods of protecting information by using quantum carriers. The possibility of such protection is ensured by the fundamental laws of quantum mechanics. One of the promising directions of quantum cryptography is Quantum Secure Direct Communication (QSDC) that offers secure communication without any shared key. A characteristic feature of this method is the absence of cryptographic transformations, accordingly, there is no key distribution problem. The purpose of this work is a general overview of quantum cryptography protocols, finding their weak points for further development and improvement, as well as identifying vulnerabilities to different attacks.

The article analyzes new methods and protocols, as well as presents their advantages and disadvantages. Based on partial generalizations of theoretical provisions and practical achievements in the field of quantum cryptography, a generalized classification was developed. By comparing various factors of the protocols, and their resistance to certain cyberattacks, we have the opportunity to identify several problems in this field and expand the possibilities for choosing appropriate methods for building modern quantum information protection systems. In accordance with this, conclusions were presented regarding the use of protocols and increasing the level of their effectiveness.

Keywords: quantum cryptography, classification, quantum direct secure communication, quantum key distribution.

Тетяна ОХРІМЕНКО, Сергій ДОРОЖИНСЬКИЙ, Богдан ГОРБАХА
Національний авіаційний університет, Київ, Україна

АНАЛІЗ ПРОТОКОЛІВ КВАНТОВОГО ПРЯМОГО БЕЗПЕЧНОГО ЗВ'ЯЗКУ

Розвиток сучасних обчислювальних технологій ставить під загрозу конфіденційність інформації, що майже завжди забезпечується традиційними криптографічними засобами. Ця обставина змушує шукати нові методи захисту. З огляду на сучасні тенденції, такими альтернативами можуть стати методи квантової криптографії, що дозволяють вирішити немало складних завдань, які неможливо виконати за неквантового обміну інформацією. Квантова криптографія - розділ квантової інформатики, що вивчає методи захисту інформації за допомогою квантових носіїв. Можливість такого захисту забезпечується фундаментальними законами квантової механіки. Одним з перспективних напрямків квантової криптографії є квантовий захищений прямий зв'язок (Quantum Secure Direct Communication, QSDC), який забезпечує безпечний зв'язок без спільного ключа. Характерною особливістю цього методу є відсутність криптографічних перетворень, відповідно, відсутня проблема розподілу ключів. Метою даної роботи є загальний огляд протоколів квантової криптографії, пошук їх слабких місць для подальшого розвитку та вдосконалення, а також виявлення вразливостей до різних атак.

У статті проведено аналіз нових методів та протоколів, а також представлено їх переваги та недоліки. На основі часткових узагальнень теоретичних положень та практичних досягнень у галузі квантової криптографії було розроблено узагальнену класифікацію. Порівнюючи різні фактори протоколів та їх стійкість до певних кібератак, ми маємо можливість виявити ряд проблем у цій галузі та розширити можливості вибору відповідних методів для побудови сучасних систем квантового захисту інформації. У відповідності до цього, представлено висновки щодо використання протоколів та підвищення рівня їх ефективності.

Ключові слова: квантова криптографія, класифікація, квантовий прямий безпечний зв'язок, квантовий розподіл ключів.

Introduction

Quantum cryptography is a branch of quantum informatics that studies methods of protecting information by using quantum carriers. The possibility of such protection is ensured by the fundamental laws of quantum mechanics. One of the promising directions of quantum cryptography is Quantum Secure Direct Communication (QSDC) that offers secure communication without any shared key. A characteristic feature of this method is the absence of cryptographic transformations, accordingly, there is no key distribution problem.

Types of QSDC protocols [1]: 1) Ping-Pong (PP) protocol (various variants) also known as deterministic protocol, 2) protocols with block transmission of entangled qubits, 3) protocols with single qubits, and 4) protocols with groups of entangled qubits. Most of the QSDC protocols proposed so far require the transfer of qubits in blocks. This makes it possible to detect the eavesdropping of the quantum channel before the transmission of the message itself and in this way guarantee the security of the transmission – if the eavesdropping is detected before the transmission of the message, then the legitimate parties interrupt the session and no information is leaked to the attacker. However, to store such blocks of qubits, a large quantum memory is required. Quantum memory technology is actively being developed, but it is still far from mass application in standard telecommunications equipment. Therefore, from the point of view of technical implementation, protocols in which transmission is carried out by single qubits or small groups of them (per one cycle of the protocol) are preferred. Few such protocols have been proposed, and they have only asymptotic security, that is, the attack will be detected with a high probability, but before that, the attacker will be able to receive some part of the message. Accordingly, there is a problem in strengthening the security of such protocols, that is, creating such methods of preprocessing the transmitted information that will make the information intercepted by the attacker useless for him.

The **purpose of this work** is a general overview of quantum cryptography protocols, finding their weak points for further development and improvement, as well as identifying vulnerabilities to different attacks.

Main part

In QSDC protocols, Alice encodes a secret message consisting of several qubits using a pre-selected encoding rule and sends them to Bob [2]. After some security checks, the recipient can accept the secret message. If the protocol is designed incorrectly, it can give Eve a chance to impersonate a legitimate party. To avoid this, legitimate parties must verify the legitimacy of other parties, which is required by quantum authentication protocols.

In 2006 was introduced first QSDC protocol with authentication, and many researchers have worked in this field since then. Several quantum cryptography protocols have been proven to be invulnerable to various common attacks such as intercept and replay attacks, impersonation attacks, denial of service attacks, man-in-the-middle attacks, Trojan horse attacks, etc. These are active attacks, meaning an interceptor can access the qubits being transmitted in the quantum channel between legitimate parties and actively participate in the protocol. Some passive attacks can also cause information leakage problems in communication protocols.

In 2020, the QSDC protocol, which works on the principle of combining a single photon and a pair EPR was introduced and mutual authentication was achieved. For simplicity, it is called the YZCSS protocol (Yan, Zhang, Chang, Sun, Sheng protocol) [3]. In this protocol, Alice, the sender of the message, prepares pairs of qubits corresponding to the secret message and its authentication identifier. She sends all the qubits to Bob, the recipient of the message, and Bob uses its authentication keys to recover the secret data. However, the YZCSS protocol is not immune to interception and retransmission attacks and impersonation attacks. If an eavesdropper uses any of these attacks, he can obtain the entire secret message, which means that not only part of the message has been leaked, but the entire message has been leaked. Furthermore, with impersonation attacks, legitimate parties cannot detect the presence of eavesdroppers. Therefore, it is necessary to modify the YZCSS protocol to improve its security.

YZCSS (Yan, Zhang, Chang, Sun, Sheng) protocol

In the YZCSS protocol [3], which has two sides Alice and Bob with their identificators ID_A and ID_B accordingly, where ID_A, $ID_B \in \{0, 1\}^N$. Alice sends a message $M \in \{0, 1\}^N$. Then Bob applies individual photons and Bell states, which are defined by the formulas:

$$|\phi \pm\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle\, or \,|\phi^-\rangle\right),$$

$$|\varphi \pm\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right).$$

The stages of the protocol are as follows:

First stage. Alice and Bob have common identifiers ID_A and ID_B, use some QKD to exchange data. Alice begins the process of preparing two packets of data in two-qubit states S_M and S_A, according to M message and her own identification ID_A, each ordered set contains pairs of N qubits. For $1 \leq i \leq N$ let the i-th bit M (either ID_A or ID_B) will be M_i (either $ID_{A,i}$ or $ID_{B,i}$) and the i-th qubit S_M (або S_A) will be $S_{M,i}$ (or $S_{A,i}$). She prepares qubits using the following rule: (a) if M_i (or $ID_{A,i}$) = 0, so that $S_{M,i}$ (or $S_{A,i}$) = |01| or |10| with equal probability, (b) if M_i (or $ID_{A,i}$) = 1, so that $S_{M,i}$ (or $S_{A,i)}$ = $|\Phi^+|$ or $|\Phi^-|$ with equal probability.

Pairs of qubits of an ordered set S_A are called decoy states. Alice now inserts these state decoys into an ordered set S_M according to such a directive: (a) if $ID_{B,i} = 0$, then she inserts $S_{A,i}$ before $S_{M,i}$ and (b) if $ID_{B,i} = 1$, then she inserts $S_{A,i}$ after $S_{M,i}$.

Let the newly ordered set be S containing 2N pairs of qubits. Alice addresses S to Bob using a quantum communication channel. Consider an example:

Sample 1. Let's suppose that, M=10110, ID_A=01101 and ID_B=01001. Then

$$S_M=\left\{|\phi^+\rangle,|01\rangle,|\phi^+\rangle|\phi^-\rangle,|01\rangle\right\},\ S_A=\left\{|10\rangle,|\phi^-\rangle,|\phi^-\rangle,|01\rangle,|\phi^+\rangle\right\} \text{ and}$$

$$S=\left\{|10\rangle,|\phi^+\rangle,|01\rangle,|\phi^-\rangle|\phi^-\rangle,|\phi^+\rangle,|01\rangle,|\phi^-\rangle,|01\rangle,|\phi^+\rangle\right\}.$$

Second stage. After Bob receives S, he knows the basis of the two photons corresponding to his ID. ID_B. Bob measures these decoy photons in the correct bases. If $ID_{A,i} = 0$, he chooses the basis Z × Z, where Z = {|0i, |1i}, so that Z × Z = {|00i, |01i, |10i, |11i}, and if $ID_{A,i} = 1$, then he chooses the Bell basis = $\{|\Phi^+|, |\Phi^-|, |\Psi^+|, |\Psi^-|\}$ for measuring $S_{A,i}$. Bob also randomly measures pairs of qubits S_M in the basis Z × Z or in the Bell basis. After that, he notes the results of the measurements.

Third stage. Bob asks Alice to declare the starting states of the S_A qubit pairs for a security check. They compare the initial states and the decoy photon measurements and calculate the number of errors. If the number of errors is greater than the seventh predefined threshold, they stop the protocol, otherwise, they continue.

Fourth stage. Bob obtains all the bits of the secret message by calculating pairs of qubits S_M. The relationship between the measurement results and the bits of the secret message is shown in Table 1. Alice and Bob open seven parts of the received data to verify the integrity of the message.

The IZCSS protocol is robust against impersonation, interception, and retransmission attacks, man-in-the-middle attacks, etc. However, an eavesdropper can develop a strategy that allows him to perform an intercept and resend attack effectively.

Table 1.

Different cases of decoding the YZCSS protocol

Bits of Alice's secret message M_i	Encoded qubits $S_{m,i}$	Bases selected by Bob	Bob's measurement results	Decoded secret bits
0	$\|01\rangle$	bases $Z \times Z$	$\|01\rangle$	0
		Bell bases	$\|\psi^+\rangle or \|\psi^-\rangle$	0
	$\|10\rangle$	bases $Z \times Z$	$\|10\rangle$	0
		Bell bases	$\|\psi^+\rangle or \|\psi^-\rangle$	0
1	$\|\phi^+\rangle$	bases $Z \times Z$	$\|00\rangle or \|11\rangle$	1
		Bell bases	$\|\phi^+\rangle$	1
	$\|\phi^-\rangle$	bases $Z \times Z$	$\|00\rangle or \|11\rangle$	1
		Bell bases	$\|\phi^-\rangle$	1

Protocols using GHZ-like states

Recently, two very interesting DSQC protocols [4] based on particle reordering have been proposed. Yuan's protocol uses a four-qubit symmetric W state for communication, while Tsai's protocol uses dense coding of four-qubit cluster states. Current work is aimed at increasing the qubit efficiency of existing DSQC protocols and exploring the possibility of developing DSQC and QSDC protocols using GHZ-like and other quantum states.

GHZ-like states can be described generally as

$$\frac{\left(|\psi_i\rangle|0\rangle+|\psi_j\rangle|1\rangle\right)}{\sqrt{2}},$$

where $i, j \in \{0, 1, 2, 3\}$, $i \neq j$, also $|\psi_i|$ and $|\psi j|$ — Bell states, which are usually denoted as

$$|\psi_0\rangle = |\psi_{00}\rangle = |\psi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}},\ |\psi_1\rangle = |\psi_{01}\rangle = |\psi^+\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}},$$

$$|\psi_2\rangle = |\psi_{10}\rangle = |\psi^-\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}},\ |\psi_2\rangle = |\psi_{11}\rangle = |\psi^-\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}.$$

GHZ-like states are useful for controlled quantum teleportation. It is also possible to form an orthonormal basis set in 2^3 3-dimensional Hilbert spaces of 8 states that can be used for dense coding and DSQC. Thus, states are created as a useful resource for quantum information processing.

DSQC using GHZ-like states without using dense coding

Assume that Alice and Bob are two remote or spatially separated legitimate/authenticated communicators. Alice wants to give Bob a secret classic message. The proposed protocol [5] can be implemented using the following steps:

1. It can be assumed that Alice prepared n-copies of the GHZ-like state

$$|\lambda\rangle = \frac{|\phi^+0\rangle+|\phi^+1\rangle}{\sqrt{2}} = \frac{1}{2}\left(|010\rangle+|100\rangle+|001\rangle+|111\rangle\right).$$

Alice now prepares a sequence P of n-ordered triplets of entangled particles as P = {p_1, p_2......., p_n}, where index 1, 2, ..., n denotes the triplet order of particles p_i = {h_1, t_1, t_2}, which is in a state |λ|. Symbols h and t are used to denote the home photon (h) and the companion photon (t), respectively.

2. Alice encodes her secret message in the sequence P by applying one of four two-qubit unitary operations $\{U_{00} = X \otimes I,\ U_{01} = I \otimes I,\ U_{10} = I \otimes Z,\ U_{11} = I \otimes iY\}$ into particles (h_1, t_1) of each triplet. Unitary operations $\{U_{00}, U_{01}, U_{10}, U_{11}\}$ encodes a secret message {00, 01, 10, 11} respectively. Here [5]

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|,$$

$$X = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|,$$

$$iY = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|,$$

$$Z = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

These operations U_{ij} (i, j∈{0, 1}) will transform a GHZ-like state $|\lambda|$ into another GHZ-like state $|\lambda_{ij}|$, where

$$|\lambda_{00}\rangle = U_{00}|\lambda\rangle = \frac{1}{2} X \otimes I\left(|010\rangle + |100\rangle + |001\rangle + |111\rangle\right) =$$

$$\frac{1}{2}\left(|010\rangle + |000\rangle + |101\rangle + |011\rangle\right) = \frac{|0\psi^{+}\rangle + |1\phi^{+}\rangle}{\sqrt{2}}.$$

$$|\lambda_{01}\rangle = U_{01}|\lambda\rangle = \frac{1}{2} I \otimes I\left(|010\rangle + |100\rangle + |001\rangle + |111\rangle\right) =$$

$$\frac{1}{2}\left(|010\rangle + |100\rangle + |001\rangle + |111\rangle\right) = \frac{|0\phi^{+}\rangle + |1\psi^{+}\rangle}{\sqrt{2}}.$$

$$|\lambda_{10}\rangle = U_{10}|\lambda\rangle = \frac{1}{2} I \otimes Z\left(|010\rangle + |100\rangle + |001\rangle + |111\rangle\right) =$$

$$\frac{1}{2}\left(-|010\rangle + |100\rangle + |001\rangle - |111\rangle\right) = \frac{|0\phi^{-}\rangle + |1\psi^{-}\rangle}{\sqrt{2}}.$$

$$|\lambda_{11}\rangle = U_{11}|\lambda\rangle = \frac{1}{2} I \otimes iY\left(|010\rangle + |100\rangle + |001\rangle + |111\rangle\right) =$$

$$\frac{1}{2}\left(-|000\rangle + |110\rangle + |011\rangle - |101\rangle\right) = \frac{\left(|0\psi^{-}\rangle + |1\phi^{-}\rangle\right)}{\sqrt{2}}.$$

3. Alice stores the home photon (h1) of each triplet and prepares an ordered sequence, $P_A = [p_1(h_1), p_2(h_1), ..., p_n(h_1)]$. Similarly, it uses all traveling photons to prepare an ordered sequence $P_B = [p_1(t_1, t_2), p_2(t_1, t_2), ..., p_n(t_1, t_2)]$.

4. Alice disrupts the order of a pair of traveling photons in P_B and creates a new sequence $P'_B = [p'_1(t_1, t_2), p'_2(t_1, t_2), ..., p'_n(t_1, t_2)]$. The actual order is known only to Alice.

5. To prevent eavesdropping, Alice prepares m = 2n decoy photons. Decoy photons are randomly prepared in one of four states {|0|, |1|, |+|, |–|}, where |+|=|0|+|1|/√2 and |–| =|0|–|1/|√2, that is, the state of decoy photons $\otimes_{j=1}^{m}|P_j|$, $|P_j|$∈{|0|, |1|, |+|, |–|}, (j = 1, 2, ..., m). Alice then randomly inserts these decoy photons into the sequence P'_B and creates a new sequence P'_{B+m}, which she hands to Bob, P_A stays with Alice.

6. After confirming that Bob has received the entire sequence P'_{B+m}, Alice announces the positions of decoy photons. Bob measures the corresponding particles in sequence P'_{B+m} using base X or Z randomly, where X = {|+|, |–|} and Z = {|0|, |1|}. After the measurement, Bob publicly announces his result and the basis used for the measurement. Alice now has to reject 50% of the times Bob chose the wrong basis. From the remaining results, Alice can calculate the error rate and check whether it exceeds a predefined threshold or not. If it exceeds the threshold, Alice and Bob stop this communication and repeat the procedure from the beginning. Otherwise, they proceed to the next step.

7. Knowing the position of the decoy photons, Bob already had the sequence P'_B, Alice reveals the actual order of the sequence, and Bob uses this information to transform the reordered sequence P'_B to the original sequence P_B. Therefore, Alice needs to exchange 2n classical bits.

8. Alice measures photons on a computational basis (Z basis) and announces the result. Bob measures the received qubits in the Bell base. Knowing the results of Alice's measurements and his measurements, Bob can easily decode the encoded information. For clarity, in Table 1, we have provided the relationship between measurement results and secret messages.

Table 2.

Relationship between measurement results and secret message in DSQC using GHZ-like states without full use of dense coding

Alice's measurement result	Bob's measurement result	Decoded secret
0	ϕ^{+}	01
	ϕ^{-}	10
	ψ^{+}	00
	ψ^{-}	11
1	ϕ^{+}	00
	ϕ^{-}	11
	ψ^{+}	01
	ψ^{-}	10

A similar DSQC protocol based on particle rearrangement was recently proposed by Yuan and the others [6]. In their work, they used a four-qubit symmetric state W to securely transmit 2 bits of classical information. They compared their protocol with the previous DSQC protocol proposed by Cao and Song. Their protocol also uses 4-qubit W-states for DSQC, but each of these W-states can only be used to transmit one bit of classical information. With this in mind, Yuan et al claim that their protocol has high throughput because each W state can transport two bits of information that is secret[7]. The advantage is that the encoding is performed by performing a single operation on two qubits (photons), but only one of them is stored as the master photon. The same conclusion requires the GHZ state and any other significantly densely encoded tripartite state.

Summarizing, it is possible to demonstrate weak positions for each of the mentioned protocols, as well as to show which cyber-attacks they are resistant to.

Table 3.

Presentation of the resistance of protocols to different types of cyber-attacks, where "+" means resistance, and "-" indicates vulnerability to such attacks

QSDC Protocols	**The main types of cyber attacks**								
	C	**NC**	**MiM**	**DoS**	**TC**	**FS**	**PBS**	**PNS**	**TH**
Ping-Pong, DLL, PP^{GV}	+	–	–	–	+	+	+	+	–
Entangled qubits in groups	+	+	–	–	+	+	+	+	–
With groups of confused qudites	+	+	–	–	+	+	+	+	–
With single qubits	+	+	–	–	+	+	+	+	–
YZCSS	+	+	–	–	+	+	+	+	–
using GHZ-like states	+	+	–	–	+	+	+	+	–
using GHZ-like states without using dense coding	+	+	–	–	+	+	+	+	–

Conclusions

Thus, this paper analyzes modern protocols of quantum cryptography (identifies their advantages and disadvantages), and their existing classifications. Based on partial generalizations of theoretical provisions and practical achievements in the field of quantum cryptography, a generalized classification was developed. By comparing various factors of the protocols, and their resistance to certain cyberattacks, we have the opportunity to identify several problems in this field and expand the possibilities for choosing appropriate methods for building modern quantum information protection systems.

References

1. Zhmurko T., Kinzeryavyy V., Yubuzova Kh., Stojanovic A.: Generalized classification of modern quantum cryptography and communication methods. Ukrainian Scientific Journal of Information Security, 2015, vol. 22, issue 3, p. 287-293.
2. Banerjee A., Pathak A.: Efficient protocols for deterministic secure quantum communication using GHZ-like states. Quantum Physics, 2018.
3. Yan L., Zhang S., Chang Y., Sun Z., Sheng Z.: Quantum secure direct communication protocol with mutual authentication based on single photons and Bell states. Computers, Materials & Continua, 63(3):1297–1307, 2020.
4. Banu N., Ghosal P, Panigrahi P. K.: "Quantum information splitting of an unknown two qubit state by using two three qubit GHZ like states," 2014 International Conference on Electronics and Communication Systems (ICECS), 2014, pp. 1-4, doi: 10.1109/ECS.2014.6892773.
5. Guo W., Hou X.: An Efficient Controlled Quantum Secure Direct Communication Protocol via GHZ-like States. 2019 IEEE 5th International Conference on Computer and Communications (ICCC), 2019, pp. 821-825, doi: 10.1109/ICCC47050.2019.9064457.
6. Shukla Ch., Banerjee A., Pathak A.: Improved Protocols of Secure Quantum Communication Using W States. International Journal of Theoretical Physics, 2018, vol. 52, pp. 1914–1924.
7. Yuan, H., Song, J., Zhou, J. et al. High-capacity Deterministic Secure Four-qubit W State Protocol for Quantum Communication Based on Order Rearrangement of Particle Pairs. Int J Theor Phys 50, 2403–2409 (2011). https://doi.org/10.1007/s10773-011-0729-7

Tetiana Okhrimenko **Тетяна Охріменко**	PhD, Senior Research Fellow, Research Laboratory of Cyber Threats Counteraction in Aviation, National Aviation University, Kyiv, Ukraine, e-mail: t.okhrimenko@npp.nau.edua.ua https://orcid.org/0000-0001-9036-6556	к.т.н., страший науковий співробітник науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі, Національний авіаційний університет, Київ, Україна
Serhii Dorozhynskyi **Сергій Дорожинський**	PhD-student, assistant of the department of telecommunications and radioelectronic systems, young scientist of scientific research department, National Aviation University, Kyiv, Ukraine, e-mail: dorozhun1706@gmail.com. https://orcid.org/0000-0002-5395-6423	PhD-аспірант, асистент кафедри телекомунікацій та радіоелектронних систем, молодший науковий співробітник науково-дослідної частини, Національний авіаційний університет, Київ, Україна
Bohdan Horbakha **Богдан Горбаха**	Graduate student, Laboratory assistant of scientific research department, National Aviation University, Kyiv, Ukraine e-mail: 4591078@stud.nau.edu.ua, https://orcid.org/0000-0003-0713-4426	студент магістратури, Лаборант науково-дослідної частини, Національний Авіаційний Університет, Київ, Україна