

REPUBLIC OF TURKEY

AKDENİZ UNIVERSITY



**ON THE USE OF QUANTUM CRYPTOGRAPHY IN FINANCIAL IT
SYSTEMS**

Sevil TEİFUROVA

INSTITUTE OF NATURAL AND APPLIED SCIENCES

DEPARTMENT OF COMPUTER ENGINEERING

MASTER THESIS

JUNE 2021

ANTALYA

REPUBLIC OF TURKEY

AKDENİZ UNIVERSITY



**ON THE USE OF QUANTUM CRYPTOGRAPHY IN FINANCIAL IT
SYSTEMS**

Sevil TEİFUROVA

INSTITUTE OF NATURAL AND APPLIED SCIENCES

DEPARTMENT OF COMPUTER ENGINEERING

MASTER THESIS

JUNE 2021

ANTALYA

REPUBLIC OF TURKEY
AKDENİZ UNIVERSITY
INSTITUTE OF NATURAL AND APPLIED SCIENCES

**ON THE USE OF QUANTUM CRYPTOGRAPHY IN FINANCIAL IT
SYSTEMS**



Sevil TEİFÜROVA

DEPARTMENT OF COMPUTER ENGINEERING

MASTER THESIS

This thesis unanimously accepted by the jury on 24/06/2021

Asst. Prof. Dr. Murat AK (Supervisor)

Prof. Dr. Cafer ÇALIŞKAN

Asst. Prof. Dr. Hüseyin Gökhan AKÇAY

ÖZET

KUANTUM KRİPTOGRAFİNİN FİNANSAL BİLGİSAYAR SİSTEMLERİNDE KULLANIMI ÜZERİNE

Sevil TEİFUROVA

Yüksek Lisans Tezi, Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Murat AK

Haziran 2021; 102 sayfa

Günümüzde veri kullanımının artmasıyla yüksek korumalı daha gelişmiş iletişim kanalları gerekmektedir. En güvenilir yazılımda bile güvenlik açıkları mevcutken biz bilginin güvenilir bir şekilde korunmasını nasıl sağlayabiliriz? Şimdilik klasik kriptografi sayesinde bu görevlerin oldukça başarılı bir şekilde yerine getirildiğini söyleyebiliriz. Günümüzde klasik kriptografiye yönelik en önemli tehdit hesaplamada kullanılan kuantum mekaniği ilkeleridir. Birçok uzmana göre, teknolojinin şu anki aşamasında kuantum kriptografi yardımı ile bilgileri güvenilir bir şekilde korumak mümkündür. Kuantum biliminin deneysel olarak en gelişmiş alanı kuantum kriptografidir. Kuantum kriptografi, kuantum mekaniğinin temel ilkelerine dayanarak bilgi güvenliğini sağlamaktadır.

Teknolojinin aktif gelişimi yaşamın her alanına yayılıyor. Dünya’da modern bilgi teknolojilerinin finansal sistemdeki rolü sürekli artmaktadır bu nedenle bu tür sistemlerin güvenliği büyük önem arz etmektedir. Bugün finansal teknoloji pazarı çok aktif bir şekilde büyümektedir. Finansal bilgi teknolojilerindeki karmaşıklığın artması, bilişim sistemlerinde oluşabilecek güvenlik risk faktörlerinde önemli bir artışa yol açmaktadır.

Bu çalışmada, bugüne kadar geliştirilmiş olan kuantum bilgi yöntemlerinin kısa bir özetini ve analizini sunmaktayız. Burada finansal sistemlerin bilgi güvenliğinde kuantum teknolojilerinin kullanımını analiz ediyoruz. Kuantum kriptografisinin en iyi bilinen yapı taşlarını ve protokollerini inceliyoruz. Ticari olarak temin edilebilen kuantum anahtar dağıtım sistemleri ile teorik ve laboratuvar araştırması aşamasında olan çalışmaları tanımlıyoruz. Kuantum ve klasik kriptosistemlerinin özelliklerini karşılaştırıyoruz ve buna dayanarak avantajlarını ve dezavantajlarını araştırıyoruz. Benzer şekilde, kuantum kriptografi çerçevesinde veriyi korumaya yönelik bazı yaklaşımları inceliyoruz. Son

olarak finansal sistemlerde ortaya çıkan kriptografik problemleri ve literatürde bu problemler için önerilen bazı çözümleri derliyoruz.

ANAHTAR KELİMELEER: Finansal Sistemler, Kuantum Algoritması, Kuantum Anahtar Dağıtımı, Kuantum Kriptografi, Post-kuantum Kriptografi

JÜRİ: Dr. Öğr. Üyesi Murat AK

Prof. Dr. Cafer ÇALIŞKAN

Dr. Öğr. Üyesi Hüseyin Gökhan AKÇAY



ABSTRACT

ON THE USE OF QUANTUM CRYPTOGRAPHY IN FINANCIAL IT SYSTEMS

Sevil TEIFUROVA

MSc Thesis in Computer Engineering

Supervisor: Asst. Prof. Dr. Murat AK

June 2021; 102 pages

Nowadays, with the increase of data usage, more advanced communication channels with high protection are required. How can we ensure that information is reliably protected when even the most reliable software has security vulnerabilities? For now, we can estimate that these tasks have been accomplished, thanks to classical cryptography. Today, the most critical threat to classical cryptography is the principles of quantum mechanics used in computing. According to many experts, it is possible to reliably protect information with quantum cryptography at the present stage of technology. The most experimentally advanced area of quantum science is quantum cryptography. Quantum cryptography provides information security based on the basic principles of quantum mechanics.

The active development of technology spreads to all areas of life. In the world, the role of modern information technologies in the financial system is constantly increasing, so the security of such systems is of great importance. Currently, the financial technology market is growing actively. Increasing complexity in financial information technologies leads to a significant increase in security risk factors that may occur in information systems.

In this paper, we present a summary and analysis of quantum information methods that have been developed to date. Here we analyze quantum technologies in the data security of financial systems. We examine the most well-known primitives and protocols of quantum cryptography. Also, we describe studies that are at the theoretical and laboratory research stage with commercially available QKD systems. We compare the features of quantum and classical cryptosystems and, based on this, explore their advantages and disadvantages. Correspondingly, we examine the approaches to data protection within the framework of quantum cryptography. Finally, we compile cryptographic issues arising in financial systems and the solutions suggested for these problems in the literature.

KEYWORDS: Financial Systems, Quantum Algorithm, Quantum Cryptography, Quantum Key Distribution, Post-quantum Cryptography

COMMITTEE: Asst. Prof. Dr. Murat AK

Prof. Dr. Cafer ÇALIŞKAN

Asst. Prof. Dr. Hüseyin Gökhan AKÇAY



ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Asst. Prof. Dr. Murat AK, who was always with me in this thesis preparation. I am extremely grateful for his unconditional support, guidance, and feedback throughout this thesis.

Further, I would like to express my respect and gratitude to all my esteemed professors, who have shed light on my path since my undergraduate education, who has always been an example of their personalities and professional achievements.

Finally, I would like to extend my endless thanks to my dear family and dear friends, who have always been with me in this very intense academic year, as in every step I have taken.



LIST OF CONTENTS

ÖZET	i
ABSTRACT	iii
ACKNOWLEDGEMENTS	v
TEXT OF OATH	ix
LIST OF ABBREVIATIONS	x
LIST OF FIGURES	xi
LIST OF TABLES	xii
1. INTRODUCTION	1
1.1. Objective of the Thesis	3
1.2. The Organization of the Thesis	4
2. LITERATURE REVIEW	6
2.1. Related Works	11
2.1.1. Use of quantum systems in finance	13
2.2. Introduction to Cryptography	14
2.2.1. Historical background	16
2.2.2. Modern cryptography	18
2.2.3. Encryption and decryption	19
2.2.4. Symmetric algorithms	19
2.2.4.1. Vernam cipher	20
2.2.4.2. Key distribution	21
2.2.5. Asymmetric algorithms	22
2.2.5.1. Diffie–Hellman key exchange	23
2.2.5.2. RSA algorithm	24
2.2.5.3. Hybrid systems	25
2.2.6. Digital signature	25
2.2.7. Other primitives and security requirements	26
2.3. Fundamentals of Quantum Computing and Communication	30
2.3.1. Quantum computer	30
2.3.2. Quantum states and qubits	33
2.3.2.1. The Bloch sphere	35
2.3.2.2. Quantum entanglement	36
2.3.2.3. Quantum superposition	37
2.3.3. Basic gates	38
2.3.3.1. Single qubit gates	39

2.3.3.2. Multiqubit gates	41
3. MATERIAL AND METHODS	44
3.1. Introduction to Quantum Cryptography	44
3.2. Idea of Quantum Cryptography	46
3.3. The Main Directions of Development of Quantum Cryptography	48
3.4. Quantum Protocols	49
3.4.1. QKD	49
3.4.2. Prepare and measure protocols	51
3.4.2.1. BB84 protocol	51
3.4.2.2. B92 protocol	54
3.4.2.3. SARG04 protocol	57
3.4.3. Entanglement based protocols	58
3.4.3.1. E91 protocol	58
3.4.4. Quantum teleportation	60
3.4.5. Superdense coding	62
3.5. Quantum Algorithms To Break Classical Cryptography	64
3.5.1. Shor's algorithm	66
3.5.2. Grover's algorithm	68
3.6. Post-quantum Cryptography	69
3.6.1. Lattice-based cryptography	71
3.6.2. Multidimensional quadratic systems	71
3.6.3. Electronic signatures on hash functions	71
3.6.4. Code-based cryptography	72
3.6.5. Isogeny of elliptic curves	73
4. RESULTS AND DISCUSSION	74
4.1. Computational Problems in Finance	74
4.1.1. Classical cryptography in financial systems	76
4.1.2. Threats to information security	79
4.1.2.1. Confidentiality threats	80
4.1.2.2. Integrity threats	80
4.1.2.3. Availability threats	81
4.1.3. Cryptographic protection problems of financial information	81
4.1.4. Classical cryptography problems	82
4.2. Solutions to Computational Problems in Finance	84
4.2.1. Problems of quantum cryptography	85

4.2.2. Vulnerabilities in quantum cryptography	87
4.2.3. Comparing quantum solutions to classical one	88
4.3. Practical Implementation of Quantum Cryptography	91
4.4. Future Works	94
5. CONCLUSION.	96
6. REFERENCES	97
CURRICULUM VITAE	



TEXT OF OATH

I declare that this study "On the Use of Quantum Cryptography in Financial IT Systems", which I present as master thesis, is in accordance with the academic rules and ethical conduct. I also declare that I cited and referenced all material and results that are not original to this work.

24/06/2021

Sevil TEIFUROVA



LIST OF ABBREVIATIONS

CNOT	: Controlled Not
DoS	: Denial-of-service
EDS	: Electronic Digital Signature
GSA	: Grover Search Algorithm
HFE	: Hidden Field Equations
IT	: Information Technology
LPA	: Leakage Power Analysis
MITM	: Man in the Middle
NIST	: The National Institute of Standards and Technology
PNS	: Photon Number Splitting
PRNG	: Pseudorandom Number Generator
QFT	: Quantum Fourier Transform
QKD	: Quantum Key Distribution
RSA	: Rivest–Shamir–Adleman
SIDH	: Supersingular Isogeny Diffie–Hellman

LIST OF FIGURES

Figure 2.1.	Symmetric-key Cryptosystem	20
Figure 2.2.	Public-key Cryptosystem	23
Figure 2.3.	Hybrid Cryptosystem	25
Figure 2.4.	Information Security	30
Figure 2.5.	Bloch Sphere	35
Figure 2.6.	Notations of Quantum Circuits Elements	39
Figure 3.7.	Photons generated by Alice	53
Figure 3.8.	Bob's chosen polarization methods	53
Figure 3.9.	Results of Bob's measurements	53
Figure 3.10.	Correct and incorrect types of measurements	53
Figure 3.11.	The resulting sequence	54
Figure 3.12.	Quantum Teleportation Circuit	61
Figure 3.13.	Quantum Fourier Transform	68
Figure 3.14.	Grover's Algorithm with 3 Qubits	69

LIST OF TABLES

Table 2.1.	One Qubit Gates	40
Table 2.2.	Multiqubit Gates.	41
Table 3.3.	The Polarization Basis	52
Table 3.4.	BB84 Protocol Example	54
Table 3.5.	B92 Protocol	56
Table 3.6.	Quantum Teleportation	60
Table 3.7.	Superdense Coding	64
Table 4.8.	QKD Advantages and Disadvantages	93



1. INTRODUCTION

The primary direction of the twenty-first century is that the widespread informatization and digitalization of all processes of social functioning. All data generated and stored by humans has been transferred to digital media, so the demand for paper media is declining every year. This fact forces technical and scientific establishments to develop new and improve old technologies to simplify and reduce the price of the informatization process of society. Like any information, digital information is also not protected from intruders. We can see it within the example of the worldwide Internet. The Internet has accumulated lots of unnecessary and inaccurate information, and access to the network is mostly anonymous and not secure. Hence, the event of recent technologies and results is aimed not only at digitalizing data but also at protecting it.

Today, in almost all areas of human activity, personal data is processed. When creating appropriate information systems for processing and storing personal data, we should always take measures to prevent threats from unauthorized access, as well as from specific influences on such information to destroy, distort, or block access to it. Using modern information technologies has brought us to such a level that with the issues of reliability and stability of their functioning, the ensuring problem of the data security circulating in it arises. In such conditions, information leakage, violation of its integrity, and data blocking occur in systems. Therefore, today the most important element of avoiding computer violations within the financial sector is the use of modern technical means of protecting data. In the sphere of protecting information from unauthorized access, a special place is covered with cryptographic protection.

Information security is one of the most important factors of national confidence, and its importance is increasing. Using foreign-made information security tools poses serious threats to countries and their citizens. These threats especially appear in information and communication technologies and when using the facilities of the global network of the Internet. Cryptographic methods play a specific role in an integrated approach to information security. However, quantum information processing technologies and quantum computing devices, which have been advertised in recent years, may change the current problems in cryptography. The number of both hypothetical and real threats to information security has increased many times. It is assumed that the emergence of a full-fledged

quantum computer will negate the possibility of ensuring information security by using asymmetric and symmetric cryptographic systems with a limited key length that is not theoretically well-established. This development can lead to a significant reduction in the cryptographic technology suitable for practical applications. Uncompromising reliability is preserved only by cryptographic technology, which implements theoretically stable cryptographic algorithms.

Quantum cryptography is a new scientific field that offers reliable ways to protect information. The quantum encryption protocols will ensure secure data transfer. The development of the basic ideas of quantum computer science, which emerged at the intersection of quantum mechanics and information theory, marked the beginning of research on the creation of quantum computers and quantum communication lines. One of the most experimentally developed field of quantum computer science is quantum cryptography. Quantum cryptography allows us to achieve a data transfer. As a physical information carrier, it uses the quantum states of individual particles. The fundamental principles of data protection in quantum communication lines are the impossibility of copying the state of a quantum object and the impossibility of obtaining any information about the quantum states of this object without disturbing them. Thus, the fundamental laws of quantum mechanics act as a guarantee of protecting the transmitted data. Many experts believe that quantum cryptography will be the only method that can protect information both now and in the future. The ideas and prospects of this research turned out to be so attractive that many research groups has begun working actively on the creation of devices. The problem of creating quantum communication systems is constantly becoming a more vibrant area of research.

The primary factor affecting the political and economic components of national security is information and information environment protection. That is why the issues of providing the security of information and telecommunication technologies and guaranteed data protection in computer networks of economically significant structures are becoming urgent. Many computers crimes have proved the need for reliable protection in the financial sector and government agencies. The number of unlawful acts committed by remote attacks using geographically distributed data transmission networks has significantly increased. Such offenses are dangerous in that there is no established practice of combating them today. Financial security is a condition for the existence and development of the

object of relations. Also, financial security is the process of object creation and maintenance. The commercial sector can meet the various needs of continuous development and work with minimal risk of disruption.

Quantum information theory combines the ideas of classical information theory and quantum physics. The most advanced research areas under this theory so far are quantum computing and quantum cryptography where researchers achieve significant theoretical results. New methods discovered in these fields lead to progress in quantum cryptography. Even today, the high-tech market presents devices that allow the implementation of quantum key distribution protocols in actual communications. It means that the idea of quantum information encompasses a specific application in information and communication technologies. Typical tasks of the quantum theory are the development and research of various algorithms for informatics. In terms of quantum cryptography, we are talking about such information processing algorithms that allow us to reduce the average reciprocal information between the sender and the recipient of the message, which is available to the eavesdropper. In the theory of quantum information, this value is called information leakage. We should note that quantum computers do not limit using these algorithms to their use in quantum cryptography protocols or information processing. In classical information theory, these algorithms are good for high-speed systems with feedback when building algorithms for information processing in communication systems and networks. However, the primary application field of these algorithms is the QKD protocols.

1.1. Objective of the Thesis

The objective of the thesis is to study cryptographic problems in the financial systems and to examine the effectiveness of cryptographic information protection in quantum cryptographic systems. The following tasks planned and solved to achieve this goal:

- Summarize the basics of quantum cryptography and describe the protocols for transmitting the information.
- Describing the idea of quantum cryptography.
- Consider solutions to problems in the financial sector using quantum cryptography.
- Conclude and discuss development trends.

- Comparing quantum and classical solutions to computational problems in finance.

1.2. The Organization of the Thesis

The second chapter comprises three sections and devotes itself to an introduction to the basic concepts and ideas of classical cryptography, quantum computing, and quantum communication. Section 2.1 examines some related works in the quantum cryptography. Section 2.2 summarizes the basic concepts of cryptography and discusses the historical development of cryptography. It is devoted to modern cryptography. The section considers technologies used for the transmission of classified information. Also, it forms two encryption technologies considered symmetric and asymmetric cryptosystems and the principles of studying their stability. We also mention the RSA algorithm as the most common public-key encryption algorithm and the possibility of its decryption using a quantum computer, which shows the fundamental unreliability of public-key encryption. Section 2.3 is concerned with the main quantum information theory concepts—the branch of science to which quantum cryptography owes its appearance. This section describes the concept of quantum states, their measurement, and quantum channels. Then, we review the most important principles of quantum information theory: the impossibility of cloning quantum states, the impossibility of reliably distinguishing non-orthogonal quantum states. Also, we introduce the concept of a quantum bit, superposition, and quantum entanglement. The Bloch sphere shows the difference between a qubit and a classical bit of information.

The third chapter of the thesis applied to quantum cryptography and its ideas. This chapter also describes quantum cryptography protocols and algorithms. Section 3.1 is assigned to a detailed description of the main resources of quantum mechanics, which are widely used for quantum cryptography construction. Section 3.2 focuses on the fundamental ideas of quantum cryptography. Section 3.3 discusses the major trends in the development of quantum cryptography. Section 3.4 gives the protocols for quantum cryptography. First, we describe the BB84 protocol, the first and most studied quantum key distribution protocol. We also discuss other quantum cryptography protocols below: B92, SARG04, which is more flexible than BB84. This section also covers the E91 protocol. This protocol is based on the impossibility of cloning and entanglement. Also, we gave an introduction to the theory of two related quantum protocols: the protocol of quantum

teleportation and the protocol of superdense coding. Section 3.5 covers quantum algorithms to break classical cryptography, such as Shor's algorithm and Grover's algorithm. Section 3.6 gives a brief information about post-quantum cryptography.

The fourth chapter divides into 4 sections. Section 4.1 discusses the classical cryptography in finance and the problems of cryptographic protection of banking information, also gives information about the main threats of information security. In this section, we describe the most common threat types, such as confidentiality threats, integrity threats, and availability threats. Section 4.2 discusses the problems and vulnerabilities of quantum cryptography, quantum solutions to computational problems in finance. Also in this section gives a comparison of quantum solutions with classical ones. Section 4.3 outlines the results of the thesis and discusses practical implementation of quantum cryptography and section 4.4 gives suggestions for future research directions.

2. LITERATURE REVIEW

A theory was suggested in 1926, stating that possible to protect the confidentiality of data transmission when using encryption with an one-time pad (Vernam). The disadvantage of this method is the need for a preliminary agreement on the key used. Applying the same key twice not allows for ensuring unconditional secrecy (Shannon 1949). Therefore, it is necessary to store large volumes of private keys on the sender and recipient sides and update them.

From a truly scientific point of view, Claude Shannon was the first to adopt cryptography. In his article (1949), he first planned the theoretical basis of cryptography and introduced many concepts. Without these concepts, today's information theory is unimaginable. One of the major achievements of Shannon is being an exhaustive study of absolutely the secrecy concept of systems. He proved the existence of strong, unbreakable ciphers and planned the conditions necessary for this. Also, Shannon described the fundamentals that strong ciphers must accommodate. He introduced the mixing concepts and scattering and aimed to build strong cryptographic systems from quite simple transformations.

In everyday cryptographic tasks, it is necessary to transfer encrypted messages between users in many parts of the planet. Under such conditions, a previous exchange of private keys is impossible. Public-key cryptography techniques are adapted to contain such problems. The idea of these methods is the use of one-way functions, which can be computed easily, whereas inverting them is computationally infeasible.

Currently, the most common algorithm for asymmetric encryption is RSA (Rivest et al. 1978). The RSA algorithm is based on the problem of factoring a large number into its two prime factors. The user with whom a secure connection is established calculates the product of two random primes (the private key), the result (the public key) is transmitted to the future sender of the message. The sender encrypts their message corresponding to the algorithm using the public key. After many years of research, it is assumed that no classical algorithm can solve this problem in polynomial time. Thus, the use of large enough primes makes the decryption process takes too long without the private keys.

However, Shor proposed in 1994 an algorithm which allows the decomposition of numbers into prime factors in polynomial time employing a quantum computer. Exper-

imental implementations of this algorithm (Shor 1994) are even at the stage of demonstrations. Thus, factorizations of the numbers 15 and 21 were experimentally done (Vandersypen et al. 2001; Martín-López et al. 2012). At the moment, the quantum computer is not yet developed but the development of the quantum computing industry shows that even today we need to think about the vulnerabilities of the RSA algorithm.

Information is the scientific and practical area concept that studies the transmission, processing, and storage of data. In addition to the well-known and widely used transmission methods, it can also be encrypted in the states of quantum systems, for example, in the polarization states of single photons and transmitted through the corresponding physical communication channel. It happens when distributing keys using quantum cryptography methods. The quantum state itself is a special information resource that contains information about the statistics of various measurements on a quantum system (Nielsen and Chuang). The information in the quantum state has qualitative differences from classical information, and therefore the term quantum information is used for it (Resch and Karpuzcu 2019; Nielsen and Chuang 2010). The most striking difference between quantum information and classical information is the impossibility of cloning an arbitrary unknown quantum state (Bužek and Hillery 1996; Holevo 2012). This fact is known as the no-cloning theorem.

Quantum computing could be a key focus of the second quantum revolution. Unlike the first quantum revolution (lasers and semiconductor technologies), the second quantum revolution will allow us to use the properties of individual particles rather than collective effects. The basis for the breakthrough was such pure quantum phenomena as entanglement (Gisin 2014), teleportation (Brassard et al. 1998), and no-cloning (Bužek and Hillery 1996).

A quantum computer is a computer which uses the laws of quantum physics. It differs from classical computers, which operate supported the laws of classical physics. Richard Feynman proposed one of the first models of a quantum computer in 1982. Feynman also noted that we cannot correctly calculate the quantum particle's behavior description on a classical computer. Quantum parallelism with the entanglement of states is the basis for the quantum computer's construction and quantum algorithms.

Quantum entanglement is one of the most profound and strange characteristic of quantum mechanics. It is a physical phenomenon in which the quantum states of several par-

ticles are interconnected regardless of the distance between them. This phenomenon is used in quantum teleportation, quantum cryptography, and computer technology. The term quantum entanglement was first introduced by Schrodinger in his work (1935), it was also considered in other researches (Bennett et al. 1996).

Currently, there are two of the best-known quantum methods to break classical cryptography. The first one is the Shor algorithm (1994), which is employed for fast factorization of large numbers, and the second one is the Grover algorithm (1996) for the faster search of the required element from an extensive set of unordered information. The possibility of building a quantum computer with the meaningful development of the quantum theory is related to the evolution of the many particles. Implementing new complex experiments described to the construction of quantum computer elements is additionally of interest. Therefore, the work on designing quantum computer elements, even at the abstract level, is one of the holy grails of modern physics.

As previously mentioned, the utilization of the OTP allows us to transmit data with absolutely proven secrecy. However, the major issue is the distribution of the private key between two remote users. It is the secret distribution of the private key with the help of quantum physics that has become the most direction of quantum cryptography. One foundation of the QKD is the no-cloning theorem (Bužek and Hillery 1996). In keeping with it, it is impossible to create an exact copy of an unknown quantum state.

Quantum cryptography, QKD refers to the problem of generating a secret key among two remote parties using quantum teleportation of qubits. The generated key is used for classical information protection. Cryptographic quantum protocols make it possible for remote users to distribute a secret random key using conventional communication channels (Wiesner 1983).

For the first time, Stephen Wiesner expressed the theory of quantum information security in 1970 in the conceptual framework of quantum money. This idea was not widely accepted, as was the primary and most well-known so far BB84 protocol developed by Charles Bennett and Gilles Brassard (1984). Cryptographic quantum protocols make it possible for remote users to distribute secret random keys among themselves through conventional communication channels (Wiesner 1983). There are many variations of quantum cryptography protocols. The most well-known protocol is a protocol with two sets of orthogonal states. Bennett and Brassard proposed this protocol in 1984. The operation of

this protocol is quite easy to clarify if we use the optical states of light. In this protocol, it transmits the secret code using single photons polarized in four directions. The laws of quantum physics forbid the simultaneous measurement of observables for a single photon in two orthogonal bases, which is the basic idea of the BB84 protocol. Measuring one observable associated with one set of basis states introduces an unavoidable imbalance in the statistics of states from another basis set.

The technology of quantum cryptography relies on the fundamental uncertainty of the behavior of a quantum system. It is unacceptable to get the particle coordinates and momentum simultaneously. It is impossible to measure one photon parameter without distorting the other. This fundamental property in physics is understood because of the Heisenberg uncertainty principle, formulated in 1927.

The main quantum resources used to build quantum cryptography systems are:

- No-cloning theorem (Wooters and Zurek 1982);
- Entanglement states of quantum systems (Schrödinger 1936);
- Quantum randomness (Gisin 2014).

Quantum cryptographic systems supported the resource of the impossibility of cloning an unknown quantum state include the cryptographic systems BB84 (Bennett and Brassard 1984), B92 (Bennett 1992), and their various modifications and generalizations, for instance, SARG04 (Scarani et al. 2004). An example of a quantum cryptographic system based on two quantum resources, the no-cloning, and entanglement, is E91 (Ekert 1991). It had been the first time that quantum entanglement was applied. Although this technique was harder to achieve, the paradigm of applying quantum entanglement formed the idea for proving the confidence of quantum cryptography.

Einstein, Podolsky, and Rosen challenged the fact that quantum mechanics is a complete theory. The quantum theory leads to a violation of the principle of local realism, which is natural from the classical point of view. This discussion went down in the history of physics under the name EPR paradox (Einstein et al. 1935). The American physicist Bell suggested a revision that can prove entangled states for violations of local reality by these states. The results of experimental tests confirmed that Einstein, Podolsky, and Rosen were wrong.

The idea of quantum teleportation and superdense coding protocols is closely associated with Charles Bennett. Currently, he is being one of the most famous co-authors of the primary works on quantum computer science and one founder of this scientific direction.

Quantum cryptography protocols allow two or more users to share a ciphertext between themselves in a way that is not possible in classical cryptography. Quantum teleportation and superdense coding protocols are fundamental and an integral part of quantum mechanics. These protocols do not work on classical objects since, in classical physics, there is no entanglement. Therefore, the practical implementation of protocols is an important task not only from a practical but also from a fundamental point of view to confirm the correctness of the use of the rules and concepts of quantum mechanics.

The non-local nature of quantum mechanics allows us to observe the effects of transferring quantum information, which entered science in the name of quantum teleportation (Bennett et al. 1993). In the quantum teleportation protocol, unknown quantum information destroys at the place where its sender performs some measurement and instantaneously appears at the recipient point, provided that the sender and the recipient initially established a quantum communication channel between them. Another idea of quantum computer science based on similar ideas is the superdense coding protocol (Bennett and Wiesner 1992). A superdense coding protocol may be of interest for more data transfer with the least amount of storage media.

These quantum protocols are based on the idea of quantum entangled states of two particles, each of which is considered in a two-dimensional Hilbert space. There are 4 such maximally entangled independent states, also known as Bell states (Nielsen and Chuang 2010). The Bell equations are given at 3.22, 3.23, 3.24, 3.25.

A qubit is a unit of quantum information. In more detail, a qubit is a fundamental concept in quantum computing and the quantum information field, having the meaning of a quantum information unit. This sense of the concept represents a qubit as a mathematical object.

Currently, there is a rapid development of quantum computer science, which results in the consideration of ideas of quantum networks, quantum games, and even the introduction of a high-level programming language for quantum computers. The performed studies have shown that most of the difficulties that experimenters face in technical implementations of long-lived entanglement quantum states are related to the need for a

technical solution to the decoherence elimination problem (Schlosshauer 2005). Decoherence is a physical treat in which there is a loss of coherence of the quantum state. Because of decoherence, the quantum state fails to be true. Quantum objects with many particles may have properties different from the classical ones, which may prove in their strange nature inconsistent with the admitted one. We know the decoherence effect is the serious obstacle to the creation of large quantum objects. The quantum decoherence quickly destroys the nascent quantum system of many particles, turning it into a classical object (Kiefer and Joos 1998). We can say that decoherence handles difference between quantum and classical items.

It is necessary to realize that there is data that requires to be kept secret for many years. Such data include, for example, state data, commercial data, military data, etc. An interceptor can record and store such information in encrypted form until a new classical algorithm or a powerful quantum computer appears. Therefore, it is necessary to consider these risks when sharing data that matters in the long term today. Also, do not forget that the conversion to new encryption standards can take many years.

One of the suggested solutions to the security issue is post-quantum cryptography (Bernstein 2009). The one-way functions in post-quantum cryptography used to generate keys are chosen to consider the remaining algorithms for a quantum computer. At the moment, post-quantum cryptography can be considered a reliable means of protection. However, there is no evidence that new quantum or classical algorithms will not be developed in the future that compromise post-quantum encryption.

It is assumed that in the future, post-quantum and quantum cryptography will exist in parallel. Post-quantum cryptography will keep information that makes sense in the short term. Quantum cryptography will be applied in those fields where the data sensitivity period is the longest.

2.1. Related Works

In recent years, research in quantum cryptography has moved from theoretical work to the practical implementation and first commercial prototypes. Shortly, technologies based on the quantum mechanics laws will allow states and corporations to ensure their data safety. Quantum cryptography makes it possible to identify attempts to listen to conversations and ensure the secrecy of the transmitted data using fundamental requirements

rather than technical or computational constraints. The bottleneck in cryptography is still the transfer of cryptographic keys.

Bennett and Brassard conducted the first successful experiment in quantum data transmission in late October 1989. In this experiment, they established a secure quantum communication at 32.5 cm. The setup changed the photons' polarizations, but the power supply made distinct noises depending on the polarization was. They then carried these experiments out using an optical fiber as the propagation medium. After Muller's first experiments in Geneva, using a 1.1 km optical fiber (Muller et al. 1994 and 1995) the transmission distance increased to 23 km via an optical fiber laid underwater (Muller et al. 1995 and 1996). At almost the same time, Townsend from British Telecom showed a 30 km transmission (Marand and Townsend 1995). Later, he continued testing systems using different optical network structures (Townsend 1997) and increased the range to 50 km (Townsend 1998). In 2004-2005, two groups in Japan and one in the United Kingdom reported conducting experiments on quantum key distribution and single photons interference over a distance of over 100 km (Kimura et al. 2004), (Gobby et al. 2004), (Takesue et al. 2005). Scientists from Toshiba conducted the first experiments on transmission over 122 km using detectors based on avalanche photodiodes (Gobby et al. 2004). In July 2005, Toshiba engineers took the lead in the race to increase the key distributing distance by introducing a system capable of transmitting a key over 122 km. The record for the information transmission distance belongs to the Los Alamos association of scientists and the NIST and is 184 km (Hiskett et al. 2006). It used single-photon receivers cooled to temperatures close to $0^{\circ}K$.

Thus, in less than 50 years, quantum cryptography has progressed from an idea to commercial QKD systems. The present equipment allows us to distribute keys through a quantum channel over a distance of over 100 km (a record of 184 km), with speeds suitable for transmitting encryption passwords but not acceptable for stream encryption of trunk channels using the OTP cipher (Vernam 1926). The primary users of quantum cryptography systems are state and financial organizations. At the moment, the high cost of QKD systems is limiting their mass use for organizing confidential communication between small and medium-sized associations and individuals.

In October 2007, the quantum encryption methods were first applied in a wide-scale project. The quantum secure transmission system, established by the Swiss company ID

Quantique, was used to transfer data on the voting results in the parliamentary elections in the Swiss canton of Geneva.

In the following years, such commercial giants as Toshiba, NEC, IBM, Hewlett Packard, Mitsubishi, and NTT joined the design and manufacture of quantum cryptography systems. But along with them, small but high-tech companies appeared on the market: MagiQ, ID Quantique, Smart Quantum.

The American company MagiQ Technologies specializes in the development of quantum cryptography technologies. MagiQ Technologies started constructing equipment for protecting information transmitted over fiber-optic networks using quantum cryptography technology back in 2004.

ID Quantique is a Swiss company that has been producing QKD systems, quantum-secure network encryption, and hardware for PRNG since 2001. It is the first company that has introduced the QKD method into commercial use.

On an international scale, China is stepping forward as a leader in the quantum field. Researchers have already built a 2000 km long Beijing-Shanghai quantum network, which consists of four local quantum systems. This network connects 12 Chinese banks and Alibaba. They use a QKD system to exchange private information and protect user data. They implemented quantum cryptography using fiber lines and in open space. For example, in Earth-satellite mode, can implement the global distribution of cryptographic keys. Chinese scientists have already conducted quantum-protected video conferencing via satellite key distribution between Beijing and Vienna.

2.1.1. Use of quantum systems in finance

Currently, many financial establishments are interested in practicing quantum computing to implement management and analysis functions. Soon, ultra-fast quantum computers will replace conventional computers in considering risk models, identifying new computerized trading strategies, and changing the prices of the derivatives in actual time. IBM is already working with commercial companies, such as Barclays, and JP Morgan to establish specialized financial software for quantum computers. Many scientists think that with the help of quantum computers, the recognition of financial fraud and data theft attempts can speed up.

IBM Q and the Qiskit Finance framework have already been used to achieve quan-

tum algorithms in pricing and investment portfolio optimization. But it can extend this approach to further complex cases. The examples may include the pricing of trajectory-dependent derivatives in complex market dynamics or issues, such as dynamic portfolio optimization and pricing that are unsolvable today. Quadratic acceleration can have a positive impact on business by forcing the demand for central allocation, seeking new investment opportunities, and responding more quickly to market volatility. JPMorgan Chase Bank and Barclays Bank are planning to use quantum computing to speed up risk reduction and improve productivity models (Lacan et al. 2019).

Large commercial banks and financial organizations, government agencies, as well as Data Processing Centers actively used quantum communication security technologies. The global quantum cryptography market was estimated at \$343 million in 2018 and is expected to double to \$506 million in 2021 (Wood 2018).

Data and communications protection is a leading preference for companies that deal with an organization, personal, and government commercial data. Financial institutions are more exposed to cyberattacks than other organizations. Attackers eventually get access to them as they improve the capabilities of quantum computing. QKD will help protect communication channels from conventional and quantum threats. Using quantum principles can make sure the present and future confidence of encryption keys. Also, quantum principles can help prevent eavesdropping by illegitimate persons. Companies must act now to adopt cryptographic techniques which will protect data on both classical and quantum computers. For example, types of lattice-based cryptography are already being investigated. This appears to be proof against to quantum computer attacks. So far, none of the known algorithms can crack these data encoding techniques. Post-quantum cryptography is discussed in Section 3. 6.

2.2. Introduction to Cryptography

There are various ways to protect data. Thanks to modern means of computer technologies, the scientific and technical revolution have recently reached a large scale in society informatization. It requires protection from unauthorized access by persons who shall not have access to it.

The information security problems in all spheres of human activity nowadays come to the fore. Computer networks and the information environment they support are fertile

ground for cybercrime. There are many attacks, like the theft of confidential information, the destruction of data, web resources, and the theft of money from the owner's accounts. Means of protection against cyber threats are also progressing. So, the theory of information security studies the methods of cryptography that help protect data from unauthorized access.

From the early days of writing until the mid-20th century, cryptography was an art. It is not only a well-developed science area at the mathematics and computer science intersection now, but it is also what we use every day. The best minds of all times and peoples have been searching for discovering ways and methods to encrypt data for a long time. People before used cryptography only in diplomacy, politics, and military affairs. It becomes necessary to protect intellectual property, with the development of writing, from persecution by the Inquisition or borrowing by intruders. Even then, cryptographers created such encryption methods that decryption for the intruders was a practically impossible task.

Nowadays, the most popular medium for data transmission is the global Internet. Ensuring the protection of the integrity and reliability of the transmitted information is of importance. Using cryptographic techniques makes it possible to transfer confidential information, establish the authenticity of transmitted messages, and store information on media in encrypted form. Thus, cryptography helps us to protect user data.

Cryptology is the science that studies the techniques of encryption (cryptography) and decryption (cryptanalysis) of information. Cryptography is the science of how to protect a message. Cryptanalysis is the science of a way to extract the plaintext without knowing the key.

Cryptography is the science of mathematical methods to ensure the confidentiality and authenticity of the information. It is the main element of data protection, which allows us to solve the security issues of computer systems and networks. With the information society formation, cryptography becomes one of the principal tools for ensuring privacy, authorization, electronic payments, confidentiality of organizations, and many other things.

Methods of encrypting information to protect it from unauthorized access are called ciphers. In this process, the source data is called plaintext, and the result of applying a cipher to it is the ciphertext. These processes of message transformation are called

encryption and decryption.

Traditionally, the participants in the encryption/decryption process called Alice and Bob. Also, cryptography considers the possibility of eavesdropping. Usually, an eavesdropper is called Eve. The eavesdropper has modern computing resources, is fully conscious of the cryptographic methods, algorithms, and protocols used, and tries to breaking them. The breaking means illegitimate reading of classified message. All these actions of the eavesdropper are called cryptographic attacks. Cryptography aims at developing techniques that provide resistance to any attacks. However, at the time of the creation of the cryptosystem, it is impossible to foresee unknown attacks.

2.2.1. Historical background

Cryptography is one of the oldest sciences. Its history goes back about 4 thousand years. There are four stages in the history of cryptography. The first period we can characterize by the dominance of monoalphabetic ciphers. This period is characterized using any, usually primitive, methods of confusing the enemy about the content of encrypted messages. A fundamental principle is an alphabet replacement of the original text by another alphabet by substituting letters with other letters or symbols. One of the first recorded examples is the Caesar cipher, which comprises replacing each letter of the original message with another one that is separated from it in the alphabet by a certain number of positions.

The second period was marked by introducing polyalphabetic ciphers into use. This period is associated with the emergence of formalized and relative resistance to manual cryptographic analysis of ciphers.

The third period is characterized by introducing electromechanical devices into the work of cipher-fellers. From that time on, people talked about cryptology as the science of transforming information to ensure its secrecy.

By the early 30s, the branches of mathematics that are the scientific basis of cryptology were finally formed: probability theory and mathematical statistics, algebra, number theory, the theory of algorithms, information theory, and cybernetics developed actively. The basis of cryptology as a science was the work of Shannon's "Communication Theory of Secrecy Systems" (1949). For a long time, people associated cryptography only with the development of transforming information methods. Computer technology for data

processing radically changed the tasks of cryptography. The need to protect information arose long before information technology. His work summed up the scientific basis for cryptography and cryptographic analysis.

The fourth period from the middle of the 20 century is the period of transition to mathematical cryptography. This period owes its appearance to computing tools with sufficient performance to implement cryptographic systems that provide several orders of magnitude higher cryptographic strength at high encryption speed than manual and mechanical ciphers. However, until 1975, cryptography remained classical. It is cryptography with a secret key. The emergence and development of a new direction distinguish the modern period of cryptography development. This direction is called public-key cryptography or asymmetric cryptography. New technical capabilities mark not only its appearance but also the relatively widespread use of cryptography for use by everyone. The legal regulation of cryptography used by people in different countries varies from permission to complete ban.

The first class of cryptographic systems, the practical application of which became possible with powerful and compact computing tools, were block ciphers. In 1978, NIST developed the American DES encryption standard. It is a block cipher with symmetric keys. Its key length is too short compared to modern methods, making it vulnerable to brute-force attacks. Thus, it is not suitable for storing secrets for a long time, but it may well serve in applications where information needs to be closed for a short time.

In the mid-70s of the twentieth century, there was a genuine breakthrough in modern cryptography – the emergence of asymmetric cryptographic systems that did not require the transfer of a secret key between the parties. The beginning of this period was the work published by Whitfield Diffie and Martin Hellman in 1976. It is the first to plan the principles of exchanging encrypted information without exchanging a secret key. A few years later, Ron Rivest, Adi Shamir, and Leonard Adleman discovered the RSA system. It is the first practical asymmetric cryptographic system whose stability was based on the problem of factorization of large numbers. Asymmetric cryptography has opened several new applications, EDS, and electronic money systems.

In the 1980s and 90s, completely new areas of cryptography appeared: probabilistic encryption, quantum cryptography, and others. But unfortunately, the practical significance of these areas is not fully disclosed.

2.2.2. Modern cryptography

It is complicated to develop a new cipher, so the cipher must serve for a long time. Dutch mathematician Kerckhoff, who lived in the 19th century, formulated a rule according to which cipher strength should be based not on the cipher algorithm secrecy itself but only on keeping the key secret. This requirement for cryptographic systems remains relevant to this day. For this purpose, we allocate a replaceable element to the cipher. This element is key. Currently, if the adversary knows the current cipher, there is no need to invent a new one, enough to change the key. Also, it makes it possible to use the same cipher independently by different people.

The development of modern cryptology as a science is predicated on a set of theoretical conceptions and laws of mathematics, physics, information theory, and computational complexity, which are very difficult for a comprehensive and deep understanding, even for professionals. However, despite its intrinsic complication, many theoretical achievements of cryptology are now used by us in everyday life, for example: in bank cards, in e-mail, in bank payment systems, in electronic exchange, in document management systems, in database management, electronic voting systems, etc. Such a rate of total internal complexity and practical applicability for theoretical science seems to be unique.

The achievements of modern cryptography allow us to protect information from unauthorized access, distortion. These achievements give us to deal with issues with the document authorship and many others. One of the hardest issues in the cryptosystem's operation is the secrecy of keys. The human factor influences the key safety, and it is the weakest link in the security system. We should still consider that for many crypto algorithms on the inability to solve mathematical problems in a reasonable time (the cheapest route, discrete logarithm, prime factorization). But it is possible to find new algorithms that can solve these problems in a shorter time. Also, the possibility of finding a quick way to solve these problems using a quantum computer is not excluded.

Despite the visible benefits of its use, cryptography is fraught with the probability of creating the illusion of complete security and, as a result, weakening attention to other methods of protecting information. Cryptography remains one of the most rapidly developing fields of knowledge and remains a reliable among the means of ensuring data security.

2.2.3. Encryption and decryption

Encryption is applying a cipher to the secured information. It is converting the protected information into an encrypted message applying rules in the cipher.

Decryption is the reverse procedure of encryption. It is the conversion of an enciphered information into protected message using rules in the cipher.

The key is the most important part of the cipher, responsible for choosing the transformation used to encrypt a particular message. Usually, the key can be a letter or numeric sequence.

Cryptographic systems by the type of encryption algorithm are divided into two large groups: symmetric and asymmetric. Currently, the use of symmetric and asymmetric cryptography, along with the use of stream ciphers and hashing functions, has become widespread. Besides encryption algorithms, the strength of modern passwords also depends on the length of the encryption keys used. Modern cryptography assumes that the secrecy of the cipher is provided only by the encryption key since the algorithm itself can eventually become known to the enemy.

2.2.4. Symmetric algorithms

Symmetric algorithms are algorithms used for tasks such as encrypting large databases, file systems, and storage. With symmetric encryption, the parties exchanging data use the same secret key to encrypt and decrypt data, as shown in Figure 2.1. The third-party does not know this key, so it does not have access to the data. Depending on the principle of operation, symmetric encryption algorithms are divided into two types: block and stream cipher.

Block cipher algorithms encrypt data in blocks of fixed length. Depending on the algorithm, block length can be 64, 128, or any other number of bits.

A stream cipher is an encryption technique that works on a specific sequence of input bits. Most stream ciphers work by achieving a long string of random bits from the key, which are later connected with the data to encipher.

Symmetric encryption requires fewer resources and produces higher encryption speed than asymmetric encryption. Most symmetric ciphers are resistant to attacks by quantum computers, which in theory pose a threat to asymmetric algorithms. The weakness

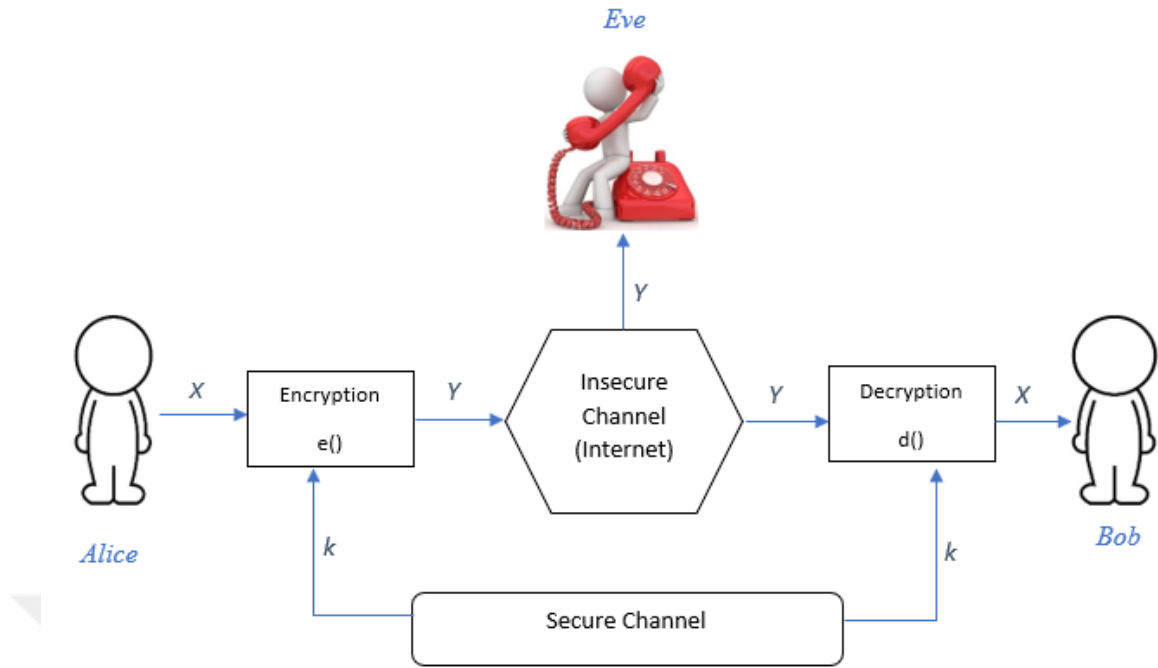


Figure 2.1. Symmetric-key Cryptosystem

of symmetric encryption is the key exchange. In many systems, this problem is solved by encrypting the key using an asymmetric algorithm. The most established symmetric encryption methods are such algorithms as DES, AES.

2.2.4.1. Vernam cipher

Vernam cipher is a symmetric encryption system that uses the same key for encryption and decryption. Gilbert Vernam, an AT&T telegraph operator, invented it in 1917. In cryptography, this cipher is also known as the OTP. It is the only type of encryption with strictly proven cryptographic strength. In OTP cipher, used a unique encryption key to encrypt data. It is rarely used since the required key length is equal to the entire transmitted text. However, because of its absolute cryptographic strength, it is used to protect important communication lines.

To make the password truly strong, we must follow the following three rules:

1. The encryption key is selected randomly.
2. The length of the key must be corresponding to the length of the plaintext.
3. The key must be used only once.

The Vernam cipher is very simple and is the only known absolute secret cipher. The secret lies in the fact that the message is encoded by a bitwise xor with a one-time key,

the length of which is not less than the length of the transmitted message. If we denote the key as k , the plaintext as m , and the ciphertext as c then the encryption and decryption algorithms will look as following:

$$\text{encryption: } c = m \oplus k$$

$$\text{decryption: } m = c \oplus k$$

2.2.4.2. Key distribution

No matter how complex and reliable cryptographic systems are, the key distribution problem is their weak point in practical implementation. To exchange secret information between two entities, one entity must generate a key and then secretly transmit it to the other entity.

A key distribution protocol is a conditional sequence of user actions to create a secure communication channel. This channel contains generating and exchanging session keys and authenticating messages. The main task of the key distribution protocols is to develop a common key by the participants, Alice and Bob. Both Bob and Alice must be sure that they conduct the communication with the interlocutor and not with an eavesdropper.

Key distribution protocols fall into the following categories:

- Protocols based on asymmetric cryptography.
- Protocols based on symmetric cryptography.
- Protocols that use a certification authority.

In modern cryptography, we solve the key management problem using cryptographic protocols. The basis of these protocols is the generation and distribution of keys between users.

There are key distribution schemes in symmetric cryptographic systems, where a mandatory component is a secure communication channel through which the secret key is transmitted. Symmetric cryptography involves encryption and decryption using the same secret key. It is necessary for users to develop the shared key correctly, as well as securely transfer it. It is difficult to do in an unprotected channel.

However, the most efficient methods are asymmetric cryptographic systems. This system is an encryption or EDS system in which the public key is transferred over an

open channel and applied to verify the EDS and to encrypt the information. Their essence is that each addressee generates two keys connected by a rule. The public key is published and accessible to anybody who wishes to send a message to the recipient. The private key is kept secret.

The transmission of encrypted files over the channel allows us to solve the problem of intercepting information in the clear. By pre-encrypting the files, the system user can ensure their security. However, there are problems related to file distribution, and the main problem is related to the distribution of keys.

The problem of key distribution in a cryptosystem is one of the most important and expensive procedures since the key requirement for confidentiality and authenticity is to change the keys after each session of information exchange.

We can only guarantee the confidentiality of the transmitted password when the key does not reach the eavesdropper. We should emphasize that there is no classic encryption mechanism that can completely guarantee that the key will not be intercepted during transmission through the classical communication channel.

2.2.5. Asymmetric algorithms

All the above applies to classical cryptography, so-called cryptography with a secret key. A key that both parties exchanging information must know and keep in the strictest confidence. However, when mathematicians Ron Rivest, Adi Shamir, and Leonard Adleman developed their RSA algorithm in 1977, a new era began. This is the public-key cryptography era. There is no need to send the private key to the partner via a stable channel. It can simply distribute the keys through any communication channel. We use a public key known to everyone to encrypt information and use a corresponding private key known only to the owner to decrypt it. Thus, anyone can encrypt a message, but only the owner can decrypt it. Getting a private key over an open one is a task of enormous computational complexity. Such systems are also called asymmetric systems. The scheme of public-key encryption is shown in the Figure 2.2.

Asymmetric cryptography is based on the complexity of computing the discrete logarithm in finite groups, defined over various algebraic constructions, or on the complexity of the decomposition of a natural number into prime factors. This encryption method uses a pair of keys: public and private keys. These keys allow the cryptographic algorithm to

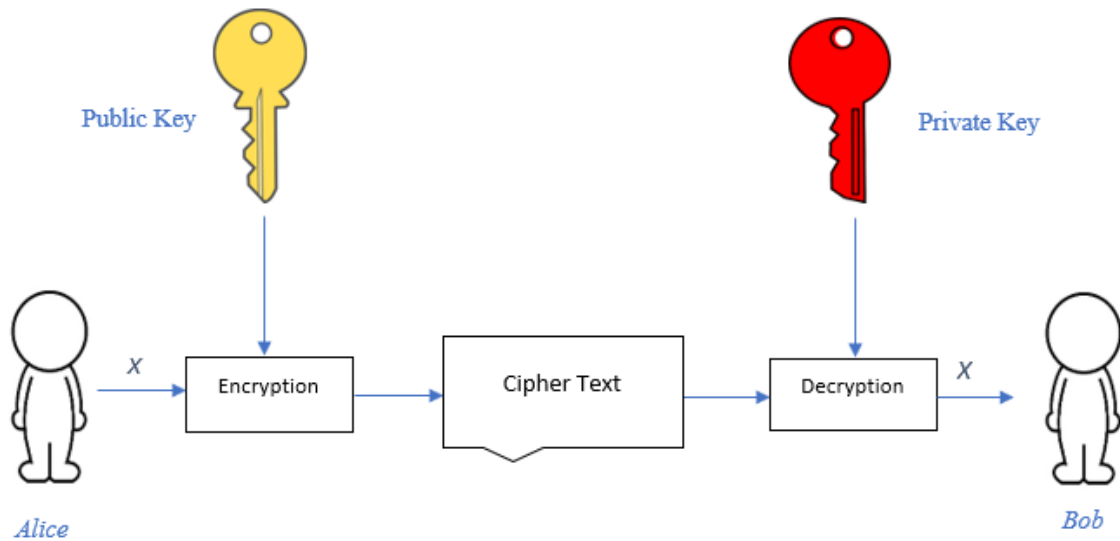


Figure 2.2. Public-key Cryptosystem

encrypt and decrypt the message. However, messages enciphered with a public key can only be decrypted using a private key. Mathematical dependencies link these keys. It is almost impracticable to compute the private key from the public key. The public key is published in the owner's certificate and is available to the connecting client. The certificate owner stores the private key. It allows the public key to be freely transferred to others. Using an asymmetric approach, parties can start an exchange without sharing secret information. Here, the recipient knows both keys and passes the sender only the public key.

2.2.5.1. Diffie–Hellman key exchange

The DH method is the first technique that provided us to keep data without needing secret keys transmitted over protected channels. This cryptosystem was discovered in the mid-70s and led to a real revolution in cryptography and its practical operations. In this algorithm, we get the shared key from the sender's private key and the recipient's public key. The receiver calculates the same key using its private key and the sender's public key. An attacker who observes the key exchange gets the public keys of both subscribers at his disposal. However, he cannot calculate the secret key on which we will perform the encryption. It is because we apply equations linking the private and public keys the easy to solve in one direction and hard in the other. If we denote the private key as X and the public key as Y , then their ratio will look as

$$Y = A^X \pmod{P}. \quad (2.1)$$

For large values of A , X , and Y , within a reasonable time cannot be calculated for A known X and Y . It is necessary to calculate the discrete logarithm of Y in base A , whereas the exponentiation operation is relatively easy.

2.2.5.2. RSA algorithm

Currently, RSA is the most developed method of cryptographic protection of information with a public key. The cryptographic strength of the algorithm is based on the theory that it is complex to determine the secret key from a known key since this requires solving the factorization problem. This problem does not have an effective solution to date. The advantages of this algorithm include very high cryptographic stability, simple software, and hardware implementation.

In the RSA every user needs to generate a public-private key pair. To do this, a user chooses two large primes. Typically these primes will have bit length 512, 1024, 2048, 4096, etc. The most crypto-resistant systems use 1024-bit and large numbers.

The RSA works as follows:

1. The user chooses two large prime numbers p, q .
2. The user will calculate $n = p \cdot q$ and $\phi(n) = (p - 1) \cdot (q - 1)$.
3. The user also picks a public key e and a private key d such that

$$e \cdot d \equiv 1 \pmod{\phi(n)}$$

4. Thus private keys of the user becomes $p, q, \phi(n)$ and public keys are n, e .

To encrypt messages applying the public key n, e , the user need to break the ciphertext into blocks, each of which can be defined as a number $m(i) = 0, 1, 2, \dots, n - 1$. Then, encrypt the ciphertext with

$$c = m^e \pmod{n}$$

To decrypt this message using the private key d, n , need to achieve the following

algorithm

$$m = c^d \mod n$$

2.2.5.3. Hybrid systems

Asymmetric information encryption systems have two main drawbacks. It is the dimension of the keys and the complexity of the operations performed. Hence, asymmetric systems in their pure form are rarely used. The most widespread is the so-called hybrid systems (Figure 2.3). In this system, we use symmetric algorithms to encrypt information, and asymmetric cryptography is used to sharing symmetric keys.

A hybrid cryptosystem can be built applying any two different encryption systems:

- A key encapsulation system, which is an asymmetric-key algorithm.
- A data encapsulation system, which is a symmetric-key algorithm.

A hybrid cryptosystem is an asymmetric key encryption whose public and private keys are the same as in the key encapsulation system.

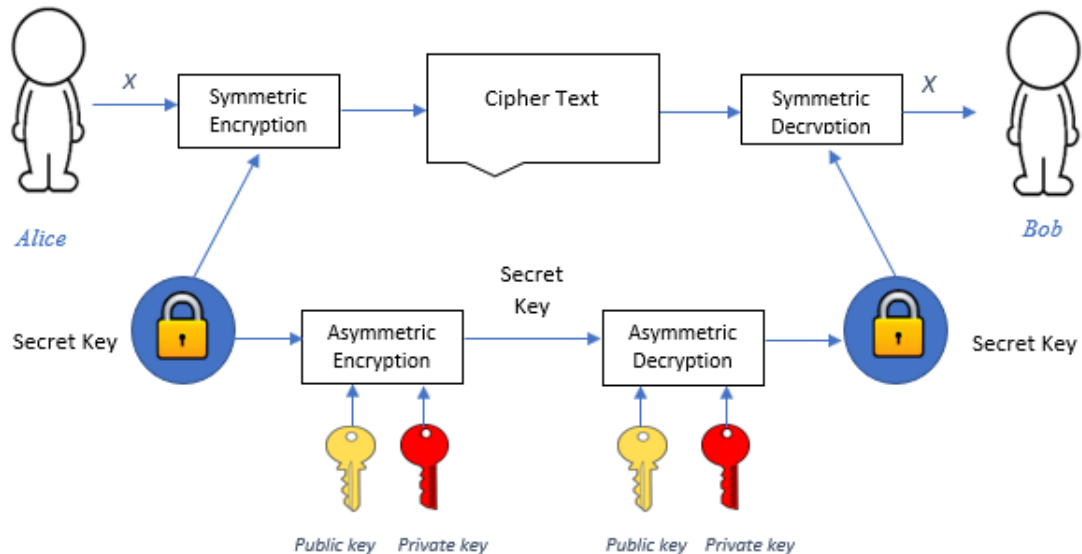


Figure 2.3. Hybrid Cryptosystem

2.2.6. Digital signature

Digital signatures most often use public-key cryptography. They have a digital identifier based on a certificate issued by an accredited certification authority. They are part of the

mechanism for verifying the security and authenticity of digital messages. An EDS is information in electronic form, which is formed using a unique combination of characters and gives an electronic document legal force.

The electronic document containing the EDS confirms the authentication of the declared sender, the non-repudiation of the message, and handles the integrity of the transmitted data. Using EDS reduces the cost of collecting, processing, delivering, recording, and storing documents. Thanks to a sophisticated encryption system, the electronic signature guarantees the authenticity of documents and the confidentiality of data exchange. Electronic signatures are commonly used to conduct financial transactions, distribute software, generate tax and budget reports, and detect forged documents or falsifications.

An EDS is a sequence of characters that allows us to identify the owner of the EDS and verify the integrity of the document contents. A hash function is used to create an EDS, which is a one-way function. We can easily calculate the hash function with a known argument, but find the argument value with a known hash function is difficult.

2.2.7. Other primitives and security requirements

Information technologies increase in the speed of processes documentation and also using the Internet allows each user to build their communication with the bank based on personal preferences. These have a significant impact on increasing the attractiveness of banks for the user. The provision of financial services for online banking is becoming important every day. The customer gets any report about their accounts that interest him by accessing the bank's website, to clarify the correctness of the details specified by the prospective partner, to do any available operations with a card, and all these services do not require a bank employee. Non-bank financial establishments are still gaining popularity and are struggling to raise funds. But, there is also cooperation among banks and other financial institutes. The participation will further develop information technology in this field to improve the interactive system of these financial organizations.

Ensuring the stability of the event and operation of banking systems has occupied a special place in the commercial sphere. As it introduces internet banking services into the system, this problem becomes more serious. Now a wide range of requirements is established on the security system.

The fundamental safety principles are:

- Confidentiality is an avoiding disclosure of knowledge to unauthorized people.
- Integrity could be a preventing damage, distortion, or modification of information or services.
- Authentication is an identification of identity or another object before providing this identity or an object of data access.
- Identification is a procedure for allowing a subject by his identifier. The identifier assigned to the present subject and entered the database at the time of registration as a legitimate user of the system.
- Authorization is an ensuring access to data just for those persons who are properly allowed and received the rights.
- Availability is an ensuring the operability and availability of information resources, services, and equipment.

Confidentiality is the principle of non-disclosure of information that is not intended for public access or use by everyone. The term “confidential” comes from the Latin word “confidentia,” which means trust. Confidential information is oral or documentary information that is not subject to public disclosure, got by a private person in a confidential, frank, or secret environment, and of a definite value. A threat to economic, state, or personal security may be created when such information is disclosed. Confidentiality shows the desire to define access to resources for a specific group of people. Information becomes available only to users who are introduced in information processes and have passed identification.

Information integrity is a property of information that characterizes its resistance to accidental or deliberate destruction or unauthorized modification. Integrity divide into static and dynamic. Static integrity is the immutability of information. Dynamic integrity related to the correct execution transactions. We use dynamic integrity to analyzing the flow of financial messages to detect theft, reordering, or message duplication. Integrity turns out to be a significant aspect of information security when information serves as a guide to action.

Availability is a support that the user will receive the required information or information service within a specific time. The time factor in determining the information

availability sometimes is necessary. Some types of data and information services make sense only in a certain period. Information accessibility means that users with access can always freely exercise these rights. They have access, store, change, copy, and use this information. Availability threats are restricting or blocking access to data (for example, the inability to connect to a server with a database because of a DoS attack).

The term authentication refers to confirming the identity of a person or object. In electronic information processes, the authentication is a single method applied to control access to user accounts and secret information. Authentication verification involves users submitting their accurate identification data together with one or more identity verification aspects to the information system to confirm its authenticity.

The authenticity of the information is authenticity, completeness, and accuracy of the data. It means that the information

- was created by legitimate participants in the data handling;
- was not subject to accidental or deliberate distortions;

Authentication is one of the key mechanisms for protecting information on the network. It means checking the user so he can get this or that resource. The operating principle is that when a user wants to access any server, it provides him with an authentication form. When the user fills this form, entered data checks on the server. After receiving a positive response from the authentication server, it permits the user access to the desired resource. The authentication principle is such that the recipient writes what he knows. It is the secret word that he provides to the authentication server. One of the authentication schemes is the use of passwords. A password is a character set known to a connected user. The user enters it at the network interaction session beginning and sometimes at the end of the session. This scheme is the most simple and vulnerable. Another person can intercept and use the password. It is not good from a security point of view. The most common is to use the OTP scheme. It will be useless at the next registration, and to get the next password from the previous password, please provide time and resources. When generating an OTP used generators at the software and hardware level, which are inserted into the computer slot. Knowing the password gives the user the right to work with the device. Existing authentication methods employ three main classes of factors:

- What the user knows (PIN, password).

- What the user has (for example, a plastic card, electronic key Token).
- What the user is characterized by (for example, biometric characteristic).

Authentication procedures using over one factor are significantly more complex to break than single-factor systems. Accurately designed and realized multifactor authentication schemes are more predictable and effective against attackers. For example, using a username/password to log into the system is one-factor authentication (that is, what the user knows). An ATM transaction demands two-factor authentication, a presentation of what the user possesses (debit card) linked with what the user knows (password).

Two-factor authentication methods should also include defining the amount of failed authentication attempts to reduce the risk of brute-force attacks. Enterprises can only use one-factor authentication on monitoring and auditing subsystems. Using one-factor authentication is unacceptable in systems performing transactions related to access to info about user or the movement of funds.

Identification is the procedure for authorizing a person by a unique identifier assigned to this user earlier and entered the database at the time of registration as a legal user of the system. It performs this function first when the user attempts to log on to the network. Upon request, the user informs the system of its identifier, and the system checks its existence in the database. User identifiers can be, for example, a plastic card or the format of a username, a bank card number, name.

Identification and authentication are the interrelated processes of user identification and authentication. It is on them that the next decision of the system depends. It is possible to allow access to the system resources to a specific user or process or not. After identifying and authenticating the person, it performs its authorization.

Authorization is a procedure for granting a subject certain powers and resources in this system. It establishes the user and the resources available to this user. If the system cannot reliably distinguish an allowed person from an unauthorized person, the confidentiality and integrity of information in it may be compromised. Unlike authentication, which provides us to recognize legal and illegal users, authorization deals only with users who have successfully passed the authentication procedure.

The relationship between identification, authentication, and authorization:

1. Identification determines the name or number

2. Authentication checks the password (key or fingerprint)

3. Authorization provides access

This relationship is shown in Figure 2.4.

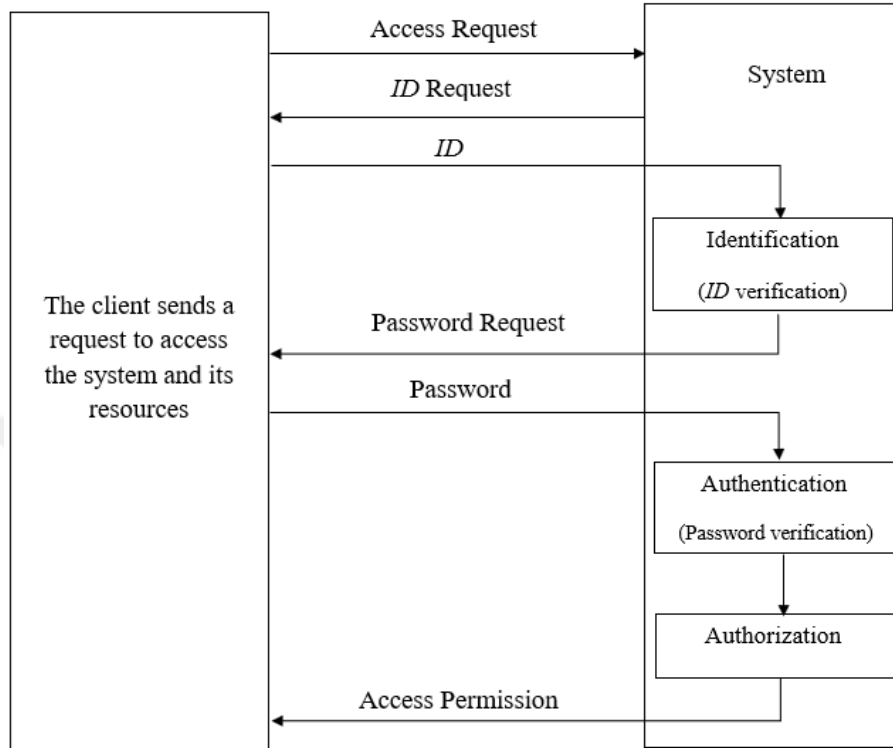


Figure 2.4. Information Security

2.3. Fundamentals of Quantum Computing and Communication

2.3.1. Quantum computer

People use computers everywhere to improve their social lives. In science, computers are necessary for analyzing and calculating complex systems and visualizing the data obtained. By definition, a computer is a device that can convert input information into output in the desired way.

The modern digital civilization directly depends on computers, which are becoming more powerful, smaller, and cheaper. Today, the average size of transistors that are the main components of computers is 14 nm. Progress in this area does not stand. Scientists have reached the physical limit of technology. They created the atomic-sized transistor whose central component is only 1.5 nm in size. But at this scale, the quantum effect has already worked. Electrons can use quantum tunneling to jump to the other side of the

closed gate. Scientists hope to use this feature to its advantage by developing quantum computers.

Using the quantum mechanics laws, we can create a new type of computer that will allow us to solve many problems. Even these problems are inaccessible even to the most powerful digital devices. The speed of many complex calculations will expand; messages sent over quantum transmission lines will be impossible to intercept or copy. Today, it has already created prototypes of these quantum computers of the future.

The fundamental difference between a quantum computer and a classical one is the representation of information. The basic unit of information in a classical computer is a bit. It can take two values: 0 or 1. We can encrypt any information using bit strings (strings of zeros and ones). Logical elements (gates) are used to convert bit strings, each of which performs an elementary logical operation. Classical computer needs a billion different data sets to calculate a billion different bit combinations, while a quantum computer will only need to create a single quantum state. The combination of logical gates implements function depending on the type and order of the using elements. A classical computer can solve many tasks. However, there are problems that the classical computer does not solve well.

A quantum computer uses the phenomena of quantum superposition, quantum entanglement, and the principle of quantum parallelism to process and transmit information. The basis of such a computer is a qubit, which is something that can be in two eigenstates. A state vector which is a superposition of basis vectors describes the behavior of a qubit. A quantum register is a chain of quantum bits, over which it is possible to perform one-and two-bit operations (which are unitary).

As for the quantum computer, its operation is based on the superposition principle, and instead of bits, we use quantum bits or qubits. The qubit also has two states: zero and one. However, because of superposition, qubits can accept the values got by combining them and be in all these states at the same time. It is the parallelism of quantum computing. There is no need to iterate over all variants of the system states.

Only four pairs, such as 00, 01, 10, and 11, can be made from bits in states 0 and 1. But the state numbers for qubits is 2^n . For four, it is 2^4 , that is 16. And for 10 is already 1024. This number grows exponentially with each new qubit. The 20 qubits can already store over a million values at the same time. For the number of combinations of all states

of a quantum computer from 300 qubits, there are not enough atoms in the Universe.

Another strange property of qubits is entanglement, where each qubit instantly reacts to a change in the state of another qubit. The researchers' task is to manipulate the qubits so that each one performs its task. Then the calculations will be carried out in parallel. A quantum computer will get a result faster than a regular one by increasing the number of states. It is quantum superiority. It is assumed that quantum computers will solve complex correlation problems, for example, finding items in databases, encrypting, and decrypting data.

Quantum computing is an actively developing and promising research area in quantum electronics. It will expand and multiply our computing abilities. It relates the advantages of a quantum computer to the uniqueness of the laws of the quantum world. Using this technology will help us find solutions to problems that require calculations, such as modeling complex biological systems, creating an artificial intelligence system, optimizing complex systems, and various comparison operations. Usually the quantum computing prospects associated with exponential problems. These problems are solving acceleration and with the solution of an entire class of issues. Those are non-computable in the sense that they cannot be solved on modern classical computers, which lack computing power.

The concept of quantum computing was invented to solve problems of exponential complexity. Manin (1980) and Feynman (1982) have put the first idea of using quantum mechanics in computer technology forward. Feynman suggested that it is likely that quantum computers will have properties that will allow us to solve quantum problems. A quantum computer is a device that performs logical operations on quantum states using transformations that do not violate quantum superpositions during calculations. Schematically, the operation of a quantum computer can be represented as a sequence of three operations:

- Preparation of the initial state.
- Calculation (transformations of initial state).
- The result output (measurement, projection of the final state).

The first quantum computer resembled a clunky old computer system. The size of the quantum chip itself is small. Most of the rest of the computer's space is taken up

by cooling and shielding systems. They are designed to create the necessary conditions for the functioning of a computer and eliminate external influences. Thanks to the liquid helium-based cooling system, the temperature of the quantum chip remains at -273°C .

2.3.2. Quantum states and qubits

Before considering the basic concept in the model of quantum computing – qubit, it is necessary to study the conception of a quantum state. The quantum state is a set of symbols and coefficients attributed to it. This coefficient is a complex number. We will write the quantum state as:

$$\alpha|s\rangle \quad (2.2)$$

where α is a complex number coefficient, and s is the name of the quantum state.

The quantum state s usually consists of a single character, for example, 0, 1, +, -. So, quantum states, for example, are objects such as $|0\rangle$ and $|1\rangle$. Also, we can make complex quantum states. As mentioned above, elementary classical data carriers are bits. It is a system that can take two states, denoted by zero and one. In contrast, qubits can take on infinitely many different states and are systems whose quantum states are described by a vector of two-dimensional Hilbert space. Let us choose a pair of normalized orthogonal states in this space and denote them by $|0\rangle$ and $|1\rangle$ if these states correspond to the values 0 and 1 of the classical bit. The basis formed by these states is called the computational basis. Then, a qubit state may be written as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (2.3)$$

where α and β are complex numbers satisfying the normalization condition

$$|\alpha|^2 + |\beta|^2 = 1. \quad (2.4)$$

It follows from the condition that the vector $|\psi\rangle$ can be rewritten as

$$|\psi\rangle = e^{i\gamma} \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle, \quad (2.5)$$

where γ , θ , and ϕ are real values. Further, since the state vectors are determined up to

the general phase, we can put $\gamma=0$. Thus, the entire variety of qubit states is described by two real parameters θ and ϕ . These two numbers define a point on a three-dimensional sphere of unit radius called the Bloch sphere.

$$|\psi\rangle = \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} \end{bmatrix} \quad (0 \leq \theta \leq \pi, 0 \leq \phi \leq 2\pi) \quad (2.6)$$

The qubit has one strange feature. Its value depends on the measurement. The programmer cannot know the value of the qubit until he has measured it. Also, the very fact of measuring a qubit affects its value.

The information stored in a qubit is most often represented as a vector of the form $\begin{bmatrix} x \\ y \end{bmatrix}$, which is called the quantum state vector.

The vector $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ corresponds to a classical bit with a value of 0, and the vector $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ corresponds to a bit with a value of 1. The described vectors are the basis for the vectors of quantum states, i. e. , any vector can be expressed in terms of the sum of the basic ones:

$$x \begin{bmatrix} 1 \\ 0 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (2.7)$$

Today, more theoretical works and even practical developments appear in quantum computing. It bases this computational model on the concept of a qubit. The quantum nature of the qubit lies in the principle of superposition. A quantum computer can be treated as a set comprising n qubits for which the following operations are practically defined:

- We can prepare each qubit in a known state $|0\rangle$.
- We can measure each qubit on a basis $\{|0\rangle, |1\rangle\}$.
- A universal quantum gate can apply to any subset comprising a fixed number of qubits.
- The state of qubits is changed only through the above transformations.

One of the difficult moments for quantum mechanics perception is the lack of visual

representations for dealing with state vectors and density matrices. One of the simplest options for comparison of the vector of Hilbert's space with three-dimensional objects is the Bloch sphere. The Bloch sphere is used for convenient visualization of the quantum state vector of a qubit.

2.3.2.1. The Bloch sphere

A vector of unit length represents a qubit in three-dimensional space. Such a geometric representation of a qubit is called its representation on the Bloch sphere. The Bloch sphere is a unit two-dimensional sphere, with each pair of diametrically opposite points corresponding to mutually orthogonal state vectors. It is conventionally assumed that the north and south poles of the Bloch sphere correspond to vectors $|0\rangle$ and $|1\rangle$, which may denote electron spins (spin up and spin down).

The classical bit on the surface of the Bloch sphere can only be at points $|0\rangle$ “logical 0” and $|1\rangle$ “logical 1”, and the rest of the sphere is inaccessible to it. Any point on the surface of the Bloch sphere can represent the state of a qubit, describing the pure states of the quantum medium, which are always coherent. Mixed quantum states are incoherent and can be mapped on the Bloch sphere. Thus, it is possible to represent a state of any quantum system characterized by orthonormalized wave functions.

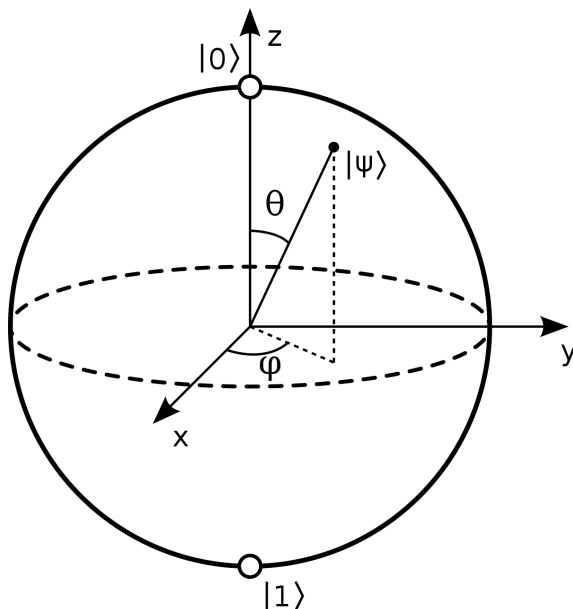


Figure 2.5. Bloch Sphere

There are infinitely many points on the Bloch sphere. A quantum bit can be in one of

an infinite number of states. We can store an unlimited amount of information using one qubit. However, this is not the case. When measuring the state of a qubit, we can find one of two states: $|0\rangle$ or $|1\rangle$. We can extract only one bit of information from a qubit. If we could get many identical copies of our qubit and measure the state of each copy, then with probability $|\alpha|^2$ we would find a qubit in state $|0\rangle$, and with probability $|\beta|^2$ in state $|1\rangle$. Numbers $|\alpha|^2$ and $|\beta|^2$ can take on infinitely many values. Thus, we would receive an infinite amount of information encoded in one qubit. To do this, we would have to, in the beginning, get many copies of our qubit. However, there is a theorem on the impossibility of cloning a qubit in an unknown state. This theorem will present in the following sections. So, only one bit of information we can get from one qubit.

2.3.2.2. Quantum entanglement

Quantum entanglement is a quantum physical phenomenon during which the quantum states of two or more objects depend upon one another. This interdependence persists even if these items are spaced apart in space beyond any known interactions. It logically contradicts the principle of locality. We can get a pair of photons that are in an entangled state. When measuring the spin of the first particle, if its helicity turns out to be positive, so the helicity of the second particle turns out to be negative and vice versa.

Quantum entanglement is, on the one hand, impossibility to represent a state vector of the quantum system as a direct product of state vectors of its parts, and, on another hand, it is the interdependence of parts when they behave as a single whole. We cannot independently describe the quantum state of each part from each other.

A quantum system with two different states $|0\rangle$, $|1\rangle$, can carry 1 bit of information. Photons, atoms, ions, atomic nuclei can act as a qubit. Spin is the proper angular momentum of an atom is a nucleus, an ion, or a photon which is defined as the vector sum of spins of elementary particles that form a system of orbital connections that move within the system.

According to the first postulate of quantum mechanics, the wave function fully describes the state of a quantum system. However, sometimes quantum systems cannot assign their wave functions, but only one for all. Such a state is called entanglement. Quantum entanglement allows us to bind qubits that are at an infinite distance from each other in such a way that changing one of them instantly affects the state of the others. This

phenomenon is used to bind qubits together and is of great importance in the realization of quantum teleportation.

Quantum teleportation is a transfer of a quantum state over an unlimited distance. The initial state is irreversibly destroyed and exactly reconstructed at the endpoint. One option of teleportation application in practice is the construction of ultra-secure communication networks. A message transmitted through the quantum network will reach only that addressee, who possesses a properly entangled photon, which will allow this message to receive and read.

Entangled states are at the heart of the quantum informatics paradigm, and their implementation is one of the most challenging tasks in building quantum computers. This task is workable for a short time. Nowadays, quantum entanglement is a familiar physical entanglement, ranging from zero to one.

2.3.2.3. Quantum superposition

Superposition is the tool of operations in a quantum computer, and it provides exponential growth of the computational power in it. The probability function $|\psi\rangle$ can represent the qubit superposition, which depends on the amplitude of the qubit in the Hilbert space α and β . The phenomenon of qubits which can take any value between $|0\rangle$ and $|1\rangle$ called superposition and exists only in quanta. Quanta is a tiny object, which can be any object that exhibits quantum behavior, such as a photon, molecules, atoms, and subatomic particles.

Superposition is the general expression of any state in terms of substates that make up for it. We can bring a state that is not in a superposition into a superposition with the Hadamard gate. It is one of the significant features of quantum technologies.

A qubit in superposition collapses into one of two deterministic states (0 or 1) when measured. The state probability 0 or 1 is determined by the superposition of the qubit. If a qubit is in equal superposition, it is half in state 0 and a half in state 1. When measured, a qubit has a 50% probability of going to state 0 and an equal probability of going to state 1. If a 75% qubit goes to state 0 and 25% goes to state 1, in 100 measurements the qubit will go to state 0 about 75 times and state 1 about 25 times. Because of the presence of superposition, n qubits can be in 2^n states simultaneously, while n classic bits are always in only one state. As a result, when performing operations on qubits, we change

$2n$ states at once instead of one in a classical computer. It provides quantum parallelism of calculation, which makes it possible for a quantum computer to solve problems of exponential complexity class in polynomial time. Such problems include, for example, problems of the integer factorization (Shor's algorithm) and the problem of finding a solution to the equation: $f(x) = 1$, where f is a Boolean function of n variables (Grover's algorithm).

2.3.3. Basic gates

The process of qubits performs logical operations in quantum computers. It breaks them down into a discrete set of time-sequential quantum logic operations. Each quantum gate produces a unitary transformation with selected qubits in a fixed time interval. A quantum gate performs reversible operations, and from this perspective, a classical reversible computer is an analog of a quantum computer. One of the prime conditions for building a quantum computer is a universal collection of quantum gates. Quantum logic gates are examples of conditional quantum dynamics. They could serve as building blocks for general quantum information transmission systems. Any single qubit gate operation can be represented as a rotation of the vector characterizing the state of a qubit to another point of the sphere.

The basics of building quantum circuit diagrams as follows:

- Time on a quantum diagram moves from left to right.
- Each qubit corresponds to a single horizontal line.
- Squares usually show gates. Letters or other symbols in this square show the type of gate. There are exceptions to this rule: these are qubit gates, which have classical analogs, for example, the NOT gate.
- Some gates may correspond to several diagram elements (for example, the NOT gate).
- Because of measuring the qubit, all superpositions collapse, the quantum properties of the qubit disappear, and it turns into an ordinary bit. Therefore, we can assume that the measuring element (shown below) receives a qubit as input and outputs a classic bit.

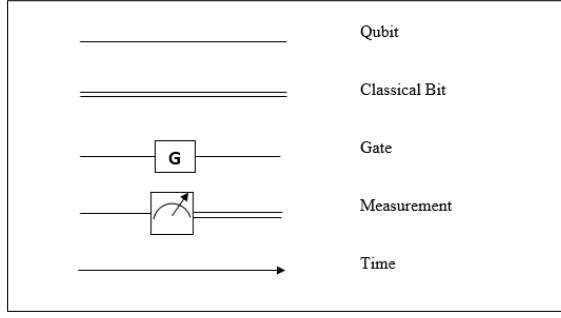


Figure 2.6. Notations of Quantum Circuits Elements

One-qubit operations describe the state of a single qubit, and two-qubit operations in the quantum algorithm represent the interconnection of one qubit (control qubit) with another (target qubit). There can also be multiple qubit operations to form a quantum register. The connection of qubits requires physical interaction between them. Quantum gates are implementing this connection. These gates transfer qubits from one state to another, which is working with superpositions. The most famous gates are Hadamard gate, Pauli gates, SWAP gate, Controlled NOT, Toffoli gate.

2.3.3.1. Single qubit gates

Single qubit gates are naturally the simplest. The operation performed by any single qubit gate can be represented as a rotation of the vector characterizing the qubit state to another point of the Bloch sphere.

The Hadamard gate is crucial because it can create a superposition of the states $|0\rangle$ and $|1\rangle$. Hadamard gate acts on $|0\rangle$ or $|1\rangle$ qubits and transforms them as follows;

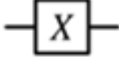
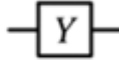
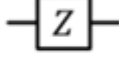
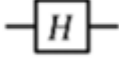
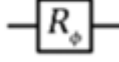
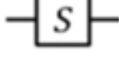
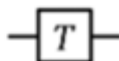
$$|0\rangle \rightarrow |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}; |1\rangle \rightarrow |+\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (2.8)$$

The Pauli-X gate is very similar to the classical gate NOT. It converts $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. This operation is equivalent to rotating the vector on the Bloch sphere around the x -axis by π radians (or 180°).

$$|\psi'\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2.9)$$

The Pauli-Y gate expectably corresponds to rotating the vector around the y -axis by

Table 2.1. One Qubit Gates

Name	Matrix Representation	Symbol
Pauli-X	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	
Pauli-Y	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	
Pauli-Z	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	
Hadamard H	$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	
Phase Shift, R_ϕ	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$	
Phase S, $\frac{\pi}{4}$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$	
Phase T, $\frac{\pi}{8}$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$	

π radians. This operation turns the vector $|0\rangle$ into $i|1\rangle$ and $|1\rangle$ into $-i|0\rangle$.

$$|\psi'\rangle = -i\alpha|0\rangle + i\beta|1\rangle \quad (2.10)$$

The Pauli-Z gate is a specific case of the phase shift R_ϕ gate when $\phi = \pi = 180^\circ$. It corresponds to the rotation of the vector around the z -axis by π radians. It leaves the vector $|0\rangle$ unchanged and converts $|1\rangle$ to $-|1\rangle$.

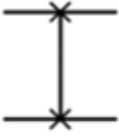
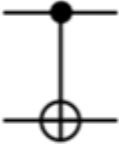
$$|\psi'\rangle = \alpha|0\rangle - \beta|1\rangle \quad (2.11)$$

The phase shift gate represents a general operation that has many useful applications. Its most common variations are the $\frac{\pi}{4}$, $\frac{\pi}{8}$ phase shift gates and the Pauli-Z gate, for which the φ parameter is equal to $\frac{\pi}{2}$, $\frac{\pi}{4}$, and π respectively.

2.3.3.2. Multiqubit gates

Multiqubit gates perform operations on two or more qubits.

Table 2.2. Multiqubit Gates.

Name	Matrix Representation	Symbol
SWAP	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	
CNOT	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	
Toffoli (CCNOT)	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$	
Fredkin gate (CSWAP)	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	

One of the simplest examples is the SWAP gate. The SWAP gate swaps two input

qubits. For example,

$$SWAP|0\rangle|0\rangle = |0\rangle|1\rangle$$

$$SWAP|0\rangle|1\rangle = |1\rangle|0\rangle$$

Another class of multiqubit gates is the so-called controlled gates. Any controlled gate has at least one control and one controlled qubit at its input, and the gate will operate on the controlled qubit only if the control qubit is in a specific state.

The CNOT gate is a multiqubit controlled gate. There is at least one control and one target qubit at the input of any controlled gate, and the gate will operate on the controlled qubit only if the control qubit is in a state. The CNOT gate does not change the target qubit value if the control qubit is 0 and reverses it if it is 1.

$$CNOT|11\rangle \rightarrow |10\rangle$$

$$CNOT|01\rangle \rightarrow |01\rangle$$

The Toffoli gate (CCNOT) is a universal controlled reversible gate with three inputs and outputs, proposed by Thomas Toffoli in 1980. It was proved that using only this gate. We can build any reversible logic circuit, for example, an arithmetic device or a processor. It is also a well-known quantum gate in the construction of reversible circuits of quantum computers.

The Toffoli gate is similar in principle to the CNOT. It has three inputs and three outputs. If the first two inputs are equal to one, then the last bit is reversed. Otherwise, all inputs are fed to the output unchanged.

$$CCNOT|110\rangle \rightarrow |111\rangle$$

$$CCNOT|101\rangle \rightarrow |101\rangle$$

The Fredkin gate (CSWAP) is a computational circuit useful for reversible computation designed by Edward Fredkin. We can build any logical or arithmetic operation entirely from Fredkin gates because it is versatile. The Fredkin gate is a three-input,

three-output circuit or device that transfers the first bit unchanged and swaps the last two bits if the first bit is 1.

$$Fredkin|000\rangle \rightarrow |000\rangle$$

$$Fredkin|101\rangle \rightarrow |110\rangle$$

$$Fredkin|110\rangle \rightarrow |101\rangle$$



3. MATERIAL AND METHODS

3.1. Introduction to Quantum Cryptography

Classical cryptography today reliably ensures the integrity and confidentiality of data. Even a powerful supercomputer will probably take hundreds or even thousands of years to solve the complex mathematical problems on which it is based. But with a large-scale quantum computer can solve a similar task in a few days or even hours. It evidences this by the results of a study conducted by American scientist Peter Shor at the Massachusetts Institute of Technology back in the mid-90s of the twentieth century.

Besides classical cryptography based on mathematical algorithms, there is quantum cryptography. Quantum cryptography is a method for protecting communications that are implemented through the phenomenon of quantum physics. Quantum cryptography transmits and received the encryption key using objects of quantum mechanics. These objects can be photons, that is, elementary particles of light. Eavesdropping on the transmission is nothing more than measuring the properties of objects. Any device with which a third party tries intercepting data will inevitably affect the photon states. It will corrupt the key. Dedicated fiber-optic lines can transmit photons, and it will require special encryption devices at both ends of such a line. The disadvantage of quantum cryptography is that it requires many infrastructure costs. Simultaneously, keys can be transmitted only for a limited distance. The speed of their generation is low, and the photons' transmission is affected by a lot of external factors.

Quantum cryptography is an interdisciplinary field of knowledge, technology, and engineering that solves providing legitimate user problems with identical random sequences of characters through the quantum states transmission. Such sequences, which are the basis for cryptographic keys, are used to encrypt private information. It is a relatively new research area that allows us to apply the quantum physics effect to create secret data transmission channels. From a purely perspective, this direction cannot be called a section of cryptography. Likely, technical methods of information protection should attribute it since quantum cryptography mainly uses material media properties. It also confirms because of physical engineers achieve progress in this field, not mathematicians and cryptographers.

Quantum cryptography, as a science, began in 1984, when the first QKD protocol, called BB84, was developed. The main advantage of quantum cryptographic protocols

over classical ones is a strict theoretical justification of their stability. If in classical cryptography stability is reduced to assumptions about the computational capabilities of an eavesdropper, in quantum cryptography, an interceptor can take all actions allowed by laws of nature, and he will not learn a secret key, and the key will remain undetected.

The property of collapse of a wave function is the prime property of quantum mechanics for quantum cryptography, so when any quantum mechanical system is measured, its initial state changes. This idea leads to the analogy that it is impossible to distinguish quantum states from their non-orthogonal set. It is this property that is used to justify the secrecy of quantum cryptography. When trying to eavesdrop on transmitted states from their non-orthogonal basis set, the eavesdropper necessarily introduces an error in them, through which additional interference on the receiving side can detect it. Hence, legitimate users, based on the observed error size on the receiving side, decide on the possibility of secret key distribution. When the value of this error approaches the critical value (depending on the protocol), then the transfer of key becomes impossible.

Quantum cryptography technology is based on a fundamental property of nature in physics on the Heisenberg uncertainty principle. According to this principle, it is impossible to measure the coordinates and momentum of a particle simultaneously. Also, it is impossible to measure one parameter of a photon without distorting the other. It is possible to design and create a communication system that can detect eavesdropping using quantum phenomena. It ensures this idea because trying to measure interrelated parameters in a quantum system will cause a violation of the rule, destroying the original signal so legitimate users can identify the activity of the interceptor by the noise level in the channel. Sending and receiving information is always performed by physical means, for example, using electrons in an electric current or photons in fiber-optic communication lines. We can consider eavesdropping as the measurement of a definite parameter of physical objects, in our case, information carriers.

The term quantum cryptography is well established and is used along with analog – quantum communication. Quantum cryptography uses a fundamental feature of quantum systems, which comprises the impossibility of accurately detecting the state of such a system that accepts one of the sets of several non-orthogonal states. It follows from the fact that it is impossible to distinguish between such states in one measurement. For example, it is impossible to determine the length of a segment in space only by its projection on one

axis. It is impossible to makeover one measurement because, after the first measurement, the system unpredictably changes its state. Also, in quantum mechanics, the theorem on the prohibition of exact cloning of systems is valid. This theorem makes it impossible to make several copies of the system under study and then test them.

Quantum cryptography systems have several fundamental features. First, it is impossible to say beforehand that the receiver will correctly receive which of the transmitted bits since this process is probabilistic. Second, an essential feature of the system is using low-energy pulses, ideally comprising one photon. It reduces the transmission speed over the same channel compared to the usual level of optical signals. For these reasons, the quantum communication channel is of little use for the transmission of user data. It is more suitable for generating symmetric cipher keys, which users will use to encrypt the transmitted data.

The main research activity in the field of quantum cryptography is carried out in several directions:

- Development and improvement of technical characteristics of devices involved in the implementation of quantum protocols;
- Development of quantum protocols based on the corresponding principles of quantum mechanics.

Based on this, we can conclude that quantum cryptography is an applied field of quantum mechanics. However, using quantum cryptography as a modern means of protecting information requires solutions that provide functionality no worse than existing classical methods. But the possibility of replacing key distribution and encryption methods with security based on complexity theory approaches with devices that support quantum cryptographic functions raises fair questions about cost-effectiveness and ease of replacement.

3.2. Idea of Quantum Cryptography

Information is the scientific concept and practical direction that study the transmission processes, processing, and storage of various data. Examples usually illustrate the essence of the information concept. The information concept refers to fundamental concepts. Besides the well-known and widely used methods of its transmission, it can also be

encrypted in the states of quantum systems, for example, in the polarization states of single photons and transmitted through the physical communication channel. It is the case, for example, when distributing cryptographic keys using quantum cryptography methods.

The main idea of quantum cryptography is to transmit information, thus that anyone cannot intercept it. And this should be not possible not because the encryption algorithms are too complicated and not because the attacker does not have high enough computing power. We build a data transmission system in such a way that its hacking contradicts the laws of physics.

The crucial question is how to do this effectively. Since we are not using a perfect system, but physical communication lines—optical fiber or open space. On the way to the receiver, many factors that can destroy it can affect a photon. We are interested in a data transfer speed between such systems and the distance over which we can spread the nodes. These are the development of the main items of different approaches, ideas, and principles of the construction of quantum cryptography systems: efficient use of data capacity, throughput, and decrease the number of repeaters, the highest level of security and safety channel. At the heart of quantum cryptography is the thesis that an attacker can try to do anything, use any tools and equipment, but he should not intercept the data. However, the existing technical solutions have already been corrupted by the attackers.

If we are running some system that an attacker might compromise, we need to transfer data in a trusted way. These can be, for example, decisions related to finance, trade secrets, government tasks. Quantum cryptography and quantum communication solve the problem that nature prohibits intercepting restricted information. Signals are transmitted over communication lines, not in the classical form, but with the help of a single photon stream. A photon cannot be divided or measured, copied, or secretly set aside. Because of this, it is destroyed and does not reach the receiving party.

The degrees of freedom of a single-photon electromagnetic field—phase frequency, polarization, and time interval are used to encrypt the original random sequence of symbols. Photons are the most convenient quantum mechanical objects for quantum cryptography since they propagate at high speed and have a set of degrees of freedom for encoding. Also, telecommunication technologies allow using some classical methods for generating, transforming, and controlling single-photon states.

3.3. The Main Directions of Development of Quantum Cryptography

In quantum cryptography, it distinguishes two main directions of the development of key distribution systems.

The first direction is based on the encrypting of the quantum state of a single particle. It is based on the principle that it is impossible to distinguish accurately two non-orthogonal quantum states. The security of the first direction based on the no-cloning theorem. Because of the quantum mechanics' linearity and unitarity, it is impracticable to create an identical copy of a quantum state without affecting the initial state. A quantum state is an information resource that contains information about the statistics of various measurements over a given quantum system. The information in the quantum state has qualitative differences from classical and is therefore called quantum information. The most striking difference between classical information quantum information is the impossibility of copying an arbitrary unknown quantum state. The no-cloning theorem forms the mathematical basis for the reliability of all modern quantum cryptography protocols.

The second direction of development based on the effect of quantum entanglement. Two quantum techniques are in an exceedingly state of correlation. So, the measurement of the chosen value performed on one system will determine the result of measuring this value on the other. No one of the entangled systems is in a definite state. Therefore, the entangled state cannot be written as a direct product of the system states. Two particles state with spin 1/2 can provide as a case of an entangled state:

$$|\psi_0\rangle = \frac{|0\rangle - |10\rangle}{\sqrt{2}} \quad (3.12)$$

A measurement done on one of the two subsystems gives the states $|0\rangle$ or $|1\rangle$ with corresponding possibility. The state of the other subsystem will be the opposite. For example, the state will be a $|0\rangle$ if the measurement result on the first system is $|1\rangle$, and vice versa. The basic protocol for QKD based on the quantum entanglement effect is the EPR (Einstein-Podolsky-Rosen) protocol. Its second name is E91.

The basic principles of these two directions formed the basis for all QKD protocol development. The main task of cryptography is to encrypt data and authenticate the sender. It is easy to accomplish if both the sender and receiver have pseudo-random sequences of bits called keys. Before the exchange begins, each of the participants must receive a key.

And they should perform this procedure with the highest level of confidentiality so that no third party can access part of this information.

The problem of secure key forwarding can be solved using QKD. The security of the method based on the inviolability of quantum physics. An attacker cannot divert part of the signal from the communication channel. It is impossible to separate the electromagnetic quantum into parts. Any attempt by an attacker to interfere with the transmission process will produce an extremely high error rate. Reliability in this method is higher than in asymmetric algorithms. Here, the key can be generated during transmission over a completely open optical channel. The data transfer speed with this technique is not high, but it is unnecessary to transfer the key. Quantum cryptography can replace the DH algorithm, which is now often used to send secret encryption keys over communication channels.

3.4. Quantum Protocols

A protocol is a set of actions performed in a sequence by two or more legitimate entities to achieve a defined result. Several key distribution protocols based on discrete quantum states are known. They can divide into two groups. The first one includes quantum cryptography protocols that operate with non-orthogonal quantum states. The most famous of them are BB84, B92, SARG04. The second is protocols based on the so-called entangled quantum states and verification of the fulfillment of Bell's inequality. Entangled states are states of a component system whose wave function cannot be expressed in wave functions in terms of subsystems. In other words, they fully define such a component system. A wave function describes it, and the von Neumann entropy is zero. And the states of subsystems are indeterminate in full. They are in a mixed state, and their entropy reaches a maximum value. The best-known protocol for the entangled state is the Ekert protocol or E91.

3.4.1. QKD

Currently, quantum cryptography includes several sections: QKD protocols, quantum secure direct communication protocols, quantum message authentication, and quantum digital signature. In recent years, among these areas, much attention has been paid to

QKD. There are already experimental commercial samples of such systems. Hence, a detailed analysis of the reliability of various QKD protocols is of paramount importance.

QKD is a system that can distribute a key between two subscribers if they have access to a quantum transmission and an open conventional channel. A quantum communication channel is a channel for transmitting individual quantum particles, for example, photons. An open channel allows us to authenticate the sender of the message. Bits transmitted over a quantum channel are used to create a secret key, which then encrypts messages transmitted over any open channel.

The main advantage of QKD over conventional systems is the fundamental ability to detect an eavesdropping agent, which, for quantum physics laws, is required to perturb the states of transmitted quantum objects during eavesdropping. Key distribution is because Eve cannot extract any information from the quantum states passed from Alice to Bob without breaking their state. First, according to the no-cloning theory, Eve cannot duplicate the quantum state prepared by Alice. Second, it is impossible to identify between two non-orthogonal quantum states because a signal or noise accompanied the extraction of information. Alice and Bob get an upper estimate of any noise and eavesdropping by checking the transmitted state for violations.

It can separate QKD protocols:

- By the encoding method
- According to the quantum mechanical principles underlying this protocol security.

QKD protocols include three execution steps:

1. Generation of primary keys through quantum states transmission over the quantum channel and further measurements on the receiving side. The measurement result is a string of bits that differ from the original transmitted sequence of Alice. After receiving the measurement results, it exchanges information through an open conventional communication channel. At the end of the first stage, legitimate users (Alice and Bob) have a primary key.

2. Coordination of information (error correction) through the exchange of classical information through an conventional channel (for example, the Internet). The fundamental difference between this procedure and the usual error correction systems in classical information theory is that all information transmitted over an open communication channel

is known to the eavesdropper. It carries the correction out among spatially remote users.

3. Increased the secrecy of the cleared key. After correcting the error and discarding some bits, it will leave a shorter length bit string for legitimate users. Compression can reduce the eavesdropper's information to an exponentially small value for the selected secrecy parameter (hashing by universal hash functions). QKD is a statistical analysis for the communication and registration of quantum states, with subsequent processing of measurement results. The final product is a shared key between the transmitting and receiving parties, which is a random sequence of bits long and which is unknown to the third-party.

Any protocol comprises the following stages: preparation, transmission, measurement of quantum states, agreement of bases, and analysis of measurement results. After these stages, participants have a bit of string—the raw key. Receiver's string contains errors. If the equipment does not have its noise, then the percentage of errors is determined by the intrusion of Eve into the transmission channel. It is impossible to determine errors introduced by the eavesdropper from errors of the equipment, so all errors applied to the eavesdropper actions.

3.4.2. Prepare and measure protocols

Quantum cryptographic systems based on the no-cloning ability of an unknown quantum state include the cryptographic techniques BB84, B92 and their various modifications and generalizations, for example, SARG04. This resource is used to form a non-compromised channel for transmitting information that serves to generate a cryptographic key. The following brief descriptions of some of them illustrate the simple features of such protocols. General to them is PRNG.

3.4.2.1. BB84 protocol

For the first time, Wiesner expressed the idea of using quantum particles to secure information in 1970. He came up with the idea of a quantum security banknote. This idea did not find implementation. Then Wiesner shared his idea with Bennett. A few years later, it changed into a data protecting technique called quantum cryptography. In 1984, Bennett worked with Brassard to refine Wiesner's idea of transmitting enciphered messages using quantum technology. They proposed using quantum channels to transfer

one-time keys, and the length of such keys had to be corresponding to the message length. It allows encrypted data to be transmitted in the OTP mode.

A BB84 is based on photon polarization ideas. The key comprises bits that are transmitted as photons. The BB84 is one of the main protocols, the secrecy of which has been most studied. This encryption method provides mathematically proven cryptographic strength. One of the primary tasks of quantum cryptography is the secure distribution of keys. The key is generated and transmitted using photons brought to a definite quantum state.

As a quantum particle for information transmitting, we use a photon. We can use the hardware to get it and can measure its parameters. However, the data transfer requires an encrypting method that would produce a combination of zeros and ones. As already mentioned, unlike classical technology, where zeros and ones are encrypted as different signal potentials or directional pulses, such encoding is impossible in quantum systems. Therefore, we need a photon parameter that can be set during its generation and then measured with the required confidence. This parameter is the polarization, which can be considered as the orientation of the photon in space.

The photon can be polarized at angles of 0, 45, 90, 135 degrees. By measuring the photon, we can identify only two commonly perpendicular states or bases:

- Rectilinear bases - the photon is polarized vertically or horizontally.
- Diagonal bases- the photon is polarized at angles of 45 degrees or 135 degrees.

Table 3.3. The Polarization Basis

	0	1
Rectilinear	—	
Diagonal	/	\

Thus, it is impossible to identify a horizontal photon from a photon polarized at an angle of 45 degrees. These properties of the photon established the basis of the BB84 protocol. It transmits information in its application through polarized photons, as a zero or one.

In the BB84 protocol, a photon with a polarization type orthogonal to the transmitted photon is recorded at the receiving end of the quantum communication line. It is possible

to prove the protocol secrecy using fundamental entropy uncertainty relations. This is the uniqueness of the protocol with a strictly single-photon source. These ratios allow us not to iterate over all eavesdropper attacks on the transported key and not to present an optimal attack. Optimality is in the maximum's sense of eavesdropper information about the key for an observable error on Bob's receiving side.

Key generation steps:

The first stage is called primary quantum transfer. Alice generates photons with random polarization (0, 45, 90, or 135 °). For example,



Figure 3.7. Photons generated by Alice

Bob, having received these photons, applies a diagonal (X) or vertical (+) polarization method to each of them, choosing it at random.



Figure 3.8. Bob's chosen polarization methods

Bob records the measurement results:



Figure 3.9. Results of Bob's measurements

After that, he tells Alice through an open channel the methods has chosen for each photon to measure the polarization. In response, Alice also uses an open channel to tell Bob whether he has chosen the correct or incorrect view for each photon.



Figure 3.10. Correct and incorrect types of measurements

Information about incorrect measurements is discarded, and the remaining data is converted to bits. For binary 0, photons with horizontal or 45° polarization are taken, and for binary 1, photons with vertical or 135° polarization are taken.

	1		0	0	1		0
--	---	--	---	---	---	--	---

Figure 3.11. The resulting sequence

This sequence is the result of the first stage.

Table 3.4. BB84 Protocol Example

Photons generated by Alice	/	\	—	—	/		/
Bob's chosen polarization methods	+	×	×	+	×	+	×
Results of Bob's measurements	—	\	/	—	/		/
Correct types of measurements		✓		✓	✓	✓	✓
The resulting sequence		1		0	0	1	0

At the next stage, the possibility of interception of information is evaluated. To do this, Alice and Bob randomly reveal and compare bits over an open channel. After this disclosure, the bits are discarded. If an interception is detected, the existing data is discarded, and the whole process starts over. If not, the polarization remains the same.

According to the uncertainty principle, if Eve measures the photon polarization, it will introduce an error. On average, noise contributes to an error percentage, which will increase if intercepted. In this case, Alice and Bob will know that there was an interception of photons

3.4.2.2. B92 protocol

The B92 protocol is one of the first QKD protocols that was introduced in 1992 by Charles Bennett. The B92 protocol is based on the principle of uncertainty. A feature of the protocol is the use of two non-orthogonal quantum states.

If there is no interceptor action and interference in the channel in BB84 protocol, the probability of an error on the receiving side before the basis negotiation is 25 %. It causes using a configuration of two pairs of basis vectors. The purpose of the B92 protocol is to allow flexibility in changing this parameter depending on additional conditions, such as the channel length or channel quality. It can sometimes help to achieve a higher data transfer rate.

At each step of the protocol B92, Alice sends Bob one of two non-orthogonal states $|\psi_0\rangle, |\psi_1\rangle$, where $\langle\psi_0|\psi_1\rangle = \cos\eta$ is the main parameter of the protocol. Bob, on his side, produces a "measurement with three outcomes."

$$M_0 = \frac{|\psi_1^\perp\rangle\langle\psi_1^\perp|}{1 + \cos\eta} = \frac{I - |\psi_1\rangle\langle\psi_1|}{1 + \cos\eta} \quad (3.13)$$

$$M_1 = \frac{|\psi_0^\perp\rangle\langle\psi_0^\perp|}{1 + \cos\eta} = \frac{I - |\psi_0\rangle\langle\psi_0|}{1 + \cos\eta} \quad (3.14)$$

$$M_? = I - M_0 - M_1 \quad (3.15)$$

When applying such a measurement over the specified states, the first two outcomes will correspond to the exact results in the absence of errors, while the non-relevant (inconclusive) outcome “?” does not provide useful information about the transmitted state. Therefore, such results are discarded.

After transmitting all the messages, Alice, and Bob, just as they did in the BB84 protocol, consistently reveal part of their bit sequences and estimate the number of errors. If they are greater than a definite threshold value, it interrupts the protocol execution. Else, the full secret key is extracted from the remaining part of the bit strings.

The most important property of the B92 protocol is a parameter n . This parameter is the angle between the signal states. The closer this angle is to $\frac{\pi}{2}$, the protocol is too simple to signal to forward using orthogonal states. The data transfer rate increases, but their resistance against interception decreases. When using small values of n , there is a high probability of obtaining incompatible outcomes, which reduces the data transfer rate, but significantly complicates the eavesdropper situation.

The protocol uses photons polarized in two different directions to represent zeros and ones ($|\phi_0\rangle$ and $|\phi_1\rangle$, $\langle\psi_0|\psi_1\rangle \neq 0$). Photons polarized along the $+45^\circ$ direction carry information about a one bit, photons polarized along the 0° (V) direction - about the zero bit.

Algorithm of the B92 protocol:

Alice sends photons polarized in the 0° and $+45^\circ$ directions, representing zeros and ones. Moreover, the sequence of photons sent by Alice is randomly oriented. Bob receives photons through filters oriented at an angle of 90° and 135° (-45°). At the same time, if the photon transmitted by Alice is analyzed by Bob using a filter oriented at an angle of 90° to the transmitted photon, then the photon will not pass through the filter. If this angle

is 45° then the photon will pass through the filter with a probability of 0.5. Bob analyzes the photons received by it to determine the polarization, using a randomly selected one of two non-orthogonal bases “+” or “X.”

If Bob analyzes a photon sent by a filter with an orthogonal polarization direction, he cannot determine what value this photon represents. One corresponds to a photon that does not pass, or zero corresponds to a photon that does not pass with a probability of 0.5. If the polarization directions between the sent photon and the filter are non-orthogonal, Bob can determine that a photon corresponding to 0 is received. When the photon was received successfully, the next bit of the key is encoded with 0 (if the photon was received by a filter oriented at an angle of 135°), or 1 (if the photon was received by a filter oriented in the H direction).

Table 3.5. B92 Protocol

Alice's binary signal	0	1	1	0	1
Alice's polarizing code		/	/		/
Bob's polarizing code	\	\	—	—	—
Bob's binary signal	0	0	1	1	1
The result obtained by Bob	—	—	+	—	+

In the first and fourth columns of the Table 3.5, the transmission and reception polarizations are orthogonal, and the result will be absent. In columns 2, 3, and 5, the binary bit codes are the same, and the polarizations are not orthogonal. For this reason, there is a 50% chance of a positive result in any of these cases. The table assumes that successful photon detection occurs for the occasion presented in columns 3 and 5. It is these bits that become the first bits of the transmitter and receiver secret key. Hence, the minimum number of photons Bob can take is $n=2/5$. Because of transmitting such a key, Bob will correctly detect approximately 40% of the photons.

Bob can tell Alice through an open communication channel, which 40 photons out of every 100 he received. This information will serve as the key to the new message. It is possible to transmit data over an open communication channel only about which photons were received in order, without naming the filter states, and got polarization values, so the eavesdropper does not learn information about the key. Alice can send messages to Bob encrypted with this key. To detect the removal information case in this protocol, error control is used, similar to error control in the BB84 protocol.

In the B92 protocol, a legal receiver can register a photon with a nonzero probability. Though, its analyzer is oriented orthogonally to the sender polarizer, which is impossible in the absence of unauthorized access. The crucial difference between the BB84 and B92 protocols is that even in the absence of unauthorized data acquisition in the channel, the probability of correct registration of the photon polarization type in the B92 protocol is two times less than in the BB84 protocol.

3.4.2.3. SARG04 protocol

The SARG04 protocol aims to improve the reliability of the main protocols in quantum cryptography (BB84 and B92) against PNS attacks with weak coherent pulses instead of single-particle signals. SARG04 is the first quantum protocol that has opened the possibility of using the claimed key distribution methods in practice. As the analyses showed, SARG04 ceases to be secret only when the interceptor can block all one-, two- and three-photon parcels. It means that the QKD is possible at a greater distance than using the BB84 protocol since the length of the communication line depends on the average number of photons in the message.

The first stage of the SARG04 protocol is the same as in BB84. In the second step, Alice and Bob determine the bases. But Alice does not immediately communicate her basis to Bob. She declares a pair of non-orthogonal states that she used to encode the data. If Bob used the right basis, then he will get the correct message. If he chose it incorrectly, then he will not determine the bit sequence correctly. Using multiple photons led to the appearance of PNS attacks. Eve splits off one photon or a few photons from each bit transfer for measurements. It allows Eve to receive photons without breaking Bob's message. The SARG04 protocol is resistant to PNS attacks since Alice does not immediately report her basis. Alice shows a pair of non-orthogonal states in which they encode a bit. If Bob has chosen the correct basis, he will find that he has measured one of these two states that Alice passed on. Otherwise, the bit is discarded. It means that Eve does not know which basis they used for transmission, even after Alice and Bob have chosen the basis for decryption.

Now let's look at the work of the SARG04 protocol.

Alice randomly sends one of four states:

$$|\alpha\rangle_+ = |\rightarrow\rangle, |\beta\rangle_+ = |\uparrow\rangle, |\alpha\rangle_x = |\nearrow\rangle, |\beta\rangle_x = |\searrow\rangle$$

Here, the encrypted bit is the status basis. Bob accepts them just like in BB84. Further, at the step of comparing bases, Alice publicly declares one of four pairs of non-orthogonal states:

$$|\alpha\rangle_+, |\beta\rangle_x; |\alpha\rangle_x, |\beta\rangle_+; |\beta\rangle_x, |\beta\rangle_+; |\alpha\rangle_x, |\alpha\rangle_+;$$

Let Alice send $|\alpha\rangle_+$ and declare a pair $|\alpha\rangle_+, |\alpha\rangle_x$ for certainty. One state in the pair is sent necessarily, and the other is chosen randomly from another basis. If Bob measure in the + basis, he could get an accurate result, but that result is equally likely for both bases of the pair. Bob will have to discard that value. If he took basis X, in which case a or b is equally probable, and got a, he again cannot distinguish them. However, if Bob measured in basis X and got b (probability of that is $\frac{1}{4}$), he realizes that the sent state is $|\alpha\rangle_+$. The correct basis would get a, but he got b, so X is the wrong basis). This modification makes it very difficult for Eve to conduct a PNS attack. She must block all pulses containing 1 or 2 photons and split where 3 or more.

SARG04 is vulnerable to LPA. Let Eve launch a bright flash of light into the communication line, then the light will get into the transmitting device and will be reflected from optical devices inside it. Thus, the pulse of light can get into the internal modulator and be modulated by it. By measuring the modulated pulse, Eve will get information about the modulator settings.

3.4.3. Entanglement based protocols

An example of a quantum cryptographic system based on two quantum resources (no-cloning theorem and entanglement) is E91.

3.4.3.1. E91 protocol

Artur Ekert proposed the E91 protocol in 1991. The second name of the protocol is EPR because it is based on the Einstein-Podolsky-Rosen paradox. The protocol aims to use, for example, pairs of photons created in asymmetric polarization states. The interception of one of the pair's photons does not bring Eve any information, nor does it signal to Alice and Bob that their conversation is being overheard. The E91 protocol differs from the BB84, B92, SARG04 protocol in that we get the key bits from a random process based on the properties of entangled quantum states.

An E91 cryptographic protocol allows legitimate users to get a secret key. The E91

protocol differs from the BB84 protocol in that the key bits are derived from a random process based on the properties of entangled quantum states.

The steps of the E91 protocol can be described:

1. The Alice generates N maximally entangled pairs of EPR photons. One photon from each pair she keeps for herself, the second sends to her partner Bob. The possible quantum states for these EPR pairs are

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A | \frac{3\pi}{6} \rangle_B - | \frac{3\pi}{6} \rangle_A |0\rangle_B), \quad (3.16)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(| \frac{\pi}{6} \rangle_A | \frac{4\pi}{6} \rangle_B - | \frac{4\pi}{6} \rangle_A | \frac{\pi}{6} \rangle_B), \quad (3.17)$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(| \frac{2\pi}{6} \rangle_A | \frac{5\pi}{6} \rangle_B - | \frac{5\pi}{6} \rangle_A | \frac{2\pi}{6} \rangle_B). \quad (3.18)$$

It can be written generally as

$$|\psi_n\rangle = \frac{1}{\sqrt{2}}(|0_i\rangle_A |1_i\rangle_B - |1_i\rangle_A |0_i\rangle_B). \quad (3.19)$$

From the formula, we can see that each of the three states encodes bits 0 and 1 on a unique basis.

2. Alice and Bob then perform measurements on their parts of the separated photon pairs using relevant instruments.

$$P_1 = |0\rangle\langle 0|, P_2 = | \frac{\pi}{6} \rangle\langle \frac{\pi}{6} |, P_3 = | \frac{3\pi}{6} \rangle\langle \frac{3\pi}{6} |. \quad (3.20)$$

3. Alice records the measured bits, and Bob writes their complement to 1. When Alice receives the polarization value 1, its partner registers the value 0 and vice versa. In this way, partners can always get identical pseudo-random code sequences. The results of measurements in which users preferred the same bases are used to create a raw key. For the rest of the results, Alice and Bob check Bell's inequality as a test for Eve's existence.

Experiments on implementing this protocol have recently begun. Their implementation became possible after obtaining sources of entangled pairs with high correlation and a long lifetime.

3.4.4. Quantum teleportation

Quantum teleportation is an unknown quantum state transmission over a distance using an EPR pair divided in space and divided between two participants and a classical communication channel. Quantum teleportation, in contrast to superdense coding, occurs in the absence of a quantum communication channel.

Teleportation is an ideal way of transmitting classified information, as well as:

1. The teleportation procedure does not violate the no-cloning theorem.
2. The transfer of quantum information from photon to photon can be carried out at an arbitrary distance (more than 144 km in open space, 102 km in an optical fiber).
3. Teleportation does not imply the transmission of information about the fact of its implementation.
4. If we do not measure Bell's states and confine us to projecting onto a fermionic state, then teleportation will be successfully carried out on average once in four attempts.

Quantum teleportation is the movement of a quantum state from one place to another without moving a physical particle. It is possible because of the previously discussed quantum entanglement between the sending and receiving locations over the classical communication channel.

Let's assume that there are two quantum systems, Alice and Bob. Alice wants to send a qubit state that shown in Equation 2.3 to Bob. Under the general principles of quantum mechanics and the no-cloning theorem, Alice cannot determine the coefficients α and β without destroying the qubit ψ and send their values to Bob so that he can make the corresponding qubit ψ himself. There should be a system C, which transmits entangled pairs of qubits to Alice and Bob.

Table 3.6. Quantum Teleportation

Alice's measurement results	Bob's qubit state	Bob's operations	Final state
00	$\alpha 0\rangle + \beta 1\rangle$	I	$\alpha 0\rangle + \beta 1\rangle$
10	$\alpha 1\rangle - \beta 0\rangle$	X	$\alpha 0\rangle + \beta 1\rangle$
01	$\alpha 0\rangle - \beta 1\rangle$	Z	$-\alpha 0\rangle + \beta 1\rangle$
11	$\alpha 1\rangle + \beta 0\rangle$	XZ	$\alpha 0\rangle + \beta 1\rangle$

The process of quantum teleportation is work as follows :

- Before the transmission starts, system C prepares and sends the vector in the en-

tangled state to Alice and Bob. The pair that C transmits is called the Bell pair. C performs a Hadamard operation on a qubit and then applies a CNOT operation for creating the Bell pair.

- Then, Alice performs reversible transformations on the state of the CA system, also performs measurements (with four results, which are two bits of classic information). The transformations are typical examples of logical operations used in quantum computing. First, Alice applies the CNOT operation to the CA system and then applies the Hadamard gate. Now, Alice can measure the CA system.
- Alice sends the measurement results: 00, 01, 10, 11 to Bob through the classical communication channel.
- Depending on the obtained result, Bob applies one of the unitary operators to his state: I, Pauli-X, Pauli-Y, Pauli-Z, which transforms the resulting state into Equation 2.3.

The scheme of quantum teleportation protocol shown in Figure 3.12.

One of the primary applications of quantum teleportation is quantum cryptography. The concept behind this technology is that a photon cannot be duplicated. So we can transfer information in this single photon, and no one can clone it. Whenever someone tries to learn something about this information, the photon's state changes or collapses. So, we will be notified of any attempt to get this information from third parties and can use the quantum teleportation methods for cryptography and information security purposes.

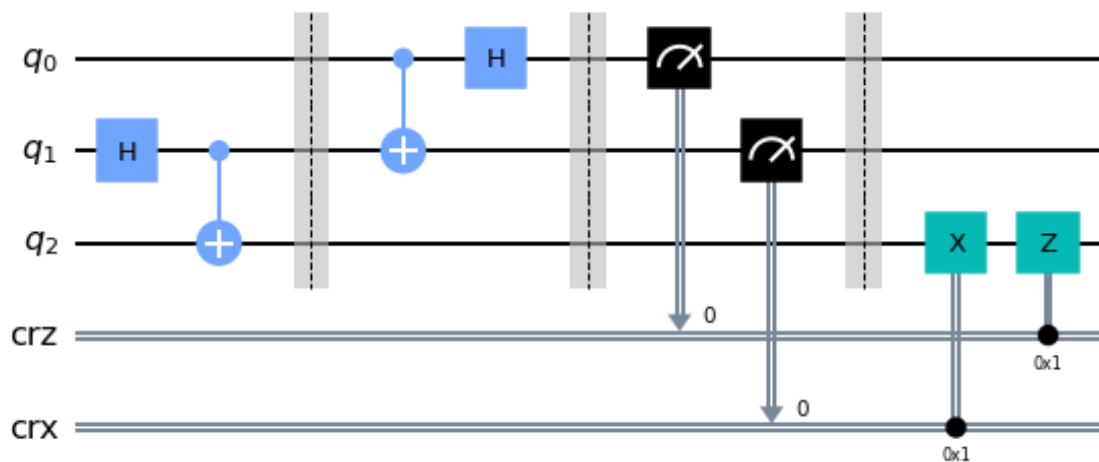


Figure 3.12. Quantum Teleportation Circuit

This technology has drawbacks. The first disadvantage is that it is impossible to create a copy of the photon. We can amplify a signal in an optical fiber. For the quantum case, since the amplification will be equivalent to some interceptor, it is impossible to amplify the signal. Also, in communication lines, it limits the transmission to about 100-150 kilometers. Unfortunately, long distances are impractical because the photons are lost in the fiber, and the speed is low. Hence, to solve this, we can put an intermediate server that will receive the information, decrypt and encrypt it again and pass it on. It is what the Chinese do, for example, when building their quantum cryptography network. The Americans use the same approach. Quantum teleportation is an alternative method that allows us to solve quantum cryptography problems and increase the distance of thousands of kilometers. And in this case, the same photon that is transmitted is repeatedly teleported. Many groups around the world are working on this task.

3.4.5. Superdense coding

Superdense coding is a method of transmitting a single qubit to encrypt two classical bits through quantum channel using the quantum entanglement phenomenon. Bennett and Wiesner proposed the superdense coding method in 1992. Then Mattle, Weinfurter, Kwiat, and Zeilinger implemented it in 1996.

Assume that Alice wants to transmit classical information to Bob using qubits instead of bits. Alice encodes a message with the qubit state, which she then sends to Bob. Bob extracts classical information by measuring the state of the qubit. We can assume that Alice will transmit only one classical bit since it cannot distinguish non-orthogonal states with certainty. Thus, using qubits instead of classical bits does not give any advantage in this case. If we assume that Alice and Bob have at their disposal the entangled state of a qubit pair (one for Alice, the other for Bob), it is possible to transmit not one but two bits of classical information, using still only one qubit. We can achieve a similar doubling of the efficiency of information transmission using quantum superdense coding. It is a quantum communication secure form. If Eve eavesdrops on Alice's qubit sent to Bob, all Eve gets is a part of the entangled state. Eve cannot get any information from Alice's qubit without access to Bob's qubit. A third party cannot eavesdrop on the data transmitted by superdense coding, and attempting to measure any of the qubits will cause that qubit's state to collapse and alert Bob and Alice.

An entangled state itself does not allow the transmission of information. The presence of such a state makes it possible to double the maximum amount of classical information transmitted from Alice to Bob if there is an ideal quantum communication channel between the systems, which allows any quantum state to be accurately transmitted. The entangled state acts as a catalyst for classical information transmission through a quantum communication channel. For clarity, think the systems of Alice and Bob, each of which has a qubit. There is an ideal quantum transmission channel between Alice and Bob. The maximum number of classical information that can be transferred from Alice to Bob is one bit and is got by encoding a bit into two orthogonal vectors, for example,

$$0 \rightarrow |0\rangle, 1 \rightarrow |1\rangle. \quad (3.21)$$

The superdense coding protocol based on a simple mathematical fact: all vectors of the Bell basis. (Equations 3.22, 3.23, 3.24, 3.25).

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) \quad (3.22)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B - |1\rangle_A \otimes |1\rangle_B) \quad (3.23)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B + |1\rangle_A \otimes |0\rangle_B) \quad (3.24)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) \quad (3.25)$$

Let there be a system C, which prepares and sends entangled states to Alice and Bob. After preparing the Bell state, system C sends the qubit described by A to Alice and sends the qubit described by B to Bob. Alice and Bob can be in distant places. It can take a long time between the entangled state preparation and separation and the rest of the process. By applying quantum gates to qubits locally, Alice can transfer the entangled state into any of the four Bell states.

1. If Alice wants to send Bob a 00, she applies gate I.
2. If Alice wants to send Bob a 01, she applies the Pauli-X gate.

3. If Alice wants to send Bob a 10, she applies the Pauli-Z gate.
4. If Alice wants to send Bob an 11, she first applies Pauli-Z, then Pauli-X gate.

Table 3.7. Superdense Coding

Intended Message	Applied Gate	Result
00	I	$\sqrt{2}(00\rangle + 11\rangle)$
10	X	$\sqrt{2}(01\rangle + 11\rangle)$
01	Z	$\sqrt{2}(00\rangle - 11\rangle)$
11	ZX	$\sqrt{2}(- 01\rangle + 10\rangle)$

After encoding, Alice sends her sequence of qubits ab to Bob. Bob already has a pair of entangled qubits in the Bell state $|\beta_{ab}\rangle$. After receiving the message, he should decrypt it. Bob will perform a CNOT operation using A as the control qubit and B as the target qubit to decrypt it. It will then perform Hadamard operations on the entangled qubit A.

3.5. Quantum Algorithms To Break Classical Cryptography

Classical algorithms involve a fixed sequence of rules or step-by-step operations. Therefore, quantum algorithms also mention the step-by-step execution procedures implemented on a quantum computer. All symmetric and asymmetric cryptographic algorithms are also working on a quantum computer. However, the term quantum algorithm is used for algorithms that consider quantum computing features (quantum superposition, quantum entanglement). All algorithms implemented on a quantum computer can be realized on a classical computer, too. All problems unsolvable with classical computers remain unsolvable with quantum computers. But the benefit of quantum computers is confirmed because some algorithms can be performed on them much faster than on classical computers.

Quantum algorithms are based on the following principles:

1. Reversibility of computations.

According to quantum mechanics, its laws are reversible in time, from which we can assume that quantum transformations should also be reversible in time. From the result of calculations, we can recover the original data.

2. Redundancy of calculations.

From the first principle to restore the original data, the output number must be equal to the input number.

3. Absence of cycles.

Calculations reversibility leads to the fact that in quantum transformations, there can be no periods and reverses. When executing a program, all operations are performed continuously.

4. Quantum parallelism.

In all cases, the quantum algorithm deals with the problem more quickly than the classical one. A fundamental property of quantum computing is quantum parallelism. Quantum parallelism allows calculating function $f(x)$ for different values of X simultaneously. Unlike parallel computing on classical computers, where technically several circuits are established that perform computations, a quantum computer performs calculations in a circuit but on a superposition of states.

Despite the absence of a full-scale quantum computer comparable in functionality to a classical computer, quantum algorithm development is one of the most popular research fields. A quantum algorithm is an algorithm that determines a sequence of quantum gates with a sign of the qubits over which it should perform them. We can define the quantum algorithm either as a verbal description of such commands or using their graphical notation as a quantum gate array. The closest classical analog of quantum computing is probabilistic computing. Some probability determines the correctness of the quantum algorithm result. In particular, the diversity of operations is expanded to increase the correct result probability in quantum algorithms. The procedure to choose these operations is that incorrect results are possible to destroy each other, and the right results probability increases.

The advantage of quantum algorithms is to reduce the time to solve the problem by parallelizing operations by generating entangled quantum states and then using them. It refers to such cases as quantum acceleration. Using quantum acceleration is most helpful in solving the problem of modeling the dynamics of complex systems and iterative mathematical problems. The general iteration case is the Grover's algorithm and the problem of finding periods is the Shor's algorithm applying the fast QFT, and their analogs.

There are three classes of quantum algorithms:

- Algorithms based on QFT;
- Quantum search algorithms;

- Algorithms for creating quantum systems.

One of the most popular for many tasks is the search algorithm. It is noted that the quantum computer solves repetitive problems, including the Grover search algorithm, which is used to search for a defined element in an unstructured database faster than the classical one.

We see all the importance of the Shor algorithm for solving practical problems in the method's example of factorization of an integer built on it. The factorization problem is hard for a conventional computer, so many public-key cryptography schemes are built on the practical impossibility of solving this problem for large prime numbers.

3.5.1. Shor's algorithm

The algorithm found by Peter Shor in 1994 allows solving the problem of the algorithmic complexity of a number factorization in polynomial time and on a polynomial number of qubits, while classical algorithms solve it in sub-exponential time. It means that once a quantum computer will be created with enough qubits, all modern cryptography will be at risk of compromise. Anyone who has access to such a quantum computer can get any information hidden using this approach.

Shor's algorithm involves two computational paradigms. The classical part prepares input data for the Shor's algorithm, also manages loops, and returns to find the correct result. The quantum part executes a linear sequence of unitary transformations over specially prepared states of input qubits.

Shor's algorithm is a quantum prime factorization algorithm that allows us to decompose the number M in time $O(\log^3 M)$ using $O(\log M)$ logical qubits. The algorithm's significance lies because with its help when using a quantum computer with several thousand logical qubits, it becomes possible to crack cryptographic systems with a public key. For example, RSA uses the public key M , which is the product of two prime numbers. One approach to break the RSA cipher is to find the M multipliers. With a sufficiently large M , it is almost impossible to do this using well-known classical algorithms at an acceptable time.

Shor's algorithm, using a quantum computer capability, can factorize a number not just in polynomial time but in a time not much greater than the multiplication time of in-

tegers. It is almost as fast as the encryption itself happens. Thus, implementing a scalable quantum computer will compromise much of modern cryptographic protection. It is not only about the RSA scheme, which directly relies on the complexity of factorization, but also about other similar schemas that a quantum computer can crack similarly.

The algorithm comprises the following steps to implement a classical part:

Algorithm 1 Shor's Algorithm

```

1. Choose a random number  $a < M$ .
2. Calculate the  $GCD(a, M)$ .
if  $GCD(a, M) \neq 1$  then
    The algorithm terminates (the degenerate case).
else
     $r \leftarrow a^x \bmod M$ 
    if  $r \% 2 \neq 0$  then
        Go back to step 1
    end if
    if  $a^{r/2} \equiv -1 \pmod{M}$  then
        Go back to step 1
    end if
else
    Determine two values of  $GCD(a^{r/2} \pm 1, M)$ , which are non-trivial divisors of the
    number  $M$ .
end if

```

Now, it is possible to implement the main part of this algorithm, namely the QFT. The QFT is the quantum analog of the discrete Fourier transform. This transformation plays a key role in Shor's algorithm, which allows us to decompose the number M into prime factors in time $O(\log^2 M \log^3(\log M))$, which gives an exponential increase in speed relative to the best known classical algorithms at the moment. Also, algorithms for modeling quantum systems on a quantum computer are built based on the QFT. The transformation itself has the form:

$$|j\rangle \rightarrow \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \omega^{jk} |k\rangle, \quad \omega = \frac{2\pi i}{2^n}. \quad (3.26)$$

It should be noted that j and k are binary entries of these numbers. This transformation is given by the recursive scheme shown in the Figure 3.13.

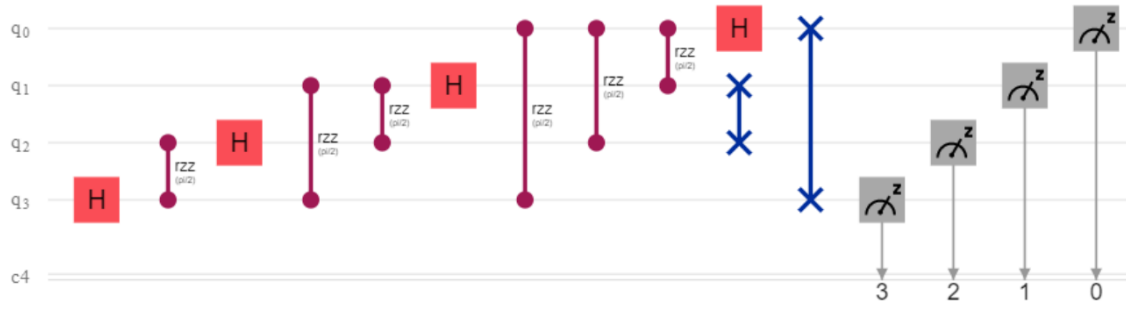


Figure 3.13. Quantum Fourier Transform

3.5.2. Grover's algorithm

In 1996, the American mathematician Lov Grover proposed another quantum algorithm based on the iterating method through numbers. Quantum computers can use this algorithm to break symmetric encryption systems. We will need to double the size of the keys to maintaining the current level of security.

Grover's algorithm is a quantum algorithm for solving the iteration problem, finding a solution to the equation $F(X) = 1$, where F is a Boolean function of n variables. It can serve as a model of complex processes at the quantum level. GSA finds the value of a definite parameter in each unordered space. Let be a Boolean function $f(x)$, $x \in (0, 1)^n$ which is represented as a black box. The goal of Grover's algorithm is to find x such that $f(x) = 1$. The function f is given as an oracle.

An oracle is a gate that encapsulates a function. It is performing the calculation of a function. It is a square matrix of the required size. On the diagonal of which there are units 1 for those elements that are not the target, and there is a value of -1 for the element that needs to be found. Non-diagonal positions have zeros. It determines the required size by the size of the element index. That needs to be found using an unstructured search. It calculates the number of the required qubits as the base 2 logarithms of the index (rounded up), and the size of the matrix are powers of 2 the number of qubits. The size of the matrix must be equal to the power of two following the index.

Grover's algorithm can be represented as follows:

- Initialization of the initial state. Here, it is necessary to prepare an equiprobable superposition of the states of all input qubits.
- Application of the Grover iteration. The Grover iteration comprises an oracle and a

Grover diffusion operator (conditional phase shift). This step is repeated $\sqrt{N}$ times.

- Measurement. At this stage, the output register of qubits is measured.

The main part of the algorithm is the Grover iteration, which is broken down into four steps:

1. The use of an oracle;
2. Applying the Hadamard transform;
3. Applying a conditional phase shift to the register;
4. Applying the Hadamard transform.

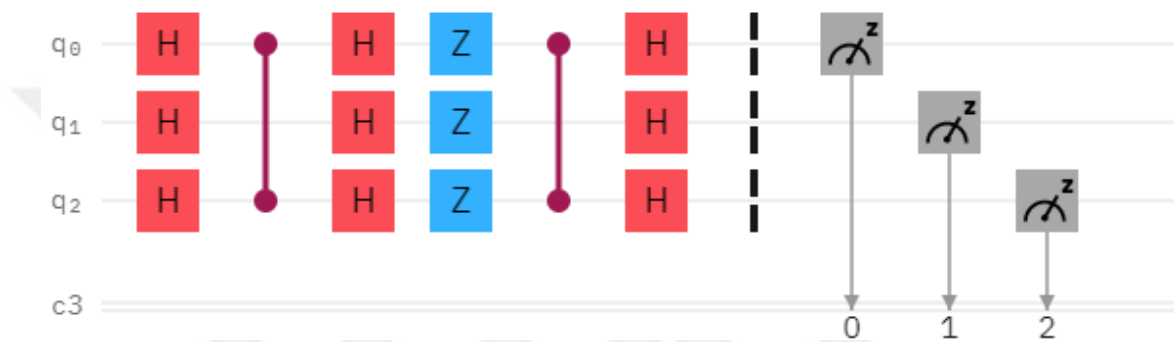


Figure 3.14. Grover's Algorithm with 3 Qubits

The last three steps are combined into the Grover diffusion operator. In the analyzed algorithm, oracle recognizes the solution to the search problem. When the input of the function f is given a value x , at which $f(x) = 1$, the oracle marks this solution by shifting the phase of the quantum state that corresponds to the value x .

The classical algorithm solves the search problem by brute force. In the best case, we will find x on the first attempt, and in the worst case, 2^n variants will have to be sorted out. Hence, this method can find x in $O(N)$ operations, where $N = 2^n$. Grover's algorithm allows us to speed up the search method—up to $O(\sqrt{N})$ operations.

Thus, based on the above, we can conclude that Grover's quantum algorithm allows us to find the value of a definite parameter in each unordered space in $O(\sqrt{N})$ calls the oracle. It gives a quadratic acceleration compared to the classical algorithm.

3.6. Post-quantum Cryptography

Many of the most effective modern communication protocols rely primarily on three basic cryptographic functionality: asymmetric key cryptography, digital signature, and

key distribution. Currently, these functions are mainly implemented using the DH key exchange protocol, the RSA, and the ECC-based cryptosystem. The security of these systems depends on the complexity of number theory problems, such as integer factorization or discrete logarithm.

As we mentioned above, quantum computers using Shor's algorithm will factorize numbers at an incredible speed. RSA and ECC cryptographic systems will be vulnerable to brute-force attacks. Such an impact on symmetric key processes is not as disastrous. Grover's algorithm ensures a quadratic acceleration for quantum search algorithms compared to classical search algorithms. This situation caused alarm, which led to new research in quantum-resistant cryptography.

The creation of quantum computers will open up new opportunities for humanity, but existing methods of protecting information will lose their effectiveness. Although quantum computers are only beyond the laboratory, there is already a need to use post-quantum cryptography.

The primary research and improvement of cryptographic algorithms at present is focused at finding solutions that would not have vulnerabilities about quantum computing while being at the same time invulnerable to attacks using conventional computers. Such algorithms are called post-quantum cryptography or quantum-safe cryptography. Like classical cryptography, quantum-safe cryptography algorithms are based on solving mathematical problems. However, the new encryption algorithms must be different so that not only classical computers but also quantum computers cannot solve them in a considerable amount of time.

Post-quantum cryptography currently includes the following main approaches:

- Lattice-based cryptography;
- Multidimensional quadratic systems;
- Electronic signatures on hash functions;
- Code-based cryptography;
- Isogeny of elliptic curves;

3.6.1. Lattice-based cryptography

The main success in quantum-safe cryptography has been the creation of practical encryption algorithms based on lattice theory. These algorithms are based on linear algebra. Lattices have been used to create key-sized asymmetric encryption and digital signature schemes, such as RSA. The new algorithm is faster than the classic algorithm. Therefore, the researchers proved that cryptography on the lattice allows you to create algorithms that were previously considered impossible.

Lattice-based cryptography is a set of ultra-reliable security protocols designed to protect data from potential attacks by hackers in the future when they can resort to the computational capabilities of quantum computers. It is possible to hide data in a multidimensional lattice using this method of cryptography. According to scientists, the recovery of such data without knowing the secret workaround is impossible, even with the help of quantum computing systems.

Lattice cryptography uses multidimensional geometric structures to hide information. A lattice is an infinite grid of points. It is assumed that by increasing the size of the lattice, cryptographers can create algorithms so complex that nothing can solve them in the future.

3.6.2. Multidimensional quadratic systems

The robustness of this section of cryptography is based on the complexity of solving a system of multidimensional quadratic polynomials over a finite field. NP-complete could be a complexity class that is the set of all problems X in NP that the other NP problem Y will be decreased to X in polynomial time. The systems in this section have good speed and low requirements for computing resources. However, the length of the public key is very large. The most well-known example is the HFE cryptosystem, based on hidden field equations. Patarin proposed it in 1996.

3.6.3. Electronic signatures on hash functions

This section includes electronic signatures constructed using hash functions, which ensures their resistance to quantum computing. With this approach, you can only generate a few signatures on a single key. Also, the disadvantages of the system include the fact

that the signer needs to record the exact number of messages already signed. An error in this entry will lead to system vulnerabilities. A classic example is the signature of Merkle, proposed in 1979.

Basic properties of a hash function:

- The input of the hash function is an arbitrary length message.
- The output of the hash function is a fixed-length data block.
- The values at the output of the hash function are distributed uniformly.
- If we change one bit at the input of the hash function, the output changes significantly.

3.6.4. Code-based cryptography

The advantages of such systems include the speed of calculations. The disadvantages are that the keys are too long. The key idea of code-based cryptography is to force an attacker to solve an NP-complete problem to decode a random linear code.

The concept here is as follows:

- Let's hide the code with a known decoding algorithm using some linear transformations (for example, permutations) over G and get a new generating matrix G' .
- Use G' to encode a word with a random error vector.
- Knowing the implemented operations to G , we can apply the inverse processes to G' and decode with an efficient algorithm, freeing it from errors.
- This code will look random for the eavesdropper.

Robert McEliece (1978) and Harald Niederreiter (1986) proposed the most popular cryptosystems in code-based cryptography. The classical cryptosystems McEliece and Niederreiter are based on the theory of algebraic coding. These algorithms are characterized by:

- Algorithms based on asymmetric encryption.

- Any linear code with an established efficient decoding algorithm can be used as a basis.
- Cryptosystems are resistant to a quantum computer attack.
- The disadvantage is the huge size of the keys (calculated in MB).

3.6.5. Isogeny of elliptic curves

The cryptographic stability of systems based on operations on elliptic curves is based on the complexity of calculating the discrete logarithm. At one time, such cryptosystems were recognized for a smaller key length, compared to RSA, which is necessary for the same level of security.

An isogeny is a map that translates the points of one elliptic curve into the points of an isogenic curve, leaving infinitely distant point stationary. Let us have two isogenic elliptic curves E_1 and E_2 . They are called isogenic if they are defined over the same field and have the same number of points.

For each isogeny, there is a single dual isogeny that performs the inverse transformation. If the isogeny has the following form $\phi : E_1 \rightarrow E_2$, then the dual to it is $\phi : E_2 \rightarrow E_1$.

The most popular SIDH protocol allows us to exchange keys over an unsecured communication channel. This fact is its distinctive feature, which guarantees perfect secrecy. With compression in mind, SIDH has the smallest key length of all post-quantum key exchange protocols. However, a full-fledged cryptosystem on isogenies has not yet been implemented.

4. RESULTS AND DISCUSSION

4.1. Computational Problems in Finance

Automation, without which impossible to improve organizations, leads to an increase in threats of unauthorized access to data, so as the need for frequent support and development of the security system. Information protection is not a one-time event or a set of methods. It is a continuous process that must take place over time at all stages of the life cycle of a computerized information processing system.

The increased performance of computer technology and the emergence of new types of attacks on ciphers have led to a decrease in the strength of known cryptographic algorithms. Therefore, the cryptographic tools that are used must be constantly updated. Maintaining and ensuring the reliable functioning of the information security system mechanisms involves solving specific tasks. Every year, information technologies have an increasing impact on both the economy and people's daily lives. The development stages of most industries and government organizations are associated with introducing information technology. Communication in social networks has become an integral part of everyday life. Information technologies open up more broad prospects for improving the efficiency of business and activity quality.

Using computing in the management systems of government and commercial structures has general infrastructure development. Using this framework allowed people with a PC and a modem to gain access to the data of the largest libraries and databases, make the hard calculations, to share data with other users of the network, regardless of distance and place of residence. But such systems entailed several difficulties, one of them being the protection of information processing and transmission. The problems are related to the development of new technologies.

On the one hand, using information technology ensures several positive aspects:

- Increasing the efficiency of management processes, information processing, and transferring.
- The feature of commercial organizations is that information losses here can express in enormous sums of money. Owing to banks keep not only the material purposes of their customers but also bank confidentiality. Any leak of such information forces

a financial institution's reputable, legal, and operational problems and income loss.

- Hacking computerized banking structures and stealing funds through illegal transfers from one account to another affects its reputation and leads to the need to recover enormous amounts of money. The same concerns for banks have transferred from accounts through falsification of bank cards and phishing.
- The solution to any problem in the financial sphere is impossible without the support of management activities and in-depth analysis of an enormous amount of information. Therefore, any leakage or misinformation of personnel and the unavailability of data can cause significant damage.

The fundamental business development trend in the banking and insurance sectors is the rapid growth of technologies for servicing the mass market. However, besides expanding the prospects, the risks of information security are also increasing. As the number of clients increases, the amount of information entered and processed explodes, which increases the likelihood of errors and makes it hard to control leaks. The requirements for the speed and accuracy of data processing are increasing. Mass clientele requires alternative approaches to service: the development of remote access to accounts and financial markets, the possibility of self-management accounts, new technologies for informing customers through mobile phones. Modern methods of serving bank customers include conventional public communication channels that are less secure than private financial networks. Also, users' independent access to financial services entails information security risks related to their ignorance, negligence, and bad faith.

Financial institutions must create extensive networks of access points to their services to protecting it, which causes complications because of their remoteness and difficulties in ensuring control over them. Scientists widely use the concept of safety in engineering. They often combine it with the risk concept. The lower the probability of an undesirable event caused by a technical device, the lower the risk. Of course, when applied to a computer, the concept of security expose specific changes. Computer security is determined by the features of both hardware and software. We cannot deny these factors. However, it is emphasized that other circumstances are crucial in ensuring the security of the information system. These include confidentiality and integrity of information, ensuring

compliance with the correct operating mode of the computer, and managing access to the resources.

Using IT technologies aimed at creating a standardized profile that satisfies all international standards will provide clients not to accept the difference between a bank office in the city center and on its outskirts. Using virtualization technology, network protocols, and high data transmission speeds, we can use a smaller number of servers to solve the information problems of branch offices and transfer the main computing and data storage tasks to the data processing center. Banks are using IT outsourcing and consulting provided by third-party companies. This activity becomes the fundamental one for many leading system integrators. The market for such services is developing every day.

4.1.1. Classical cryptography in financial systems

Discoveries in mathematics have allowed cryptographic methods in various areas, especially in banking. It is necessary to keep bank information confidential, but a more important task in the business of financial management is the reliable authentication of participants in the cash flow management process. Anyone using an EDS can implement this process.

An EDS is a fixed-length number. The value of this number depends on the content of the message and the sender's private key. Anyone can verify the signature of a document by having the corresponding public key. Signature verification confirms that the document is not distorted and that the sender composed it. The signature is even more reliable than a conventional signature on a paper document. An EDS does not protect the document from being viewed. For this purpose, we still use encryption. It is not the only application of asymmetric systems. On their basis, many interesting crypto algorithms have been developed, which are widely used, including in banking. With the current development speed of computer and digital technologies, the information security issues and information protection are becoming the most relevant.

Having conducted a study of various sources related to banking activities, we can conclude that cryptography occupies a special place in the information protection in financial systems. Cryptography has become an integral part of banking services. First, protecting banking information is carried out by organizational measures and in combination with using cryptographic means. Cryptographic algorithms, which solve the problems of en-

ensuring the confidentiality and integrity of a message, support processing, transmitting, and storing data in the banking system. For the correct solution to such issues, the availability of appropriate automated information processing tools is required.

Cryptographic technologies provide four main types of services for the banking sector: authentication (which includes identification), integrity, confidentiality, and electronic signature. These types of protection have become widespread in the banking sector because it is the most widely known means of protecting information. The highest popularity, as a means of protection, is gaining an electronic signature. For the bank, this cryptographic protection type is vital since an EDS allows the bank to transfer document flow to an electronic format and secure remote interaction with other banks.

With the development of technology, the Internet, and cellular communication, many people are worried that their personal life will become available to the entire Internet space against their will. The Internet is a global network that contains enormous amounts of information about the military, public, commercial, and private nature. There is a need to protect information that has gained such a storage format. In the modern world, cryptography used in many applications, such as in cellular communications, digital television, when connecting to Wi-Fi, in financial operations. The success of many commercial companies depends on information that is known only to them and hidden from other people.

Organizational measures combined with the use of cryptographic means mainly carried the protection of banking information when it is transmitted through communication channels out. In some areas where modem connection is used to transfer a message, encryption and EDS of various companies produce security tools for encrypted products. If we consider a payment system as an information and telecommunications system, its cryptographic protection must meet the standard requirements for such systems. Communication lines connecting terminals to computer centers are available for the interception of information. Such information may also be intentionally altered or misrepresented.

Scientists have produced strong block ciphers with a secret key designed to solve the standard task of ensuring the data confidentiality and integrity being transported or stored. Despite this, it is easy to deceive a computer. No matter how many programs protect the information, some clever attackers eventually break into the system and gain access to classified information at any moment. Hence, the protection methods are constantly up-

dated, improved, and set the bar higher. The emergence of powerful computer technologies and network computing discredited cryptographic systems that were not considered so long ago almost impossible to decrypt. However, ciphers can be resistant to cracking. The cipher can counteract the attacks of hackers. Achieving this result solves the hacking problem. Since obtaining the strength of the cipher is time-consuming work using complex mathematical calculations. The developer needs to assume possible variants of eavesdropper attacks to create the cipher strength. When attacking a cipher with increased resistance, attackers increase the number of hacking attempts and significantly increase the time for declassifying information.

The emergence of the first computers in the middle of the 20 century completely changed the situation in cryptography. With computer technology help, people have created an entire information industry, which involves all spheres of life. The successful functioning of society depends on its high-quality and well-coordinated work of information processing facilities. The computational capabilities of modern computers have raised the implementation of ciphers to a new level. But we should also note that computers also made it easier for attackers to hack them. Cryptography has undoubtedly made a significant leap in its development. The most important task for the future is to create high-speed encryption methods with high confidentiality. This task is determined by an enormous number of communication channels through which large amounts of information are transported.

Despite the intensive work of research groups in the quantum technologies field, there is no full-scale quantum computer. We can only talk about laboratory samples with limited capacity and functionality. It would seem that it is still too early to implement quantum cryptography, but it is not so. Even today, companies and users are accumulating and storing data that will be valuable in five, ten, and even thirty years. Advances in quantum computing will make such information easily accessible to 3rd parties if we do not protect them today. We cannot rule out that interested parties can intercept the information now and decrypt it later when a technical opportunity arises. Also, it is necessary to contemplate the fact that it will be difficult to update the prevailing infrastructure. It is reasonable to foresee the likely appearance of quantum computers within the future by investing in creating networks and critical data storage. After all, the infrastructure created by the organization today may be in use for over ten years.

Given the current success of the quantum computing research group, commercial companies and governments should consider the value of their data. It is recommended to implement quantum cryptography today to safeguard the information that ought to remain confidential in 20-30 years without watching for standardization. It is important to remember that it is impossible to change the quantum algorithm immediately after adopting the standard. It will require a lot of preparation work. New keys are often large, and also the infrastructure must transmit them without losing the standard message speed.

4.1.2. Threats to information security

Usage cryptographic techniques in financial institutions is increasing each day. The question of methods and criteria for determining the safety of data structures becomes quite efficient. The evaluation process should be integral since the organization's management is interested in the global stage of the organization quality itself, provided by the security level of information systems. From a practical viewpoint, the information security question is the most difficult.

The confidentiality problem of client data, the integrity of payment, and the availability of banking services are more critical than ever in our digital age. Customer loyalty is really valued considering the impressive competition and a variety of banking products. Payment security and confidentiality of information presented to the financial establishment are among the most powerful things of choice.

Threats are a disruption event for information security. In most cases, threats result from vulnerabilities in protecting information systems. An information security threat is a condition set and factor that create a potential or real-life risk of an information security violation. We identify it either with destabilizing influence on data or with the results of such an impact. There are many types of threats. When ensuring data registration, this can be theft of data and the means of processing it, and its loss. The work of any financial institution based on the trust of customers and reputation in the market. Therefore, it is difficult to overestimate the importance of information protection in business.

Main types of threats in financial institutions include:

- Confidentiality threats
- Integrity threats

- Availability threats

4.1.2.1. Confidentiality threats

The modern world is gifted with modern technologies. Digital systems have forced people closer together and permitted them to connect with people around the world. The digital field may be a system comprising sets of communications, both of individuals and corporations. There are many privacy interests related to digital media network services, a subgroup of information privacy that recognizes people to need the storage of personal data, redirection, sharing of non-public data with third parties, and the transformation of information over the Internet. An unlimited amount of data, web sites, apps, and many other tools are processed every day. Social media and applications have several features that provide users for messaging and private information sharing in open platform apps. These apps open the gates for opportunities to breach the user's private information. These privacy issues with the digital world often cause problems for the entire society.

Confidentiality threats are unauthorized access to data. The disclosure of confidential information may pose a threat to economic, state, or personal security. Security is how organizations store and protect our messages. The essence of confidentiality is to keep data from outsiders, and also the security essence is to keep the information confidential after we have collected it.

4.1.2.2. Integrity threats

Threats to integrity are violations of the transactions, reordering, fraud, duplication of data, or including other messages. We use dynamic integrity regulations, especially when considering the flow of commercial data. Integrity threats are unauthorized modification, addition, or destruction of data.

The integrity violation is an illegal modification or damage of data, which usually results in not using the data. Besides the possibility of data loss, when the integrity of the information is compromised, there is also a risk of failure of the function of the entire structure. The integrity of a data violation is determined by:

- Software bugs are modifications produced by incorrect application settings or malicious code operations.

- Sabotage is damage resulting from deliberate malicious acts. It comprises attacks by cybercriminals and also the activities of employees who attempt to disrupt the functioning of their own company.

4.1.2.3. Availability threats

The leading role of availability is clear in various management systems. Availability threats are restricting or blocking access to data. Outwardly less important but also very unpleasant issues, both material and moral, can have long-term unavailability of information services that are used by many people.

The most frequent are unintended errors of regular users, system administrators, operators, and other persons who support information systems. Sometimes even incorrectly entered data or an error in the program that caused the system to crash are risks. They create vulnerabilities that attackers can exploit. The most radical way to deal with unintentional errors is to maximize automation and strict control.

4.1.3. Cryptographic protection problems of financial information

Organizations provide the security of banking information during its transmission via communication channels out in combination with cryptographic processes in the systems using a modem for information broadcast, encryption, and EDS systems of various manufacturers of crypto products' security tools. When processing and storing banking information, cryptographic methods are used to protect against unauthorized access. Information protection has not been implemented at all stages of its processing, storage, and transmission. Based on the analysis of data on the applied means of cryptographic stability, we can propose the following conceptual provisions on the cryptographic problem of the payment system:

- The payment strategy among financial organizations is not provided with an allowed means of cryptographic protection and verification. Security measures should carry the confidence of financial information out.
- The existing organizational and technical measures do not offer absolute protection against an unauthorized connection between and inside financial organizations' networks.

- The issues of protection against intentional or unintentional violation of the integrity of commercial information stored in a computer (modification, destruction of data, and the others) have not been resolved.
- The creation of a security system must be carried out by introducing communication processes for the automated processing of financial data.
- For the cryptographic compatibility of different commercial institutions' systems, cryptographic protection should be based on principles and algorithms for cryptographic conversion and EDS. Cryptographic protection tools should have special implementations (software, firmware, hardware) and allow users to choose the most useful for individual conditions.

4.1.4. Classical cryptography problems

Cryptographic methods are widely used in practical computer science to solve many problems of information security. In the modern cryptography, we can distinguish the following three types of primary tasks that cryptography should solve:

- The transmission of confidential information through open communication channels;
- Authentication of transmitted data;
- Detect eavesdropping in communication channel.

The first type of task relates to protecting information from unauthorized access by a key. Only the key holder has access to information. The second and third problems are through the mass use of electronic processing methods and transmitting information (banking, e-commerce, communication channels). It closely relates the solution to the first task to the key distribution problem, which is then used to encrypt messages. Once the users receive the shared key, it can forward the cryptograms over any unsecured channel, possibly even over a channel subject to complete passive listening. However, to get a shared key, two users who initially do not have any shared secret information must primarily use some very reliable and private channels. Since interception is a series of measurements carried out by an eavesdropper, no matter how complex they may be from

a technical point of view, any channel can listen. It creates a security threat, which explains the importance of detecting an eavesdropper. This detecting helps us solve the third task of cryptography. Thus, the solution of the first problem is closely related to the third solution. If the key does not reach the eavesdropper, the confidentiality of the transmitted password can be guaranteed. We should emphasize that there is no classical encryption mechanism that can guarantee that they will not intercept the key during transmission through the communication channel. The second main task is message authentication. It can prevent such behaviors that violate the protection of network communications, such as modifying the content and order of messages.

Asymmetric cryptography successfully solves the problem of distributing keys over open communication channels currently. However, issues that may occur have aroused people's attention to its future. As we noted in previous sections, the stability of all schemes of asymmetric cryptography is based on the impossibility of an efficient computational solution to some mathematical problems such as factorization of large prime numbers and logarithms in discrete fields of enormous size. This impossibility is simply an assumption. It can be refuted if the opposite hypothesis is proved. It would lead to the collapse of all modern cryptography since the problems on which it is based are closely related, and hacking one cryptosystem will mean hacking most of the others. Research is being conducted in this direction, but the problem remains open. At present, the computational complexity theory is concerned with the possibility of solving this type of problems in polynomial time. It means that if even one modern cryptosystem is hacked, many others will also fail.

Another threat to modern cryptosystems comes from quantum computers. The Shor factorization algorithm allows us to factorize a number in polynomial time. In 2001, scientists successfully implemented this algorithm on the first working model of a quantum computer created by specialists from IBM and Stanford University. According to experts, a quantum computer capable of breaking the RSA encryption algorithm can be created in about 15-25 years.

Another unpleasant fact in asymmetric cryptosystems is that the minimum safe size of keys is constantly growing due to progress in the relevant field. Because of advances in mathematics, the size of data blocks and keys continues to increase. The recommended size for the RSA cryptosystem is at least 4 Kbps and 512 bits are sufficient when it is

created. In the entire 25-year history of such a system, the key length has increased approximately tenfold. But over the same period for traditional symmetric ciphers, the key size has changed less than twice. These make the long-term prospects of asymmetric cryptosystems unreliable and force us to find alternative ways to solve the same problems. We can solve some of these problems within the framework of so-called quantum cryptography.

4.2. Solutions to Computational Problems in Finance

Few people distrust the fact that soon before the beginning of the 21st century, humanity entered a new technological era — the information technology age. The IT management, which deals with the production, processing, storage, and transmission of the message, has become an integral part of the global economic organization, an independent and dynamic financial sector. Modern society's dependence on information technology is so high that deficiencies in knowledge processes can lead to significant incidents in the world.

The concept of a quantum computer is a development comparable to the discovery of classic computers. An important task is to evaluate all areas of quantum computer utilization. At the moment, the most evident and attractive area of application of a quantum computer is information security. Many experts say that hacker attacks are more dangerous than an atomic bomb, as they can penetrate a variety of areas, including politics, finance, and the military.

It is assumed that the quantum technologies of the future can provide almost absolute protection of message. The information security lies in the features of the data carriers themselves. However, a quantum computer can also be an ideal cracker of classical computers.

Modern companies manage information systems to automate their activities. The relevant systems automate all key organization treats, such as financial, personnel, customer, and document management. The information that circulates in them is classified as confidential information. For all the undeniable benefits of implementing more IT techniques, this process carries extra costs and risks for the company. The protection of information in the company becomes a prerequisite for the high competitiveness of the company and is possible by creating a security system.

4.2.1. Problems of quantum cryptography

In an ideal quantum communication system, the data interception is unacceptable because the exchange participants quickly realized the interception through the newly emerging transmission failure. However, the current systems differ from the ideal structure and have several problems.

The first problem is the participants' equipment of the information exchange is imperfect. That leads to the appearance of reception and communication errors. In these circumstances, the system should not perceive a specific error level as an attempt to eavesdrop. And this background of errors provides the eavesdropper to prevent, masking the unavoidable distortions that arise in this state under the system's errors.

The second problem is in transmission lines. Transmission lines have a signal attenuation. Signal attenuation causes the sender to extend the pulse power, for example, the amount of photons in it, or leads to the loss of some pulses in the channel. In the first case, if the pulse comprises many photons polarized in the same way, using a beam splitter from it, you can make a tap and show it then, without affecting the signal. Such interception should be carried out as close as achievable to the sender. There is a higher signal level. In the second case, the signal attenuation forces to a rise in the error rate. The eavesdropper has an extended chance to disguise the interception under the errors of the system.

The third problem is the eavesdropper has a better interception strategy than just guessing the basis. The laws of quantum mechanics prohibit only the perfect cloning of a quantum system, while imperfect cloning remains possible. At present, the theoretical possibility of a successful single copy of the quantum system state with a success probability of $5/6$ has been proved. With an increase in the number of copies, this chance decreases to $2/3$. Experiments on photon cloning show a result close to that predicted by the theory. It gives the eavesdropper the ability to copy the photon and later analyze its polarization on two different bases. Of course, there will be errors, but their level will be lower than when simply guessing the basis. If the basis is comparable to the background of system errors, listening becomes possible. Therefore, the eavesdropper always intercepts some part of the transmitted bits, masking the errors that inevitably accompany such an interception as the system's errors.

The next problem of quantum cryptography is the need to create a direct connection

between participants. Only this method of interaction gives us to organize a stable distribution of encryption keys. Here, the session key is formed from two parts. The first part is the master key, and the second part is the quantum. The client generates the master key using traditional cryptography. And the second part creates a QKD process. Finally, we get the resulting key by bitwise XOR operation of these two parts. This way, even if hackers can prevent or crack the client's master key, the messages will remain confidential. However, the cost of such systems today exceeds hundreds of thousands of dollars.

It is necessary to use various correction protocols to filter out their errors in real-world quantum cryptography systems. It is needed to use the increasing secrecy procedure to reduce the significance of the bits intercepted by the eavesdropper. Compared to the idea of real-world quantum communication, the system cannot provide the absolute secrecy of the transmitted data. It is because of a background of their errors, which can be disguised as interception attempts, and attenuation in communication channels because of the need to use multi-photon pulses. Since the channel quality is not always controllable, the latter makes nondestructive interception of data possible and is an almost unavoidable factor.

Let's assume that there are 1000 qubits in the pulse, an illegal user can intercept 100 of which. Thus, the attacker can get the information he needs by analyzing the following discussions between the participants. Any attempt by an illegal user to delete a piece of information will lead to a significant increase in the number of errors, in which case the sender must retransmit the message.

When creating practical cryptosystems based on the QKD, we have to face the following problems:

- Low data transfer rate;
- Data is transmitted only over short distances;
- Impossible to create quantum repeaters;
- Quantum pulses intensity;
- Malicious attacks on the quantum channel change the message itself.

Despite these problems, there are also great successes in this area. Such well-known companies as IBM, Toshiba, Google, and others conducted practical works in quantum

cryptography. It has also created the commercial quantum cryptosystem ID Quantique 3000 Clavius QKD System, which supports secure key exchange at a distance of up to 100 km, supports the BB84 protocol, and more.

4.2.2. Vulnerabilities in quantum cryptography

Although the QKD is positioned as invulnerable to hacking, specific implementations of such systems provide for a successful attack and theft of the generated key. There are some attack types on cryptosystems with QKD protocols. Some attacks are theoretical, but other attacks have been successfully used in practice:

- Beam splitter attack comprises scanning and splitting the pulses into two parts and analyzing each of the parts in one of the two bases.
- The Trojan Horse attack comprises scanning a pulse through an optical multiplexer toward the sending side or the receiving side. It divides the pulse into two parts for synchronous detection and admits the decrypting circuit without distortion of the transmitted photons.
- Coherent attacks are based on relay tactics. The attacker intercepts the sender's photons, measures their state, and sends the receiver pseudo-photons in the measured states.
- During incoherent attacks, the sender's photons are intercepted and confused with a group of transmitted single photons. The group state is measured, and so the changed data is shifted to the recipient.
- The research group of Vadim Makarov developed the attack with the blinding of avalanche photodetectors. It allows the attacker to get a secret key so that the recipient does not notice the interception.
- PNS attack comprises detecting over one photon in the pulse, removing, and confusing it with the sample. We send the remaining unchanged part of the message to the receiver, and the interceptor receives the true value of the transmitted bit without creating errors in the sifted key.

- If we create the photons with four different photodiodes, they have spectral characteristics. The attacker in the spectral attack can measure the color of the photon, not its polarization.
- If the sender uses a PRNG, the attacker can adopt the same algorithm and get the specific sequence of bits. This type of attack is called a PRNG attack.

4.2.3. Comparing quantum solutions to classical one

Despite the limitations, quantum cryptography has unconditional benefits over classical cryptography, as it has proven cryptographic strength. However, as experience shows, proven stability is a property of theoretical models, conceptions but not specific implementations. The currently developed methods of QKD systems deprive quantum cryptography of this advantage.

Quantum cryptosystems generate a random private key. We can only decrypt the data encrypted on this key if we guess the key. It allows us to keep the data for many years by choosing a quantum key of acceptable length.

The advantages of quantum cryptography include:

- Security is based on fundamental physical laws and principles.
- The ability to detect of a passive attacker. An attack comprises higher errors than they appear in the quantum channel because of actual noise.
- Information-theoretic security of key distribution. Keys distributed using quantum protocols with information-theoretic stability are used for better encryption accepting well-known classical symmetric algorithms. Therefore, the overall strength of the cryptosystem increases.

The primary purpose of cryptography is to protect or keep the information confidential. Cryptographic technologies provide four main types of services for the banking industry: confidentiality, integrity, authentication, identification, and control over the interaction of participants.

Cryptography transforms the message into a form that the eavesdropper cannot understand. It is assumed that the attacker cannot only intercept the transmitted messages in

the communication channel for their subsequent analysis but also purposefully changes them, as well as sends fake messages on behalf of the participants.

At the qualitative level, ensuring confidentiality is described by the interaction of three actors. The sender converts the plaintext into encrypted messages transmitted to the recipient via an open communication channel to protect it from eavesdropping. An attacker is any entity that does not have access to the transmitted information. The legitimate recipient of the information decrypts the received messages.

The eavesdropping is trying to get hold of the protected information. An eavesdropper can make both passive and active attacks. Passive attacks are associated with eavesdropping, traffic analysis, interception, recording of transmitted encrypted messages, decryption, attempts to crack the protection to gain information. An attacker during active attacks can try to substitute, interrupt the message transmission process by creating fake or changing the transmitted encrypted messages.

The QKD methods solves one of the main cryptographic tasks. QKD protocols distribute keys between remote users through an open communication channel. A key is a numeric or alphabetic array of a certain length created to encrypt a message. Quantum cryptography allows us to ensure a constant and automatic key exchange during each message transmission in the OTP mode.

QKD allows two parties connected over an open communication channel to create a shared random key known only to them and use it to encrypt and decrypt messages. An essential property of QKD is the ability to detect the illegal presence of a third party. Here we use a fundamental aspect of quantum mechanics. This aspect is expressed in the quantum's violation system during its measurement.

It is impossible to get the coordinates and impulse of a particle simultaneously and also impossible to measure one parameter of a photon without distorting the other in quantum-based technologies because the quantum cryptography technologies are based on the uncertainty principle of the system. An attempt to measure interrelated parameters in a quantum system changes the qubit state, destroying the original signals. It means that it is possible to detect an interception in the communication channel immediately. When trying to get a key, a third party must measure the quantum states transmitted over the communication channel. This measurement inevitably leads to states change and the appearance of an anomaly in the communication channel. A communication channel

that detects interception can produce anomalies using quantum superposition, quantum entanglement, and data transmission in quantum states. If the anomaly number is below a certain threshold, the key will be created that guarantees security. Otherwise, we cannot generate the secret key, and the connection is ending without the message transmitting.

The interception of keys in quantum cryptography is theoretically possible. But, for the reasons described above, the attacker cannot go unnoticed. With the widespread adoption of such a reliable means of protecting information, the dangerous type of computer attack known as a MITM may be a thing of the past.

Quantum cryptography can theoretically provide a secure key distribution. Because of the properties of the quantum system, an eavesdropper introducing a certain number of errors into the system, and the information transmitted by individual photons is distorted. The receiver can detect this eavesdropping thanks to these properties. However, natural noise in the quantum communication channel also leads to errors. No method has yet been developed to distinguish between errors caused by channel imperfections and errors caused by eavesdropping. Also, there are strategies for the eavesdropping agent to reduce the error number it makes. The amount of information that gets the eavesdropper also decreases. Thus it receives only partial information about the key. However, it is fundamental that to get at least this part of information. The eavesdropper must measure at least part of the transmitted photons, and therefore the level of errors introduced by it cannot be made arbitrarily small.

If the transmission error rate exceeds a certain threshold, all QKD protocols require legitimate users to abandon the distributed key and start the whole procedure again. This value sets depending on the average level of natural interference in the protocol's implementation. Thus, the unique contribution of quantum cryptography to cryptological science is to provide the ability to detect an eavesdropping agent. Thus, the third problem can be solved with the help of quantum cryptography.

As for the user authentication problem, quantum cryptography does not yet provide a practical solution to it, although active theoretical research is being conducted in this direction. Most researchers suggest using entangled EPR pairs or triples of photons for a quantum digital signature and develop protocols. The implementation of such protocols can be possible with modern technologies. In other words, it is proposed to use quantum computing to create a quantum digital signature, which requires quantum computers that

have not yet been created.

Also, the methods of quantum cryptography have not yet fully solved the first problem of classical cryptography. Before users start their QKD protocol, they will need to exchange authentication keys generated using classical asymmetric cryptosystems. We should emphasize that the reasons the first problem is not completely solved in either classical or quantum cryptography are different.

Classical cryptosystems do not solve the first problem of cryptography for two primary reasons. The first one is the lack of reliable ways to detect an eavesdropping agent when transmitting a key, and the other one is using keys that are not long enough, which can be decrypted. Classical cryptography can effectively solve the key distribution problem using the OTP cipher, which achieves a higher level of security. The quantum cryptography methods allow us to solve the key distribution problem, but they are doing not solve the authentication problem.

Based on the problems discussed above and the solutions to these problems, we can conclude that before creating a full-scale quantum computer to improve cryptographic strength, we can use quantum and classical cryptography together. It is possible to synthesize classical and quantum cryptographic techniques within the following composition. As a case, we can use OTP cipher for message encryption, classical authentication methods, for example, an EDS, and a quantum protocol for key distribution. Such a scheme will provide a higher level of security than any classical cryptographic scheme. As written above, active research is ongoing during this direction. Then quantum cryptography will probably be able to solve all three significant issues of cryptography.

4.3. Practical Implementation of Quantum Cryptography

The quantum information theory will change the trendy views of the scientific community supported on information security. Conducting experiments and research on information security is of great scientific activity to find solutions to the fundamental problems and problems facing quantum cryptographic systems. Such issues include the question of detecting single photons with a high probability in a quantum state with a low level of false positives, the trouble of increasing the transmission distance and the low speed of quantum key generation, and therefore the lack of controlled sources of single photons. Quantum technologies in information security systems are one of the most complicated

phenomena of quantum technologies. In recent years these types of technology have aroused great interest among specialists.

Quantum teleportation is one of the most rapidly developing areas of quantum physics. It provides information about an effort to intercept the transmitted messages. Research in quantum teleportation can lead not only to positive consequences but also to negative ones. Quantum cryptography, supported quantum teleportation, within the future, can replace many used cryptographic systems and will be used on a par with conventional means of info telecommunication. The urgency and scale of the issues related to ensuring information security will increase every day. The development of quantum information will bring results soon. Perhaps this development will cause a total change in the scientific picture of the world in IT.

Despite the inevitability of changes in modern methods of encryption and data transmission, there are not powerful quantum computers that can break existing encryption systems right now. Thus, the review shows that the information protecting problems from attacks using quantum computers has several solutions, each of which has its advantages and disadvantages. The solution using traditional encryption technology will provide enough security for the message transmission using the existing infrastructure. Thus, the review shows that the protecting information problem from attacks using quantum computers has several solutions, each of which has its advantages and disadvantages.

Quantum encryption methods need a new infrastructure along with the traditional communication channel. But they can guaranty the transmitted data security since, in principle, it will not be possible to make a connection if the transmitting listens to it. We can conclude that it will be popular when transmitting secret information, based on the advantages of quantum encryption, while traditional cryptography cannot provide security. It confirms the promise of quantum encryption techniques.

Scientists currently develop quantum protocols for secure present communication and authenticating of quantum messages and quantum EDS methods. Unlike the QKD system, these areas of quantum cryptography are still in the early stages of development. Experimental techniques of quantum secure communication that provide an acceptable communication rate do not yet exist. We note that the existing QKD systems contain quite complex fiber-optic, electronic, and software components. Now working with these systems is more like conducting a complex scientific experiment than a practical activity

using common and standard equipment. Therefore, it is necessary to solve some practical and theoretical problems to use the quantum cryptography technique in the existing data transmission network infrastructure.

Table 4.8. QKD Advantages and Disadvantages

Advantages of QKD	Disadvantages of QKD
Detection of eavesdropping	Complete solution is not proved
Unconditional security of QKD	Low data transfer rate
General unconditional security	Quantum pulses intensity
	Limitations of the quantum channel length
	Very high price
	Malicious attacks on the quantum channel change the message itself

In conclusion, we can highlight the current theoretical problems of quantum cryptography:

- Needs to develop a new and powerful QKD protocol, which can not only prevent attacks using modern technology but also prevent attacks that only remain in theory. Because such attacks, which are not available now, may well become possible in the future.
- Need to determine the dependency between the amount of information that the eavesdropper can receive and the level of error it makes. This study will provide us to compare the security levels of different protocols. Scientists have already tested basic protocols, but analyses for more complex ones have not yet been conducted.
- Development of efficient error-correcting methods that appear during a quantum channel with noise. This issue is related to the problem of error correction in quantum computing.
- Development of software that manages all key transfer operations via the quantum channel. It includes the initial generation and transmission of photons, the correc-

tion of errors in the received bit sequence, the assessment of information leakage to eavesdroppers, increasing confidentiality, and creating the key. Already scientists made such software programs for several QKD protocols.

Theoretically, quantum cryptography is a reliable method of protecting communication channels. Putting it into practice is a complicated task. We require special equipment to achieve it, such as detectors and single-photon sources. Also, it is necessary to know the orientation at both ends of the channel to measure the photon polarization angles. All this complicates the practical implementation of the method on classical computers and on mobile devices makes it impossible at all. However, quantum cryptography seemed unreachable some time ago, and now it is increasingly being described as a reliable information security system.

Our study has shown that quantum cryptography has already taken its rightful place among systems that provide information transfer. From discussing the advantages and disadvantages of various QKD protocols (Table 4.8), the scientific world has moved to the search for the most successful structural solutions that increase the communication range, expand the speed of key formation and reduce the influence of destabilizing factors. One of the development trends of the basis improvement of the quantum cryptosystem is to overcome the technical difficulties of manufacturing devices based on quantum encryption.

4.4. Future Works

The protocols looked at by us satisfy the reliability criteria of the QKD. However, they have the common disadvantage of losing messages when we apply them, thus reducing the key generation speed. Deterministic protocols that use all parameters of bases do not have this disadvantage. Such protocols are still being developed to avoid problems related to information loss. Developments in quantum cryptography to solve such issues and increase the speed of data transmission are underway. Summing up the analysis, we can conclude that the application and improvement of quantum cryptography, implementing quantum data transmission channels, is a big step in the future of cryptography.

We can point out the areas of further research :

- Research and development of the possibility of using a quantum cryptographic sys-

tem to ensure the protection of information.

- Experimental research on the development of technologies for creating quantum systems comprising long-lived particles in non-separable states.



5. CONCLUSION

The daily activities of the financial organizations are closely related to the use of modern computer technology. These systems depend on the reliable and uninterrupted operation of the computing system. The widespread use of local and global networks, satellite communication channels, and confidential data has increased the urgency of information protection issues in financial organizations. Today, computer technologies are progressively being introduced and used in the financial sector.

With the intensive development of innovative technologies, research on intelligent software and hardware products that apply computer science and quantum technology is significant. Quantum information will affect the foundation and further development of the information space in the future. The widespread use of quantum technologies implies a scientific and technological revolution, the scale of which is difficult to imagine. Quantum communication technology development is one of the promising and steps in the strategic plans of many countries. Quantum cryptography represents a new direction in the development of means of confidential information transmission. This direction includes several sections, the main of which is the distribution of secret keys through transferring quantum states of microparticles.

The contribution of the research is a comprehensive approach to the problems inherent in the modern financial IT system in the era of the quantum revolution and a discussion of their solutions in both classical and quantum cryptography. This study examines the practical aspects of using quantum cryptography in commercial systems and compares classical and quantum cryptography. Giving insights about the use of quantum computing and find out ideas that can help to determine the future direction of research.

In conclusion, we can estimate that quantum cryptography is another round of cryptographic technology and information security issues. Quantum cryptography, which is based on different principles, allows us to eliminate some risks and vulnerabilities combined with classical communication channels. However, quantum channels are associated with specific technical challenges and new classes of vulnerabilities and threats. The solution to these problems will find the direction of the development of quantum cryptography soon.

6. REFERENCES

- Barenco, A., Ekert, A., Suominen, K. A., and Törmä, P. 1996. Approximate quantum fourier transform and decoherence. *Physical Review A*, 54, 1., 139–146. <https://doi.org/10.1103/physreva.54.139>
- Bell, J. S. 1964. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1, 195–200. <https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195>
- Bennett, C. H. 1992. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68, 3121–3124. <https://doi.org/10.1103/PhysRevLett.68.3121>
- Bennett, C. H., Bernstein, E., Brassard, G., and Vazirani, U. 1997. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26, 5., 1510–1523. <https://doi.org/10.1137/s0097539796300933>
- Bennett, C. H., Bernstein, H. J., Popescu, S., and Schumacher, B. 1996. Concentrating partial entanglement by local operations. *Physical Review A*, 53, 4., 2046–2052. <https://doi.org/10.1103/physreva.53.2046>
- Bennett, C. H., and Brassard, G. 1984. Quantum cryptography: Public key distribution and coin tossing. *IEEE Conference on Computers, Systems and Signal Processing*, 175–179.
- Bennett, C. H., Brassard, G., and Breidbart, S. 2014. Quantum cryptography ii: How to re-use a one-time pad safely even if $p=np$. *Natural Computing*, 13, 4., 453–458. <https://doi.org/10.1007/s11047-014-9453-6>
- Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., and Wootters, W. K. 1993. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70, 1895–1899. <https://doi.org/10.1103/PhysRevLett.70.1895>
- Bennett, C. H., and Wiesner, S. J. 1992. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69, 2881–2884. <https://doi.org/10.1103/PhysRevLett.69.2881>
- Bernstein, D. J. 2009. *Introduction to post-quantum cryptography*. Springer, Berlin, Heidelberg. https://doi.org/https://doi.org/10.1007/978-3-540-88702-7_1

- Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H., and Zeilinger, A. 1997. Experimental quantum teleportation. *Nature*, 390, 6660., 575–579. <https://doi.org/10.1038/37539>
- Branciard, C., Gisin, N., Kraus, B., and Scarani, V. 2005. Security of two quantum cryptography protocols using the same four qubit states. *Physical Review A*, 72, 3. <https://doi.org/10.1103/physreva.72.032301>
- Brassard, G. 2005. Brief history of quantum cryptography: A personal perspective. *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005*. <https://doi.org/10.1109/itwtpi.2005.1543949>
- Brassard, G., Braunstein, S. L., and Cleve, R. 1998. Teleportation as a quantum computation. *Physica D: Nonlinear Phenomena*, 120, 1-2., 43–47. [https://doi.org/10.1016/s0167-2789\(98\)00043-8](https://doi.org/10.1016/s0167-2789(98)00043-8)
- Bužek, V., and Hillery, M. 1996. Quantum copying: Beyond the no-cloning theorem. *Physical Review A*, 54, 3., 1844–1852. <https://doi.org/10.1103/physreva.54.1844>
- Einstein, A., Podolsky, B., and Rosen, N. 1935. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47, 777–780. <https://doi.org/10.1103/PhysRev.47.777>
- Ekert, A., and Jozsa, R. 1996. Quantum computation and Shor’s factoring algorithm. *Reviews of Modern Physics*, 68, 3., 733–753. <https://doi.org/10.1103/RevModPhys.68.733>
- Ekert, A. K. 1991. Quantum cryptography based on bell’s theorem. *Phys. Rev. Lett.*, 67, 661–663. <https://doi.org/10.1103/PhysRevLett.67.661>
- Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J., and Yeh, H. 2005. Current status of the darpa quantum network. *Storage and Retrieval for Image and Video Databases*.
- Feynman, R. P. 1982. Simulating physics with computers. *International Journal of Theoretical Physics*, 21. <https://doi.org/10.1007/BF02650179>
- Fung, C.-H. F., Tamaki, K., and Lo, H.-K. 2006. Performance of two quantum-key-distribution protocols. *Physical Review A*, 73, 1. <https://doi.org/10.1103/physreva.73.012337>
- Gisin, N. 2014. *Quantum entanglement*. https://doi.org/10.1007/978-3-319-05473-5_5

- Grover, L. K. 1997. Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Physical Review Letters*, 79, 2., 325–328. <https://doi.org/10.1103/PhysRevLett.79.325>
- Holevo, A. S. 2012. Quantum systems, channels, information. a mathematical introduction.
- Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H., and Zeilinger, A. 2000. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71, 4., 1675–1680. <https://doi.org/10.1063/1.1150518>
- Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., and Zeilinger, A. 2000. Quantum cryptography with entangled photons. *Physical Review Letters*, 84, 20., 4729–4732. <https://doi.org/10.1103/physrevlett.84.4729>
- Jennewein, T., Weihs, G., Pan, J.-W., and Zeilinger, A. 2001. Experimental nonlocality proof of quantum teleportation and entanglement swapping. *Physical Review Letters*, 88, 1. <https://doi.org/10.1103/physrevlett.88.017903>
- Kiefer, C., and Joos, E. 1998. Decoherence: Concepts and examples. *Lecture Notes in Physics*, 105–128. <https://doi.org/10.1007/bfb0105342>
- Lacan, F., Woerner, S., and Yndurain, E. 2019. Getting your financial institution ready for the quantum computing revolution.
- Martín-López, E., Laing, A., Lawson, T., Alvarez, R., Zhou, X.-Q., and O’Brien, J. L. 2012. Experimental realization of shor’s quantum factoring algorithm using qubit recycling. *Nature Photonics*, 6, 11., 773–776. <https://doi.org/10.1038/nphoton.2012.259>
- McEliece, R. J. 1978. A public-key cryptosystem based on algebraic coding theory. *DSN Progress Report*, 42-44, 114–116. <https://ci.nii.ac.jp/naid/10015155006/en/>
- Niederreiter, H. 1986. Knapsack-type cryptosystems and algebraic coding theory. *Prob. Contr. Inform. Theory*, 15, 2., 157–166. <https://ci.nii.ac.jp/naid/80003180051/en/>
- Nielsen, M. A., and Chuang, I. L. 2010. *Quantum computation and quantum information*. Cambridge University Press.
- Portmann, C., and Renner, R. 2021. Security in quantum cryptography.
- Resch, S., and Karpuzcu, U. R. 2019. Quantum computing: An overview across the system stack.

- Rivest, R., Shamir, A., and Adleman, L. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21, 120–126.
- Scarani, V., Acín, A., Ribordy, G., and Gisin, N. 2004. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92, 5. <https://doi.org/10.1103/physrevlett.92.057901>
- Schlosshauer, M. 2005. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Reviews of Modern Physics*, 76, 4., 1267–1305. <https://doi.org/10.1103/revmodphys.76.1267>
- Schrödinger, E. 1935. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31, 4., 555–563. <https://doi.org/10.1017/S0305004100013554>
- Schrödinger, E. 1936. Probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 32, 3., 446–452. <https://doi.org/10.1017/S0305004100019137>
- Shannon, C. E. 1949. Communication theory of secrecy systems. *Bell System Technical Journal*, 28-4, 656–715. <http://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf>
- Shor, P. W. 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26, 5., 1484–1509. <https://doi.org/10.1137/s0097539795293172>
- Vaidman, L. 1994. Teleportation of quantum states. *Physical Review A*, 49, 2., 1473–1476. <https://doi.org/10.1103/physreva.49.1473>
- Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., and Chuang, I. L. 2001. Experimental realization of shor’s quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414, 6866., 883–887. <https://doi.org/10.1038/414883a>
- Vernam, G. S. 1926. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Transactions of the American Institute of Electrical Engineers*, 45, 295–301. <https://doi.org/10.1109/T-AIEE.1926.5061224>
- Wiesner, S. 1983. Conjugate coding. *Sigact News*, 15, 78–88.

- Wood, L. 2018. Global quantum cryptography market 2017-2023: Market to grow from \$328 million in 2017 to \$1.2 billion in 2023, growing at a cagr of 25%. <https://www.prnewswire.com/news-releases/global-quantum-cryptography-market-2017-2023-market-to-grow-from-328-million-in-2017-to-12-billion-in-2023-growing-at-a-cagr-of-25-300623411.html> [Last access date: 05-06-2021]
- Wootters, W. K., and Zurek, W. H. 1982. A single quantum cannot be cloned. *Nature*, 299, 802–803. <https://doi.org/10.1038/299802a0>



CURRICULUM VITAE

Sevil TEIFUROVA

EDUCATION DETAILS

Graduate 2018-2021	Akdeniz University Institute of Natural and Applied Sciences, Department of Computer Engineering, Antalya
Undergraduate 2013-2018	Erciyes University Engineering Faculty, Department of Computer Engineering, Kayseri