Turkish Journal of Science & Technology
16(1), 97-101, 2021

Quantum Cryptography, Quantum Communicatıon and Quantum Computing Problems and Solutions

Muharrem Tuncay GENÇOĞLU*
Vocational School of Technical Science, Fırat University, Elazığ, Turkey
*mt.gencoglu@firat.edu.tr

(Geliş/Received: 27/01/2021; Kabul/Accepted: 13/02/2021)

Abstract: : The development of quantum technologies will open up new perspectives in the use of quantum algorithms, the creation and modeling of complex physical and biological systems, new physical methods of transmitting, receiving and processing information. In turn, this will give impetus to the development of a large number of applications in the scientific, technical, economic and social spheres of society. Quantum cryptography is a communication protection method based on certain phenomena of quantum physics. Unlike traditional cryptography, which uses mathematical methods to ensure the secrecy of information, quantum cryptography focuses on physics, where information is carried using objects of quantum mechanics. The process of sending and receiving is always carried out by physical means, for example using electrons in an electric current, or photons in fiber-optic communication lines. In this process, the current situation was determined and the problems encountered and the solution suggestions for these problems were tried to be addressed.

Key words: Quantum cryptography, quantum communication, quantum computing, quantum problems, quantum solutions.

Kuantum Kriptografi, Kuantum İletişim ve Kuantum Hesaplama Problem ve Çözümler

Öz: Kuantum teknolojilerinin gelişimi, kuantum algoritmalarının kullanımı, karmaşık fiziksel ve biyolojik sistemlerin oluşturulması ve modellenmesi, bilgi iletimi, alımı ve işlenmesi için yeni fiziksel yöntemler konusunda yeni bakışaçıları ortaya koyacaktır. Bu da, toplumun bilimsel, teknik, ekonomik ve sosyal alanlarda çok sayıda uygulamanın geliştirilmesine katkı sağlayacaktır. Kuantum kriptografi, kuantum fiziğinin belirli ilkelerine dayanan bir iletişim koruma yöntemidir. Bilginin gizliliğini sağlamak için matematiksel yöntemler kullanan geleneksel kriptografinin aksine, kuantum kriptografi, bilginin, kuantum mekaniği nesneleri kullanılarak, taşındığı fiziksel alana odaklanır. Gönderme ve alma işlemi her zaman, örneğin bir elektrik akımındaki elektronlar veya fiber-optik iletişim hatlarındaki fotonlar kullanılarak, fiziksel yollarla gerçekleştirilir. Bu süreçteki mevcut durum tespiti yapılarak karşılaşılan sorunlar ve bu sorunlara yönelik çözüm önerilerine değinilmeye çalışılmıştır.

Anahtar kelimeler: Kuantum kriptografi, kuantum iletişim, kuantum hesaplama, kuantum problemler, kuantum çözümler.

1. Introduction

Quantum information processing is a new area of expertise with tremendous potential leading to breakthroughs in many areas of science and technology. It uses fundamentally new methods of computation and communication, based on the principles of quantum mechanics, rather than classical physics. This promises tremendous computing power, far beyond the capabilities of any classical computer, guarantees secure communication, and also stimulates the development of nascent quantum and related Technologies[6].

The development of quantum technologies will open up new perspectives in the use of quantum algorithms, the creation and modeling of complex physical and biological systems, new physical methods of transmitting, receiving and processing information. In turn, this will give impetus to the development of a large number of applications in the scientific, technical, economic and social spheres of society.

Considerable interest in the world in this topic is manifested in the increase in funding for quantum information technologies in the USA, Canada, Australia, the European Union, China, Singapore, Japan and many other countries. An example is similar long-term programs adopted in the United States (QIST) and the European Union (QIPS), the creation of Centers and target laboratories for developments in the field of COIKS. Certain areas of KOIKS are funded by law enforcement agencies of many states (DARPA, ARDA, NASA, ONR, ESA, GACICN, etc.). Leading scientists in the field of quantum physics, mathematics, computing, biology, and others are involved in the development. Such large firms as Microsoft, IBM and Lockheed Martin, as well as NASA, have created special research units that develop quantum information technologies. Leading

* Corresponding author: mt.gencoglu@firat.edu.tr. ORCID: 0000-0002-8784-9634

scientists in the field of quantum physics, mathematics, microelectronics, computer technology, biology, etc. are involved in these developments[7,8].

Such technologies are based on priority fundamental research, which covers the following areas:

1) Quantum communications, including quantum cryptography:

2) Quantum computing;

3) Technologies aimed at creating a component base for quantum communications and computing.

The goal of research in the selected priority areas is to create a fundamental foundation for the development of computing and communication technologies at a fundamentally new level and the creation of appropriate new materials and devices[10].

Quantum cryptography is a communication protection method based on certain phenomena of quantum physics. Unlike traditional cryptography, which uses mathematical methods to ensure the secrecy of information, quantum cryptography focuses on physics, where information is carried using objects of quantum mechanics. The process of sending and receiving is always carried out by physical means, for example using electrons in an electric current, or photons in fiber-optic communication lines[1].

History of quantum cryptography The idea of using quantum objects to protect information from counterfeiting and unauthorized access was first expressed by Stefan Weisner in 1970. In 1984, Charles Bennett of IBM and Gilles Brassard of the University of Montreal, who were familiar with Weisner's work, suggested that photons could be used in cryptography to obtain a fundamentally secure channel. To represent zeros and ones, they decided to take photons polarized in different directions and proposed a simple quantum encryption key distribution scheme, which they called BB84. In 1989, Bennett and Brassard at the IBM Research Center built the first working quantum cryptographic system. It consisted of a quantum channel containing transmitters at the ends (traditionally called Bob's and Alice's transmitters) placed on an optical bench about[2].

In the second part of the study, the idea and applications of quantum cryptography are mentioned. In the third section, the current situation is determined and the problems are classified. While the results are included in the fourth chapter, solution suggestions are given for the problems identified in the fifth chapter.

2. Implementation of the idea of quantum cryptography

The method of quantum cryptography is based on the observation of quantum states of photons. The sender sets these states, and the receiver registers them. It uses the Heisenberg quantum uncertainty principle when two quantum quantities cannot be measured simultaneously with the required accuracy. Thus, if the sender and the receiver have not agreed between themselves which type of polarization of quanta to take as a basis, the receiver can destroy the signal sent by the sender without receiving any useful information. These features of the behavior of quantum objects formed the basis of the BB84 quantum key propagation protocol.

This scheme uses a quantum channel through which users (Alice and Bob) exchange messages, transmitting them in the form of polarized photons.

The BB84 circuit works as follows. First, Alice generates and sends to Bob a sequence of photons, the polarization of which is chosen at random and can be 0, 45, 90 and 135 °. Bob takes these photons and for each of them randomly decides whether to measure its polarization as perpendicular or diagonal. On the open channel, Bob announces for each photon what type of measurements he made (perpendicular or diagonal), but does not report the result of these measurements, for example, 0, 45, 90 or 135 °. Through the same open channel, Alice tells him whether the correct type of measurements has been chosen for each photon. Alice and Bob then discard any cases where Bob made incorrect measurements. If the quantum channel was not intercepted, the remaining types of polarization will be shared between Alice and Bob the secret information, or the key. This stage of the operation of a quantum cryptographic system is called primary quantum transmission.

The next important step is to evaluate attempts to intercept information in a quantum-cryptographic communication channel. This can be done by Alice and Bob over an open channel by comparing and discarding subsets of the data they receive randomly. If such a comparison reveals the presence of an interception, Alice and Bob discard all their data and begin re-executing the primary quantum transfer. Otherwise, they leave the same polarization, taking photons with horizontal or 45 ° polarization for binary "0", and with vertical or 135 ° polarization - for binary "1". According to the uncertainty principle, an attacker cannot measure both rectangular and diagonal polarizations of the same photon. Even if he makes a measurement for any photon and sends this photon to Bob per the result of his measurements, then in the end the number of errors will greatly increase, and this will become noticeable to Alice. This will lead to 100% confidence of Alice and Bob in the interception of photons.

A more efficient check for Alice and Bob is the parity check performed over the open channel. For example, Alice might report, "I looked at the 1st, 4th, 6th, 8th... and 998th of my 1000 bits, and they contain an even number of ones." Then Bob counts the number "1" in the same positions. It can be shown that if Bob's and Alice's data are different, parity checking a random subset of that data will reveal the number of errors. It is enough to repeat this test 20 times with 20 different random subsets to calculate the error rate. If there are too many errors, then it is considered that an interception was made in a quantum cryptographic system.
If Alice and Bob are not going to use the key they received immediately, then they face a new problem - how to keep the key secret? In 1991, Artur Ekert proposed a protocol to solve both of these problems of key distribution and storage. Eckert's protocol is based on the coupling effect of quantum particles. Linked particles behave unusually: if you measure one of them, then the other (no matter how far away it is) will necessarily "go over" into a state opposite to the state of the first particle. The paradox is that information about the state of a particle is transmitted at a speed that exceeds the speed of light. Nevertheless, this phenomenon is demonstrated experimentally by physicists and can be used to encrypt information[3-5].

In a somewhat simplified form, Eckert's protocol assumes that Alice generates a certain number of pairs of concatenated photons. She sends one photon from each pair to Bob and keeps the other. Some of the particles are immediately measured by Alice and Bob to determine if the interception was performed: if so, the consistency of the states of the particles will disappear. The rest of the particles are stored by Alice and Bob in perfectly reflecting boxes. When the need arises to exchange messages, they will measure the state of a certain number of particles stored in them, and receive a secret key[11,12].

3. Current state and problems

Quantum cryptography as a market segment is just beginning to emerge, and for now, both global computer corporations and small start-up companies can play on equal terms. Interest in quantum cryptography from commercial and military organizations is growing, as this technology can guarantee absolute security. Today, quantum cryptography has been available for commercial use for several years. But the technology is only practical in the hands of government organizations and large private sectors that can afford to have their fiber-optic networks.

But besides the successful creation and commissioning of quantum key distribution systems, there are also successful experiments on their cracking. For example, in 2007, physicists from the University of Toronto (Canada) performed an experimental demonstration of undetectable message interception in a quantum key distribution system implemented by the Swiss company ID Quantique.

3.1. Scientific and technical problems in the field of quantum communications

- Development of new protocols of quantum communication and quantum cryptography, research of their properties and experimental implementation;
- Development of methods for preparation, measurement, control and transformation of quantum states of light, including states of high dimension, macroscopic entangled states, etc.
- Search and study of effective light-matter interfaces, a study of the interaction of non-classical states of light with individual quantum objects and ensembles.
- Development of principles and methods of quantum metrology;
- Development of relativistic quantum information theory and quantum communication based on combining the concepts of relativistic quantum theory and information theory.

3.2. Scientific and technical problems in the field of quantum computing

Creation, analysis and implementation of elements of quantum computing devices and quantum simulators using:

- Spin states in specially designed condensed media having specially created ensembles of atoms or molecules with electronic or nuclear spin. For example, these can be shallow donors or in single crystals of isotopically pure 28Si, NV-complexes in diamond, etc .;
- States of ensembles of ions, neutral atoms or molecules (including highly excited Rydberg states) in electromagnetic (for example, optical) traps or inert media;
- Semiconducting and superconducting quantum multicomponent structures demonstrating relaxation to the ground state through "quantum annealing", including phenomena and devices based on hybrid

semiconducting or superconducting quantum structures with weakly interacting molecules included in them;
- Opto-nanomechanical and magneto-nanomechanical quantum systems;
- States of linear and nonlinear optical (including microwave) systems in high-quality resonators;
- States of specially synthesized molecular and supramolecular systems, in particular, polynuclear complexes, hybrid systems with charge separation;
- Topological quantum states, condensates of various particles and quasiparticles, structures based on new carbon materials, etc.

3.3. Scientific and technical problems in the field of architecture and algorithms and quantum computing

- Development of algorithms for quantum computing (including algorithms for quantum modeling and quantum tomography; correction of quantum errors to compensate for the loss of coherence; accuracy assessment);
- Development of architectural and software principles of hybrid supercomputers containing quantum computers;
- Development of methods for collecting and analyzing large amounts of data from quantum computing devices using supercomputers;
- Qualitative and quantitative characterization of confused multi-qubit quantum states as the main information resource in quantum informatics;
- Synthesis and optimization of quantum circuits (including the synthesis of reversible circuits for calculating Boolean functions; reduction of the depth of a quantum circuit; quantum technologies for testing and repairing digital circuits on crystals).

4. Conclusion

The use of photons, both for transmission and for information processing, presupposes the creation of new principles and technologies of integrated photonic devices both for distributed quantum communication lines and for classical optoelectronic or all-optical integrated devices. It is also necessary to develop atomic-scale technologies, with the use of which it is possible to "assemble" elements of systems from individual atoms or molecules. In this regard, the development of new physical principles and approaches are required to create the necessary materials and structures, new experimental methods and metrological support.

Cryptography is an important component of the modern world and is necessary primarily for the preservation of personal data and important information. Since its inception, it has undergone many modifications and is now a security system that practically cannot be hacked. It is difficult to overestimate its potential for humanity. Modern methods of cryptography are used in almost all industries in which there is a need for secure transmission or storage of data. Based on the fact that the latest developments in the field of quantum cryptography make it possible to create systems that provide almost 100% protection of the key and key information, it can be assumed that shortly all cryptographic information protection and key distribution will be based on quantum cryptographic systems[9,10].

5. Discussion and Suggestions

- Development and creation of photon sources, including one, two and N-photon, the creation of photon detectors, including single-photon, the creation of optical and microwave amplifiers with a quantum level of input noise, high-Q resonators "on a chip", quantum systems for coherent photon conversion, etc.,
- Development and creation of new materials and basic elements for problems of quantum communication and quantum information processing, including photonic materials, structures and fiber systems for the generation of special quantum states of light;
- Development and creation of quantum memory systems (including photonic ones) and the creation of practically significant quantum memory with high efficiency, long lifetime, high information capacity, as well as the ability to work at room temperature;
- Development and creation of quantum generators of random bit sequences;

- Design and creation of quantum interfaces, i.e. elements for setting the initial state of "qubits" before computation and elements for reading quantum states of "qubits" after computation. (For example, to read the state of spin qubits, one-electron transistors with a Coulomb blockade or devices based on spin-dependent transport and spin-dependent reactions can be used);
- Design and creation of "quantum wires" for the transfer of a quantum state between registers in a quantum computer.

References

[1] Cryptography and data encryption - everything you need to know. [Electronic resource]. - Access mode: https://prostocoin.com/blog/cryptography. - Date of access: 15.04.2020.

[2] Hardware Quantum Cryptography. [Electronic resource]: http://fkn.ktu10.com. - Date of access: 15.04.2020.

[3] Journal of Science and Technology "Popular Mechanics" [Electronic resource] - Access mode: https://www.popmech.ru/technologies/235655 kvantovayakriptografiya-chto-eto-takoe. - Date of access: 15.04.2020.

[4] Quantum cryptography, or how light generates encryption keys. [Electronic resource] - Access mode: https://www.osp.ru/school. - Date of access: 15.04.2020.

[5] Krasavin, V. Quantum cryptography [Electronic resource] - Access mode: https://ru.b-ok.cc/book/628590/bbd531. - Date of access: 15.04.2020.

[6] Imre, S. Gvongyosi, L. Advanced Quantum Communications: An Engineering Approach, John Wiley & Sons, 2012.

[7] Segienko, A. V. Quantum Communications and Cryptography, CRC Press, 2018.

[8] Imre, S Quantum Communications: Explained for Communication Engineers, IEEE Communications Magazine 51(8), 2013.

[9] Xin, S. Conti, A. Long, G. Muller, P. Sayeed, A. Yuan, J. Hanz, L. Guest Editorial Advances in Quantum Communications, Computing, Cryptography, and Sensing, IEEE Journal on Selected Areas in Communications 38(3), 2020.

[10] Arun, G. Mishra, V. A review on quantum computing and communication, 2nd International Conference on Emerging Technology Trends in Electronics, Communication and Networking,2014.

[11] Morimae, T. Nishimura, H. Rational proofs for quantum computing 20(3-4), 181-193, 2020.

[12] Mavroeidis, V. Vishi, K. Zych, M.D. Jøsang, A. The Impact of Quantum Computing on Present Cryptography, International Journal of Advanced Computer Science and Applications, 9(3), 2018.