ANNOTATION

Dissertation work on the topic: "METHODS OF SECURE KEY DISTRIBUTION BASED ON QUANTUM CRYPTOGRAPHY PROTOCOLS" submitted for the degree of Doctor of Philosophy (PhD) in the specialty 6D070400 - "Computer Engineering and Software"

YUBUZOVA KHALICHA IBRAGIMOVNA

Relevance of the research topic. In modern information and communication systems, the main method of ensuring data confidentiality is cryptography. Currently, as a rule, methods of symmetric and asymmetric cryptography are used, which, in addition to advantages, have certain disadvantages. Symmetric cryptosystems have a high speed and cryptographic resistance to attacks, but their use raises the difficult problem of distributing secret keys.

There are several ways to solve this problem, for example, the use of asymmetric cryptographic systems. However, the methods of asymmetric cryptography also have significant drawbacks. Asymmetric cryptosystems are relatively slow, and their cryptographic resistance to attacks is explained by the impossibility of an effective computational solution of NP-hard problems (factorization, logarithm in large discrete fields, etc.). However, with the development of technology, a rapid increase in productivity and a simultaneous reduction in the cost of computing tools, as well as with the discovery of new, more efficient algorithms for solving some NP-hard problems (Shor's, Grover's algorithms, etc.), the confidentiality and reliability provided by the traditional cryptography.

In addition, the threat of secrecy to modern classical ciphers is the possibility of the emergence of stable multi-qubit quantum computing systems, quantum computers.

In this regard, of great interest is quantum cryptography (QC), which is based on the use of specific properties of quantum systems that serve as information carriers in quantum cryptography protocols. When solving some problems of information security, QC makes it possible to achieve information-theoretic stability that does not depend on the attacker's computational and other capabilities. Over the past decades, QC has gone from laboratory experiments to the implementation of full-fledged commercial solutions.

Several works by leading domestic and foreign scientists are devoted to the development of the theory and practice of quantum cryptography, among them Akhmetov B., Bennet C., Brassard J., Vasiliou E., Gnatiuk S., Diamanti E., Zhmurko T., Zavadsky P., Zenevich A., Kilin S., Lam P., Lutkenhaus N., Renner R., Rumyantsev K., Holevo A.S., Yavich M., et al.

Most of the research results are associated with increased security (up to the information-theoretic level) and data transfer rate using QC protocols. As a rule, these indicators are interdependent and an increase in the level of resistance will

undoubtedly lead to a decrease in the speed of processing and data transfer. This reduces the efficiency of real-time encryption key distribution. In this regard, the development of modern methods for improving the efficiency of the distribution of encryption keys based on quantum cryptography protocols is an urgent scientific and technical task, which is of theoretical and practical importance for the development of QC.

Purpose of the study. The purpose of this work is to develop models for the secure distribution of secret keys and increase the efficiency of their distribution through the using of a combined model based on quantum cryptography protocols.

The goal set determined the main objectives of the dissertation.

1. Analysis of modern methods, models, and commercial systems for distributing encryption keys according to security (security) and speed criteria.
2. Development of a threat model and an intruder model in quantum cryptographic systems.
3. Development and research of a quantum deterministic protocol model in the eavesdropping control mode.
4. Development and research of a quantum deterministic protocol model in the message passing the mode.
5. Development of a combined model with modes of eavesdropping control and transmission of quantum deterministic protocol messages with pairs of entangled qutrits.
6. To offer a new method for secure key distribution of the combined model with eavesdropping and message transmission control modes of the quantum deterministic protocol.

The object of the study is the process of distributing encryption keys to ensure the confidentiality of data transmission in the ICS.

The subject of research is methods and models of secure key distribution based on quantum cryptography protocols.

Research methods - methods of information security theory; theories of cryptography and cryptanalysis; quantum information theory; theory of quantum mechanics.

Modern application packages were used:

- Matlab R2018a;
- Microsoft Visual Studio 2016;
- Wolfram Mathematica 7;
- C++.

The scientific novelty of the obtained results.

The following results were obtained in the dissertation work:

- based on the results of the analysis of the current state in the field of quantum cryptography and communication, the shortcomings of existing methods of key distribution were identified, and the classification of quantum cryptographic methods was expanded, which allows expanding the possibilities for choosing the necessary quantum cryptographic methods for building secure encryption key distribution systems;

- the model of a quantum deterministic protocol in the eavesdropping control mode has been developed, taking into account the features of a quantum channel and the probability of an error occurring in it. It makes it possible to ensure secure and fast distribution of keys, to formulate practical recommendations for the development of quantum cryptographic systems in the conditions of using a depolarization quantum channel and the presence of an intruder;

- the model of a quantum deterministic protocol in the message transfer mode has been developed, which makes it possible to increase the level of accessibility of a quantum channel when a key is transmitted by a deterministic protocol with a low level of natural noise;

-the method for enhancing secrecy using quantum entangled states and generated ternary pseudo-random sequences is proposed, which makes it possible to increase the transmission rate without loss of resistance of deterministic quantum cryptography protocols using pairs of qutrits to an incoherent attack;

- for the first time, a combined model was implemented based on the developed models of the eavesdropping and message transmission control mode of a quantum deterministic protocol with pairs of entangled qutrits using the proposed method of enhancing secrecy. This made it possible to improve the method of secure key distribution, increase the speed, and ensure the noise immunity of the depolarization quantum channel.

The practical significance of the obtained results.

The obtained scientific results and the developed models of a quantum deterministic protocol with an eavesdropping control mode and a message transmission mode with pairs of entangled qutrits are of practical value for solving the problem of key distribution, for improving the efficiency of cryptographic information protection systems.

Also developed:

- the threat model allows forming of conceptual aspects of attack prevention and formalizes the capabilities of preventive systems in the process of their development or improvement;

- the abstract model of the intruder in QC systems allows you to determine the set of measures of a different nature that need to be additionally implemented to ensure reliable protection using specific quantum systems;

- software and simulation of the quantum deterministic protocol:

- the model in the eavesdropping control mode made it possible to increase the rate of distribution of encryption keys by at least 1.52 times while ensuring protection against incoherent attacks;

- the model in the message transmission mode, allowed to obtain confirmation of the possibility of using the proposed system of error-correcting coding over the Galois field GF (3^2) at a natural noise level of up to 10%, to increase the level of availability of a quantum channel when transmitting a key by a deterministic protocol by at least 3.8%.

The results of the study were used in the educational process of the Department of Cybersecurity, processing, and storage of information of KazNRTU named after K.I. Satpayev (the act of implementation dated 09/02/2018), National Aviation

University (Kyiv, Ukraine) (the act of implementation dated 05/09/2018), EE «Belarusian State Academy of Telecommunications» (Minsk, Belarus) (the act of implementation dated 02/11/2018) and AxxonSoft (Kyiv, Ukraine) (the act of implementation dated 10/29/2018).

The author's contribution consists of:

- models of the quantum deterministic protocol in the eavesdropping control mode and models in the message passing the mode have been developed;
- the first model provides secure and fast distribution of keys, as well as the formulation of practical recommendations for the development of quantum cryptographic systems in the conditions of using a depolarization quantum channel and the presence of an intruder. Experiments have shown that it was possible to increase the rate of distribution of encryption keys by at least 1.52 times and provide protection against incoherent attacks;
- the second model provides an increase in the level of availability of the quantum channel when the key is transmitted by a deterministic protocol with a low level of natural noise. According to the results of experiments using the noise-immune coding system proposed by the applicant over the Galois field GF (3^2), at a natural noise level of up to 10%, the level of availability of the quantum channel was increased by at least 3.8%;
- a new method for enhancing the secrecy of trit deterministic protocols, a statistically stable algorithm for generating trit pseudo-random sequences, as well as practical recommendations for the use of quantum deterministic protocols in quantum cryptographic systems in the conditions of using a depolarization quantum channel and the presence of an intruder.

Approbation of work. The main results of the study were reported and discussed at scientific seminars of the Institute of Information and Telecommunication Technologies, at the Department of Computer and Software Engineering, KazNRTU named after. K.I. Satpaev, in the research work «Quantum cryptographic methods for protecting the critical information infrastructure of the state» No. 161-DB17 (state registration 0117U006770) of the National Aviation University (**Ukraine, Kyiv),** at the International Forum dedicated to the 80th anniversary of KazNTU named after K.I. Satpayev «Engineering education and science in the XXI century: Problems and prospects» (**Almaty, 2014**), at the International Satpayev readings «The role and place of young scientists in the implementation of the Kazakhstan-2050 strategy» (**Almaty, 2014**), at the II International scientific and practical conference «Information and telecommunication technologies: education, science, practice» (**Almaty, 2015**); at the II International scientific and practical conference «Actual issues of ensuring cybersecurity and information protection» (**Ukraine, Kyiv**, **2016, 2017, 2018**); at the International Scientific and Practical Conference ITSEC: Information Technology Security (**Ukraine, Kyiv, 2016**); at the International Scientific Conference UNITEX'16 (**Bulgaria, Gabrovo, 2016**); at the III International Scientific and Practical Conference «Information Security and Computer Technologies» **(Ukraine**, **Kropyvnytskyi, 2018**); at the XIV International Conference on ICT in Education. «Research and Industrial Applications.

Integration, Harmonization and Knowledge Transfer» (**Ukraine, Kyiv, 2018**); at the International Conference «Information and Telecommunication Technologies and Radio Electronics – UkrMico» (**Ukraine, Odessa, 2018**); at the XVII International Conference on Computer Information Systems and Industrial Management Applications (**Russia, Moscow, 2018**); at the International Scientific Conference «Modern Communications» (**Belarus, Minsk, 2018**); at the VIII World Congress «Aviation in the XXI-st century - Safety in Aviation and Space Technologies» (**Ukraine, Kyiv, 2018**); at the VIII International Scientific and Technical Conference «Infocommunications - Modernity and Future» (**Ukraine, Odessa, 2018**); at the IV International scientific and practical conference «Actual nutritional security of cybersecurity and protection of information» (**Ukraine, Kyiv, 2021**); at the VII International scientific and practical conference «Actual nutritional security of cybersecurity and protection of information» (**Ukraine, Kyiv, 2021**); at the IV International Scientific and Practical Conference «Department of Information Systems and Technologies. Integration of information systems and intelligent technologies in the conditions of information society transformation» (**Ukraine, Poltava, 2021**).

Publications. Based on the results of research on the topic of the dissertation, 36 papers were published, of which 6 articles are included in the Scopus/Web of Science database, 3 articles in journals recommended by the Committee for Quality Assurance in Education and Science of the Ministry of Education and Science of the Republic of Kazakhstan, 3 articles in foreign journals and 21 articles were published in the proceedings of international scientific and practical conferences in Kazakhstan and abroad.

The volume and structure of the dissertation. The dissertation work consists of an introduction, four sections, a conclusion and a list of sources used, and three appendices. The work is presented on 144 pages of typewritten text and contains 54 figures, 24 tables, and a list of references from 103 titles.

Summary of the dissertation.

The introduction reveals the relevance of the research topic, the goals and objectives of the research, research methods, scientific novelty and practical significance of the results obtained, personal contribution and approbation of the work.

In the first section of the dissertation work, a literature review and analysis of the current state of methods, models and commercial systems for distributing encryption keys according to security (security) and speed criteria are carried out. Based on the results of the review and analysis, a classification of quantum cryptographic methods was obtained, which allows expanding the possibilities when choosing the necessary quantum cryptographic methods for building secure encryption key distribution systems.

In the second section of the work, the developed extended classification of quantum cryptographic methods for distributing encryption keys is presented; abstract models of threats and an intruder in quantum cryptography systems, features of the implementation of an incoherent attack in quantum cryptography systems

based on deterministic protocols are proposed. The resulting models allow you to determine and select the most secure methods for distributing cryptographic keys.

The third section presents the developed models: quantum deterministic protocol in the eavesdropping control mode; quantum deterministic protocol in message passing mode; a new method of secrecy enhancement using quantum entangled states and generated ternary pseudo-random sequences is proposed. A combined model is also implemented based on the developed models of the control mode of eavesdropping and message transmission of a quantum deterministic protocol with pairs of entangled qutrits using the proposed method of enhancing secrecy.

The fourth section presents practical implementations in the MATLAB environment of simulation modeling of a quantum deterministic protocol in the eavesdropping control mode; simulation modeling of a quantum deterministic protocol in the message-passing mode; simulation modeling, a combined quantum deterministic protocol with an eavesdropping control mode and a message-passing mode, with secrecy enhancement. Practical recommendations are formulated for the use of quantum deterministic protocols in quantum-cryptographic systems under the conditions of using a depolarization quantum channel and the presence of an intruder.

The conclusion reflects the main results and conclusions of the dissertation work.