ABSTRACT

of the dissertation for the degree of Doctor of Philosophy (PhD) in the educational program 8D06301 – " Information security systems"
Amirkhanova Dana Sairangazhykyzy
« Lattice – Based Post – Quantum Public Key Encryption Scheme using ElGamal's Principles »

Relevance of the Research Topic. Modern technologies, such as quantum and cloud calculating, reshape the calculating landscape, offering unparalleled computing power and scalability. While these advancements promise significant benefits, they also pose challenges to the security of classical cryptographic structures. Quantum computing, with its potential to exponentially accelerate computations, threatens the safety of widely used public-key cryptosystems like Rivest-Shamir-Adleman(RSA) , Elliptic Curve Cryptography(ECC) and El-Gamal's via algorithms like Shor's algorithm, which efficiently aspects large integers and solves discrete logarithm problems. As quantum computers progress, the cryptographic algorithms safeguarding our digital security may become susceptible to attacks, necessitating the development of quantum-resistant cryptographic primitives. Cloud computing, on the other hand, introduces new security concerns surrounding data privacy, confidentiality, and integrity. While it offers convenient access to vast computational resources and storage, it also raises issues such as unauthorized data access, breaches, and insider threats. Securing data in the cloud requires robust cryptographic mechanisms, secure communication protocols, and stringent access controls. In reply to the challenges posed by quantum calculating and evolving computing technologies, lattice-based cryptography has emerged an interesting solution, on the basis of the hardness of lattice problems like the (SIS) Short Integer Solution problem. This paper presents a novel quantum- resistant cryptography public key encryption scheme on the basis of lattices, using ElGamal's principles. The scheme is on the basis of (SIS) Short Integer Solution problem. The scheme incorporates a key exchange protocol grounded the SIS problem, ensuring safety against both quantum and classical adversaries. The construction is simple and provides the solution for secure data transmission in modern cryptographic environments. This advancement underscores the ongoing evolution of cryptography to meet the challenges posed by quantum computing and emerging technologies. Considering the above, it can be concluded that there is currently a pressing need for effective methods and algorithms to enhance protection against quantum attacks through the use of a lattice-based ElGamal approach.

Research Objective: Development of a method for creating an improved lattice-based post-quantum public-key cryptography scheme using the principles of ElGamal.

Research Tasks:

1) Analysis of popular methods and algorithms of traditional cryptography and their resilience in the context of post-quantum cryptography.

2) Research on lattice-based key distribution schemes.

3) Development of a model for an efficient and secure post-quantum key exchange scheme based on lattices using the principles of ElGamal.

4) Development of an algorithm and a prototype of a post-quantum public-key cryptosystem based on lattices, utilizing the principles of ElGamal.

5) Research and testing of the efficiency of the proposed post-quantum cryptosystem.

Research Objects: The objects of the study are the processes of cryptographic data protection using public-key schemes against classical and quantum attacks.

Research Methods: Classical Cryptography, parameter sizes, lattice theory, evaluation of algorithm efficiency, experimental testing.

Scientific Novelty:

- A mathematical model for an efficient and secure post-quantum key exchange scheme based on lattices using the principles of ElGamal has been developed, which enables the creation of efficient post-quantum public-key schemes for cryptographic protocols, authentication systems, financial systems, blockchain and IoT technologies..
- An algorithm and prototype of a post-quantum public-key scheme based on lattices using the principles of El-Gamal have been developed, which has increased the speed of generating encryption keys is 240-583 times (compared to analogues - LWE, Ring-LWE), and successfully resistant to quantum attacks (compared to the classical El-Gamal scheme).

The theoretical significance and practical significance.The theoretical significance of this research lies in its contribution to advancing the development of cryptographic systems that are resistant to quantum attacks, and in broadening the scope for applying mathematical methods in the field of information security. The practical significance is demonstrated by the application of the developed algorithm and software, which can be further utilized in the evolution of other technologies that provide security against both quantum and classical threats. The developed scheme is simple and efficient in terms of speed, offering a solution for secure data transmission in modern cryptographic environments. This achievement highlights the ongoing evolution of cryptography in addressing challenges related to quantum computing and cloud computing technologies.

Key Provisions Submitted for Defense:

1. A mathematical model of an efficient and secure post-quantum key exchange scheme based on lattices and the principles of ElGamal encryption has been developed. This enables the creation of effective public-key post-quantum schemes for use in cryptographic protocols, authentication systems, financial systems, blockchain, and IoT technologies.

2. An algorithm and prototype of a post-quantum public-key encryption scheme based on lattices using ElGamal principles have been developed. The proposed scheme achieved a 240–583 times increase in encryption key generation speed (compared to analogues such as LWE and Ring-LWE), and demonstrated resistance to quantum attacks (in comparison to the classical ElGamal scheme).

3. A theoretical security model of the cryptosystem has been proposed and substantiated in accordance with the IND-CCA standard, with a reduction to the SIS problem in the quantum random oracle model (QROM), which ensures formal resistance of the scheme against quantum attacks.

Validation of the Work.The main provisions and results of the dissertation research were presented and discussed at the scientific seminars of the Department of "Cybersecurity, Information Processing and Storage" of KazNITU named after K. I. Satpayev, in the IIWT laboratory, as well as at SCSA and Caucasus University.

Validity of the Results. The validity and reliability of the results of the dissertation are confirmed by publications in journals recommended by the Committee for Quality Assurance in the Field of Education and Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan, as well as in international indexed journals included in the Web of Science and Scopus databases (e.g., MDPI, Switzerland), in international scientific conferences, and by comparison with results obtained by other researchers.

Relation to Government Programs. The topic of the dissertation is directly related to the priorities set out in the Cybersecurity Concept “Cyber Shield of Kazakhstan”, approved by the Resolution of the Government of the Republic of Kazakhstan dated June 30, 2017, No. 407 (as amended and supplemented by the Order of the Minister of Science and Higher Education of the Republic of Kazakhstan dated March 17, 2023, No. 236).The "Cyber Shield of Kazakhstan" Concept identifies the formation of a stable and secure digital environment as a key direction of state policy in the field of national security. One of its strategic goals is the development of information security that is resilient to emerging threats, including those arising from the advancement of quantum technologies.

In this context, the development of post-quantum cryptographic solutions — such as the scheme proposed in the dissertation — aligns with the objectives of the Concept. The presented research is aimed at creating a domestic cryptographic technology that is resistant to quantum attacks and can be applied to protect information and communication infrastructure, critical assets, financial systems, as well as in the context of digital transformation and protection of national data.

Publications:

1) Dana Sairangazhykyzy Amirkhanova, Maksim Iavich and Orken Mamyrbayev.*Cryptography* 2024, *8*(3),31. https://doi.org/10.3390/cryptography

8030031 (Scopus, процентиль 66,Web of Science – Q2).”Lattice- based Post-Quantum Public Key Encryption Scheme Using ElGamal’s Principles”.

2) Dana Amirkhanova., Orken Mamyrbayev., Bulletin of ABAI KAZNPU. Series: Physical and mathematical sciences volume 83 № 3(2023). “Cryptographic analysis of the scheme of polylinear cryptography”.

3) Dana Amirkhanova., Orken Mamyrbayev., Bulletin NAS RK: Vol: Physico-Mathematical Series ISSN 1991-346X Volume 3. № 351 (2024).“El-Gamal’s Cryptographic Algorithm: Mathematical Foundations, Applications And Analysis”.

4) Dana Amirkhanova., Orken Mamyrbayev., Bulletin EKTU: Vol: Information and communication technologies ISSN 1561-4212 № 1(2025))“Research And Development of a Cryptography Algorithm Based on Polylinear Algebra Using Blockchain Methodology”.

Structure and Volume of the Dissertation:

The dissertation research consists of an introduction, 3 chapters, a conclusion, a list of references containing 85 titles, and appendices. The work is presented on 96 pages and includes 39 figures and 1 table.

In the introduction, the relevance of the topic is discussed, and the problems associated with the research subject are specified. The research objective and tasks, the scientific novelty and practical value of the work, and the research methods are presented.

In the first chapter of the dissertation, an analysis of popular methods and algorithms of traditional cryptography is presented, revealing their vulnerability to quantum attacks, since quantum algorithms can effectively break such systems. Post-quantum cryptography and its importance in modern cryptography are also examined, as it offers methods and algorithms that are resistant to attacks by quantum computers.

In the second chapter of the dissertation, an analysis of existing lattice-based key distribution schemes was conducted, confirming their high resistance to quantum attacks due to the complexity of the underlying computational problems. Based on this analysis, a model of an efficient and secure key exchange scheme utilizing lattice methods and the principles of El-Gamal was developed. This combination ensures a high level of cryptographic strength and performance, making the proposed solution practically applicable in modern information security systems.

In the third chapter, based on a software implementation, an algorithm and a prototype of a post-quantum public-key scheme using lattice methods and the principles of El-Gamal were developed. The study also includes the evaluation and testing of the efficiency of the proposed cryptosystem, and a theoretical security model is substantiated in accordance with the IND-CCA standard, with a reduction to the SIS problem in the quantum random oracle model (QROM), which ensures the formal resistance of the scheme to quantum

attacks. Furthermore, the system showed high operational speed, making it promising for practical application.

The conclusion presents the main results and findings of the dissertation.