Volume 3, Issue 2, February - 2025 **ISSN (E):** 2938-3811

ENSURING THE SECURITY OF QUANTUM SYSTEMS: ALGORITHMS AND METHODS

Saidakhmedov Eldor Islomovich
Denov Institute of Entrepreneurship and Pedagogy
Teacher of the Department of Information Technologies
techmespeaker@gmail.com
0009-0001-4349-1765

Qahhorova Nargiza Xayit qizi
Denov Institute of Entrepreneurship and Pedagogy
Computer Engineering Student
qahhorovanargiza02@gmail.com

Toshtemirova Sarvara To'lqin qizi
Denov Institute of Entrepreneurship and Pedagogy
Student of Mathematics and Informatics
Toshmuradova201@gmail.com

Abstract
This article reviews the main algorithms and methods aimed at ensuring the security of quantum systems. The article provides detailed information about important technologies such as quantum cryptography, post-quantum cryptography, and quantum error correction. Algorithms such as Quantum Key Distribution (QKD), Lattice-based cryptography, Hash-based signatures, and Surface Codes are used to ensure the security of quantum systems. These algorithms ensure the confidentiality, integrity, and availability of information.
The article covers the latest achievements in the field of quantum system security and emphasizes the importance of research and development in this area. Along with the development of quantum technologies, algorithms for ensuring their security are also constantly being improved.
This article is a useful resource for those interested in the fields of information security, cryptography, and quantum computing.

Keywords: Quantum systems, quantum security, quantum encryption (Quantum Cryptography), quantum key distribution (QKD), post-quantum cryptography (Post-Quantum Cryptography), Lattice-based cryptography, Hash-based signatures, quantum error correction (Quantum Error Correction), Surface Codes, Cryptographic algorithms, Information security.

Introduction

Quantum systems have ushered in a new era in modern information technology. They have incredible capabilities in processing information compared to classical computers. However, quantum systems can also be subject to security threats. Therefore, special algorithms and methods have been developed to ensure the security of quantum systems. In this article, we

Web of Scientists and Scholars: Journal of Multidisciplinary Research

will discuss the main algorithms used to ensure the security of quantum systems and their applications.
The following algorithms are used to ensure the security of quantum systems:

Quantum Cryptography: Quantum cryptography is a method of protecting data based on the fundamental principles of quantum mechanics. The most famous example of this is Quantum Key Distribution (QKD). Through QKD, a secret key is exchanged between two parties, and this key is based on the principles of quantum security.
BB84 Protocol: This is the most popular QKD protocol, which uses the quantum states of photons. Any attempt to access the data is immediately detected and the data is secured.
BB84 The protocol consists of the following steps.
BB84 The protocol uses the polarization states of photons. Photons can be represented in the following two bases:
+ **Bazis (Rectilinear basis):** Photons are horizontal ($|0\rangle$) and vertical ($|1\rangle$) may be in some cases.
× **Bazis (Diagonal basis):** Photons 45° ($|+\rangle$) va 135° ($|-\rangle$) can be in states.
The states of photons are represented as follows:
$|0\rangle = (1, 0)$
$|1\rangle = (0, 1)$
$|+\rangle = (1/\sqrt{2}, 1/\sqrt{2})$
$|-\rangle = (1/\sqrt{2}, -1/\sqrt{2})$

Post-kvant kriptografiya (Post-Quantum Cryptography): Post-quantum cryptography was developed to combat the ability of quantum computers to break classical encryption algorithms. These algorithms are based on mathematical problems that are resistant to quantum computers.

Lattice-based kriptografiya: This method is based on mathematical lattices and is considered resistant to quantum attacks. The advantages of this type of cryptographic system are as follows.
Quantum resistance: Lattice problems are also considered difficult for quantum computers.
1. Efficiency: Lattice-based algorithms run relatively fast.
2. Flexibility: Lattice-based systems can be used for various tasks such as signing, encryption, and key exchange.

Hash-based signatures: Methods based on hash functions, such as the SPHINCS+ algorithm, provide protection against quantum attacks**.**

Code-based cryptography: Methods based on error-correcting codes, such as the McEliece encryption system, are considered resistant to quantum attacks.

Application of algorithms in quantum security

Data Encryption: Post-quantum cryptography algorithms protect data against quantum attacks. For example, Lattice-based encryption systems are currently used in many applications.

Secret key exchange: Through QKD protocols (such as BB84), a secret key is exchanged between two parties. Using this key, data is transmitted securely.

Quantum network security: Quantum networks use quantum error correction algorithms to transmit data. This increases the reliability of the networks**.**

Conclusion

Ensuring the security of quantum systems is of great importance for modern information technologies. The confidentiality, integrity and availability of information are ensured through algorithms such as quantum encryption, post-quantum cryptography and quantum error correction. In the future, as quantum technologies develop, their security algorithms will also be constantly updated.

Research and development in the field of quantum system security plays an important role in bringing humanity to a new technological stage.

References

1. Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information. Cambridge University Press. Kvant hisoblash va kvant axborot nazariyasiga oid asosiy manba.
2. Shor, P. W. (1999). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM Review, 41(2), 303–332.
3. Bennett, C. H., & Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, 175–179.
4. Regev, O. (2009). On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. Journal of the ACM, 56(6), 1–40. Lattice-based kriptografiya va Learning With Errors (LWE) muammosi haqida batafsil ma’lumot.
5. Bernstein, D. J., & Lange, T. (2017). Post-Quantum Cryptography. Nature, 549(7671), 188–194.Post-kvant kriptografiyaning zamonaviy yondashuvlari va algoritmlari.
6. Yakubov S., Khushbokov I., Saidakhmedov E. Calculation results for optimization of underground structures //American Institute of Physics Conference Series. – 2024. – T. 3154. – №. 1. – С. 020053.