

THE IMPACT OF QUANTUM COMPUTING ON CYBERSECURITY

Вінницький національний технічний університет

Анотація. У статті розглядається вплив квантових обчислень на кібербезпеку та можливості вирішення проблеми вразливості сучасних методів шифрування. Підкреслюються переваги квантово-стійкої криптографії для захисту цифрових систем.

Ключові слова: квантові обчислення, постквантова криптографія, кібербезпека.

Abstract. The article considers the impact of quantum computing on cybersecurity and the possibilities to solve the problem of vulnerability of current encryption methods. The advantages of quantum-resistant cryptography for safeguarding digital systems are emphasized.

Keywords: quantum computing, post-quantum cryptography, cybersecurity.

Introduction

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use. This would seriously compromise the confidentiality and integrity of digital communications on the Internet and elsewhere [1].

This work aims to understand how the rise of quantum computing will reshape cybersecurity. Quantum computers threaten to disrupt the cryptographic foundations of modern digital systems, potentially exposing sensitive data and undermining trust in digital communications. As a result, the development and adoption of quantum-resistant algorithms have become critical to ensuring long-term security in a post-quantum era.

Statement of basic materials

Quantum computing is a concept based on the quantum theory of physics, which deals with nature at the quantum level. A quantum is the minimum amount of a physical entity that can be considered for computing. The idea behind quantum computing is to operate the computers on extremely short pulses of light. This is practical, can speed up the operation of computers by 100,000 times. Therefore, a quantum computer can exponentially process large amounts of data better than classical computers [2].

The most pressing concern in the intersection of quantum computing and cybersecurity is the potential vulnerability of current encryption methods. Modern cryptographic systems, such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), rely on the computational complexity of mathematical problems like integer factorization and discrete logarithms. These problems are extremely difficult for classical computers to solve, forming the backbone of secure communications today [3].

However, quantum computers, leveraging algorithms such as Shor's algorithm, can solve these problems exponentially faster than classical systems. This capability threatens to render widely used encryption methods obsolete, exposing sensitive data, compromising digital signatures, and undermining the security of online transactions and communications. While large-scale, fault-tolerant quantum computers do not yet exist, the rapid pace of quantum advancements makes this threat a foreseeable reality.

Quantum-resistant cryptography, also known as post-quantum cryptography, is designed to protect data from the advanced capabilities of quantum computers.

One of the most promising approaches in this field is lattice-based cryptography, which relies on the complexity of mathematical problems related to multidimensional grids of points, known as lattices. The security of lattice-based methods is built on the difficulty of solving problems like the Shortest Vector Problem (SVP) and the Learning With Errors (LWE) problem. These problems are currently resistant to both classical and quantum algorithms, making lattice-based cryptography a strong candidate for securing data in the quantum era. Another key approach in quantum-resistant cryptography is hash-based cryptography, which leverages the computational security of cryptographic hash functions. These methods use hash functions to create digital signatures, ensuring data integrity and authenticity. A well-known example is the Merkle Signature Scheme (MSS), which provides a secure way to sign data. Both lattice-based and hash-based cryptography offer robust solutions to the challenges posed by quantum computing, ensuring that encrypted information remains protected even as quantum technology evolves [4].

As quantum computing continues to advance, the transition to quantum-resistant cryptographic systems becomes increasingly urgent. While lattice-based and hash-based cryptography represent significant progress, their widespread adoption requires further research, standardization, and integration into existing infrastructures. Organizations and governments must collaborate to develop comprehensive strategies for implementing these solutions, ensuring a seamless transition to post-quantum security. Additionally, ongoing efforts to evaluate the performance, scalability, and practicality of these methods will be critical to their success in real-world applications. By addressing these challenges proactively, the global community can mitigate the risks posed by quantum computing and safeguard the future of digital communication and data protection.

Conclusion

The study highlights the urgent need for post-quantum cryptography to address the threats posed by quantum computing. Quantum computers can break modern cryptographic systems. This capability undermines the security of digital communications, financial systems, and sensitive data, making the development of quantum-resistant solutions a top priority.

The implementation of quantum-resistant methods is essential for safeguarding digital systems in the quantum era. However, their successful adoption will require further research, standardization, and collaboration to address challenges related to performance, scalability, and integration with existing infrastructures. By proactively embracing these solutions, the global community can effectively counter the threats posed by quantum computing and ensure the continued security of digital information. This transition will not only protect current systems but also pave the way for a more secure and resilient digital future.

REFERENCES

1. <https://csrc.nist.gov/projects/post-quantum-cryptography>
2. <https://www.sciencedirect.com/topics/computer-science/quantum-computing>
3. <https://www.metacompliance.com/blog/cyber-security-awareness/quantum-computing-cybersecurity>
4. <https://www.computer.org/publications/tech-news/trends/quantum-resistant-cryptography>

Рудницька Тетяна Григорівна – старший викладач кафедри іноземних мов, Вінницький національний технічний університет, e-mail: rudnytska@vntu.edu.ua

Кубіря Варвара Іванівна – студентка групи ІКІТС-236, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: vkubiria@gmail.com

Rudnytska Tetiana Hryhorivna an Assistant Professor of Foreign Languages Department, Vinnytsia National

Technical University, e-mail: rudnytska@vntu.edu.ua

Kubiria Varvara Ivanivna – student of group 1KITS-23b, Faculty of Management and Information Security,
Vinnytsia National Technical University, Vinnytsia, email: vkubiria@gmail.com