UDC 004.056.55:004.8

A. V. Shurman
V. V. Chopliak

POST-QUANTUM CRYPTOGRAPHY: PROTECTING DATA IN THE AGE OF QUANTUM COMPUTING

Vinnytsia National Technical University

Анотація

Дана робота присвячена дослідженню викликів, які постають перед сучасною кібербезпекою у зв'язку з розвитком квантових обчислень. Розглядається вразливість традиційних алгоритмів шифрування, таких як RSA та ECC, перед алгоритмом Шора. Основна увага приділяється концепції постквантової криптографії (PQC) та аналізу нових математичних підходів, що здатні протистояти квантовим атакам. Досліджується необхідність своєчасного переходу на нові стандарти безпеки в інженерній практиці.

Ключові слова: квантові обчислення, постквантова криптографія, алгоритм Шора, шифрування, інформаційна безпека.

Abstract

This paper investigates the challenges facing modern cybersecurity due to the advancement of quantum computing. It examines the vulnerability of traditional encryption algorithms, such as RSA and ECC, to Shor's algorithm. The primary focus is on the concept of Post-Quantum Cryptography (PQC) and the analysis of new mathematical approaches capable of resisting quantum attacks. The necessity for a timely transition to new security standards in engineering practice is explored.

Keywords: quantum computing, post-quantum cryptography, Shor's algorithm, encryption, information security.

Introduction

As quantum computing technology approaches "quantum supremacy," the foundation of global digital security is under threat. While classical computers would take billions of years to crack modern 2048-bit RSA encryption, a sufficiently powerful quantum computer could achieve this in hours using Shor's algorithm. For computer engineers, this necessitates a fundamental shift in how hardware and software security architectures are designed. Post-Quantum Cryptography (PQC) aims to develop cryptographic systems that are secure against both quantum and classical computers, ensuring data remains protected in the coming decades.

Research results

The transition to quantum-resistant security involves several critical areas of research and implementation.

- Vulnerability of asymmetric encryption. Most current digital signatures and key exchange protocols rely on the difficulty of factoring large integers or solving discrete logarithm problems. Quantum computers excel at these specific mathematical tasks, making current PKI (Public Key Infrastructure) obsolete in a post-quantum world.
- Lattice-based cryptography. This is one of the most promising candidates for PQC. Unlike RSA, lattice-based problems involve finding the shortest vector in a complex multi-dimensional grid, a task that remains computationally "hard" even for quantum processors. These algorithms are currently being standardized by NIST (National Institute of Standards and Technology).
- Hash-based and code-based signatures. Other alternatives include hash-based digital signatures, which offer high security levels and are already well-understood, though they often result in larger signature sizes, posing challenges for memory-constrained embedded systems in computer engineering.
- The "Harvest now, decrypt later" threat. A significant reason for immediate action is that malicious actors may be intercepting and storing encrypted sensitive data today, intending to decrypt it once powerful quantum computers become available. This makes the implementation of PQC urgent for long-term data privacy.

Conclusion

The era of quantum computing will redefine the limits of computational power and cybersecurity. Computer engineers must lead the migration to post-quantum algorithms to prevent a global security crisis. While the hardware for large-scale quantum attacks is still in development, the mathematical and engineering foundations for defense must be integrated into IT systems today to ensure a secure digital future.

REFERENCES

1. National Institute of Standards and Technology (NIST). (2024). Post-Quantum Cryptography Standardization: https://csrc.nist.gov/projects/post-quantum-cryptography.
2. Cloudflare Learning. (2025). What is post-quantum cryptography: https://www.cloudflare.com/learning/ssl/quantum/what-is-post-quantum-cryptography/.
3. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188-194.
4. IBM Quantum. (2024). Quantum-Safe Strategy: Preparing for the Quantum Future: https://www.ibm.com/quantum/quantum-safe.
5. Nykyporets, S. S., Kot, S. O., Boiko, Y. V., Melnyk, M. B., & Chopliak, V. V. (2024). Advanced integration of virtual information environments (VIEs) in contemporary educational methodologies. *Society and National Interests. Series "Education/Pedagogy"*, 4(4), 139-154. https://doi.org/10.52058/3041-1572-2024-4(4)-139-154.
6. Nykyporets, S. S., Kot, S. O., Hadaichuk, N. M., Herasymenko, N. V., & Kukharchuk, H. V. (2025). Advancing critical thinking skills in future engineers through the analysis of AI-generated and AI-verified English-language sources. *Current Issues in Modern Science. Series "Pedagogy",* 8(38), 1143-1155. https://doi.org/10.52058/2786-6300-2025-8(38)-1143-1155.
7. Sachaniuk-Kavets'ka, N. V., & Nykyporets, S. S. (2025). Developing critical thinking in students of technical specialties through the mathematics of uncertainty and educational debates in English: An integrated experimental-methodological model. *Bulletin of Science and Education. Series "Pedagogy"*, 11(41), 1524-1541. https://doi.org/10.52058/2786-6165-2025-11(41)-1524-1541.
8. Ibrahimova, L. V., & Nykyporets, S. S. (2025). Information security in the global context: Linguistic perspectives and the role of English. In *International security studies: Managerial, technical, legal, environmental, informative and psychological aspects* (Vol. II, pp. 321-345). ISAP, Research and Education. DOI: https://doi.org/10.5281/zenodo.15356365.
9. Nykyporets, S. S., & Kukharchuk, H. V. (2025). Intercultural communication in information security: Risks, conflicts, and educational opportunities for English language teachers. In *International security studies: Managerial, technical, legal, environmental, informative and psychological aspects* (Vol. II, pp. 398-420). ISAP, Research and Education. DOI: https://doi.org/10.5281/zenodo.15356424.

Шурман Артем Віталійович – студент групи 1ПІ-25Б, Факультет Інформаційних Технологій та Комп'ютерної Інженерії, Вінницький національний технічний університет, Вінниця, e-mail: artshurman08@gmail.com.

Науковий керівник: ***Чопляк Вікторія Володимирівна*** – викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: nikavnuchkova@gmail.com.

Artem Shurman – student of group 1PI-25B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: artshurman08@gmail.com.

Scientific Supervisor: ***Victoriia V. Chopliak*** – teacher of English, Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, e-mail: nikavnuchkova@gmail.com.