004.415.2:004.056

S. S. Sarafinchan
V. V. Chopliak

METHODOLOGY OF SOFTWARE ARCHITECTURE MIGRATION TO POST-QUANTUM CRYPTOGRAPHIC ALGORITHMS

Vinnytsia National Technical University

Анотація

Публікація присвячена дослідженню архітектурних стратегій переведення сучасних програмних систем на квантово-стійкі стандарти шифрування. Розглядається вплив постквантових криптографічних алгоритмів на затримку системи, споживання пам'яті та накладні витрати під час передачі даних. Визначено, що впровадження гнучких криптографічних рівнів (cryptographic agility) дозволяє програмним компонентам адаптуватися до мінливих вимог безпеки без необхідності повного редизайну системи.

Ключові слова: архітектура ПЗ; постквантова криптографія; криптографічна гнучкість; безпека даних; методологія міграції; квантові обчислення.

Abstract

The publication is devoted to the analysis of architectural strategies for transitioning modern software systems to quantum-resistant encryption standards. The impact of post-quantum cryptographic algorithms on system latency, memory consumption, and data transmission overhead is examined. A structured migration framework is proposed to isolate cryptographic primitives from the core business logic, thereby preventing architectural rigidity. It is determined that the implementation of agile cryptographic layers allows software components to adapt to evolving security requirements without requiring complete system redesign.

Key words: software architecture; post-quantum cryptography; cryptographic agility; data security; migration methodology; quantum computing.

Introduction

Within the modern software engineering ecosystem, data security remains a foundational quality attribute. However, the rapid advancement of quantum computing poses a critical threat to traditional asymmetric encryption methods, such as RSA and ECC, which rely on the mathematical complexity of integer factorization and discrete logarithms [1]. The eventual emergence of cryptographically relevant quantum computers necessitates an immediate architectural shift toward lattice-based and code-based cryptographic primitives. A significant challenge for software engineers is the "cryptographic rigidity" inherent in legacy codebases, where security protocols are deeply intertwined with core functionalities [2]. Consequently, a systematic methodology is required to decouple encryption mechanisms, ensuring a seamless and secure migration to post-quantum standards while maintaining system stability, scalability, and performance.

Research results

The investigation indicates that a successful transition to quantum-resistant software depends heavily on the implementation of cryptographic agility within the system architecture [2]. This study identifies a three-tiered architectural framework designed to mitigate the performance overhead associated with larger key sizes and increased computational demands of post-quantum algorithms [4].

First, an isolation layer must be introduced via architectural patterns such as the Abstract Factory or Dependency Injection [3]. By separating the instantiation of cryptographic services from the execution logic, components can switch between classical and post-quantum algorithms at runtime based on the security context or data classification. This approach minimizes technical debt and preserves code maintainability.

Second, the structural integration of hybrid encryption schemes is evaluated. Due to the unverified long-term stability of initial post-quantum algorithms, combining a classical cipher with a quantum-resistant

primitive provides a dual-layer defense mechanism. Utilizing the Decorator pattern allows developers to dynamically wrap existing data streams with post-quantum encapsulation keys without modifying the underlying transport protocols.

Finally, experimental analysis demonstrates that network protocols experience increased payload sizes during the key exchange phase of lattice-based algorithms [1]. To balance scalability and security, a microservices-based routing strategy is recommended, where computationally intensive cryptographic verifications are offloaded to dedicated, independently scalable authentication services.

Conclusion

The research demonstrates that migrating software systems to post-quantum cryptography is an architectural challenge rather than a simple dependency update. By establishing cryptographic agility through structured design layers, software engineers can significantly reduce the complexity of system updates. While the integration of quantum-resistant algorithms introduces additional latency and memory constraints, the long-term benefit of a secure, sustainable, and future-proof architecture justifies the initial development overhead. Ultimately, proactive architectural adaptation is a strategic necessity that protects digital assets against future quantum threats.

REFERENCES

1. Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). Post-Quantum Cryptography. Springer Science & Business Media.
2. Bass, L., Clements, P., & Kazman, R. (2021). Software Architecture in Practice (4th ed.). Addison-Wesley Professional.
3. Gamma, E., Helm, R., Johnson, R., & Vlissides, J. (1994). Design Patterns: Elements of Reusable Object-Oriented Software. Addison-Wesley.
4. National Institute of Standards and Technology (NIST). (2024). Federal Information Processing Standards (FIPS) – Post-Quantum Cryptography Standardized Algorithms. NIST Computer Security Resource Center. – URL: https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
5. Kot, S. O., & Nykyporets, S. S. (2025). Activating students' cognitive engagement in technical English learning with AI tools. In *Science and education in the third millennium: Information technology, education, law, psychology, social security and work, management. International collective monograph* (Vol. I, pp. 295-332). Lublin, Polska: Institute of Public Administration Affairs. DOI: https://doi.org/10.5281/zenodo.16942267.
6. Nykyporets, S. S., & Hadaichuk, N. M. (2025). Foreign language media literacy as a protective factor against AI-generated disinformation and psychological stress in technical higher education in Ukraine. In *Transformational vectors of public administration, law, and humanities in the development of the modern educational system: Scientific monograph* (pp. 305-330). Baltija Publishing. https://doi.org/10.30525/978-9934-26-647-8-14.
7. Nykyporets, S. S., Herasymenko, N. V., & Chopliak, V. V. (2025). Developing digital language competence as a factor of competitiveness of future master's degree holders in power engineering in the digital economy. In O. H. Cherep (Ed.), *Artificial intelligence as a tool to protect the economy disinformation: Innovative solutions and international practices: Collective monograph* (pp. 140-193). Baltija Publishing. DOI: https://doi.org/10.30525/978-9934-26-586-0.

Сарафінчан Софія Славівна – студентка групи 2ПІ-25б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: mega.sofia2008@gmail.com.

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

Sofiia S. Sarafinchan – a student of 2SE-25b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: mega.sofia2008@gmail.com.

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