Science and Innovation

Volume 6, Issue 4, pp. 45-63

Published 2024/11/20

DOI: 10.12345/si.2024.4.003

Post-Quantum Cryptography: Preparedness Assessment for National Digital Infrastructures

Authors: Davit Kurtanidze, Ana Gegeshidze, Zviad Lortkipanidze

Abstract

Quantum computing poses an existential threat to current public-key cryptographic standards. This paper assesses the preparedness of national digital infrastructures in transitioning to post-quantum cryptographic (PQC) algorithms as standardized by NIST in 2024. We evaluate the technical, institutional, and economic dimensions of PQC adoption across 12 countries, developing a readiness index and identifying key implementation gaps. Results show that while awareness has grown significantly, fewer than 30% of assessed institutions have begun concrete migration planning.

Keywords: quantum computing, post-quantum cryptography, NIST, cybersecurity, digital infrastructure

References

NIST (2024). Post-Quantum Cryptography Standards. National Institute of Standards and Technology.

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188?194.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38?41.

Campagna, M., et al. (2015). Quantum safe cryptography and security. ETSI White Paper No. 8.