# Implementing Post-Quantum Cyber Security in Financial Systems

**Dr. Nadav Voloch**
Senior Lecturer and Head of Cyber, Department of Computer Engineering, Ruppin Academic Center, Israel

## Abstract

Quantum computing poses a substantial threat to classical cryptographic systems, especially those safeguarding financial infrastructures. This paper examines the critical need for post-quantum cryptography (PQC) integration in financial systems, addressing the vulnerabilities of RSA, ECC, and Diffie-Hellman algorithms to quantum attacks. We explore standardized PQC algorithms selected by NIST—Kyber for key encapsulation, and Dilithium, Falcon, and SPHINCS+ for digital signatures—highlighting their implementation potential in real-world financial applications. The research emphasizes hybrid cryptographic models as essential transitional tools for maintaining backward compatibility during the migration to quantum-resilient security frameworks. In particular, we analyze the feasibility of deploying post-quantum TLS 1.3 in financial communications and blockchain systems. Furthermore, the study reviews performance trade-offs, regulatory considerations, and implementation methodologies necessary for large-scale adoption. Our findings advocate a phased, proactive integration strategy, underscoring that delay in PQC adoption could expose financial institutions to future quantum threats. By adopting robust cryptographic frameworks today, financial systems can ensure long-term security and resilience in a rapidly evolving technological landscape.

## Keywords

Post Quantum Cryptography (PQC), Cybersecurity, Encryption, Financial Systems, Quantum Resilience.