Quantum Cybersecurity for the Financial Sector

Efe Büke
American Collegiate Institute

Abstract*—The exponential growth of digital finance—encompassing online banking, digital assets, decentralized finance (DeFi), and algorithmic trading—has intensified the need for robust cybersecurity frameworks. However, the rise of quantum computing presents a dual challenge: while it enables revolutionary advances in data analytics and optimization, it simultaneously threatens the cryptographic foundations of contemporary financial systems. This research explores the emerging field of quantum cybersecurity and its implications for safeguarding financial infrastructures in the post-quantum era. Traditional encryption methods such as RSA, ECC, and Diffie–Hellman key exchange are vulnerable to quantum attacks, particularly through Shor's algorithm and Grover's search algorithm, which can efficiently break asymmetric and symmetric cryptographic schemes. The study evaluates quantum-resistant cryptographic protocols—including lattice-based, hash-based, and multivariate polynomial encryption—as viable solutions for ensuring financial data integrity, transaction confidentiality, and regulatory compliance in quantum-vulnerable environments. Furthermore, it investigates Quantum Key Distribution (QKD) and Quantum Random Number Generation (QRNG) as hardware-assisted techniques for achieving unconditional security in financial communications and transaction authentication. By integrating quantum cryptography, hybrid encryption, and AI-driven threat modeling, this work outlines a roadmap for financial institutions transitioning toward quantum-secure infrastructures. The findings demonstrate that quantum cybersecurity is not merely a defensive measure but a transformative enabler for resilient digital finance, aligning with global efforts to achieve technological sovereignty, financial stability, and sustainable innovation in the era of quantum computing.

The financial sector operates as one of the most data-sensitive and technologically dynamic domains in the global economy. Its infrastructures—from digital banking networks and payment gateways to high-frequency trading systems and blockchain-based assets—are critically dependent on encryption technologies for secure communication, authentication, and record-keeping [3]. As quantum computing advances, it poses both unprecedented opportunities and existential risks to this digital ecosystem. While quantum processors promise computational acceleration in portfolio optimization, fraud detection, and financial modeling, they also possess the capacity to decrypt existing cryptographic standards, threatening the confidentiality and integrity of vast financial datasets [2].

At the core of this threat lies the power of Shor's algorithm, which can factor large integers exponentially faster than classical computers, undermining the security assumptions of RSA and elliptic-curve cryptography [1]. Likewise, Grover's algorithm offers quadratic speedups for brute-force attacks on symmetric encryption, significantly reducing the effective key strength of widely used algorithms such as AES [7]. These capabilities render the current cybersecurity infrastructure of financial institutions obsolete in a post-quantum scenario, necessitating the rapid adoption of quantum-resistant and hybrid encryption models.

Digital Object Identifier 10.62802/p9hhgn28

Date of publication 18 11 2025; date of current version 18 11 2025

