Quantum Computing and Cryptography in Banking

A. Xyz[1], B.A. Author[2], C.D.E. Thirdauthor[2], Corresponding Author[1,*]
[1] *Department, University, City, Country*
[2] *Institute, City, Country*
(* Corresponding Author Email: xyz@gmail.com or institute specific email)

Online banking is a crucial financial service but faces growing cyber threats. Traditional encryption methods like RSA and ECC, though widely used, are at risk due to advancing quantum computing. This paper explores quantum computing's role in securing online banking, analyzing cyberattacks such as the Cosmos Bank heist and C-Edge ransomware attack. It introduces solutions like Quantum Key Distribution (QKD) and Post-Quantum Cryptography (PQC) for enhanced security.

Online Banking Security Threats:
Data breaches: Unauthorized access to sensitive financial data.
Man-in-the-Middle attacks: Interception of communication between users and banks.
Credential theft (phishing): Obtaining user credentials through social engineering.
Ransomware: Encrypting financial data and demanding payment for decryption.

Classical cryptographic methods, including RSA and ECC, rely on mathematical problems that are difficult for conventional computers but solvable by quantum computers using algorithms like Shor's Algorithm. With advancements in quantum computing, current encryption methods risk being compromised, necessitating the transition to quantum-safe security measures

Types of Quantum Computing for Bank Security
Quantum Key Distribution (QKD): Secure communication based on quantum mechanics for encryption key distribution.
Post-Quantum Cryptography (PQC): Quantum-resistant algorithms for long-term security.
AES-256: A stronger symmetric encryption method that remains quantum-resistant.
Quantum Random Number Generation (QRNG): Uses quantum mechanics to generate truly random numbers, making cryptographic keys more secure.

Table 1 Comparison of Classical vs. Quantum Security in Banking

Parameter	Classical Algorithms	Quantum Security
Key Distribution	RSA, ECC (vulnerable to QC)	QKD (Quantum-secured)
Encryption Strength	AES-128, RSA-2048	AES-256, Post-Quantum Cryptography
Random Number Generation	Pseudo-Random Generators	Quantum Random Number Generation
Security Against Attacks	Susceptible to brute-force	Resistant to quantum attacks

Conclusion:
With the emergence of quantum computing, banking security must evolve beyond traditional encryption methods. Implementing QKD, PQC, and quantum-resistant encryption strategies can safeguard financial institutions from future cyber threats. The transition to quantum-safe cryptography is essential to ensure the continued security of online banking and financial systems.

Reference(s):
1. Quantum Key Distribution, Wikipedia.
2. Post-quantum cryptography, Wikipedia.
3. Cryptography in the Banking Industry ,*Arpan Kumar Kar.*