Title: Quantum Computing's Impact on Modern Cryptography

Abstract: This paper explores how quantum computing, particularly Shor's algorithm, poses a threat to current cryptographic systems and discusses emerging quantum-resistant alternatives.

1. Introduction to Quantum Computing Quantum computing uses quantum bits (qubits) to perform computations exponentially faster than classical computers for specific problems.
2. Shor's Algorithm and Its Threat to RSA Encryption Developed by Peter Shor in 1994, Shor's algorithm can factor large integers in polynomial time. This capability threatens RSA encryption, which relies on the difficulty of factoring large numbers. For example, a 2048-bit RSA key could be broken in hours with a sufficiently powerful quantum computer.
3. Quantum-Resistant Cryptographic Alternatives
    - Lattice-Based Cryptography: Based on the hardness of lattice problems, resistant to quantum attacks.
    - Hash-Based Cryptography: Uses hash functions for secure digital signatures, such as Lamport signatures.
    - Code-Based Cryptography: Relies on error-correcting codes, e.g., McEliece cryptosystem.
4. Conclusion As quantum computing advances, transitioning to quantum-resistant cryptography is critical for future security.

References: - Shor, P. W. (1994). Algorithms for quantum computation.