Quantum Computing vs. Encryption: Is Cybersecurity Under Seige?

Tazkia Malik, Sharmila Surovi, Homaira Zahin

Computer Science and Engineering, University of Dhaka

Abstract

This poster articulates the imminent threat of quantum computing to established cryptographic standards, particularly algorithms such as RSA and ECC. As quantum computer capabilities advance, the security of these foundational systems is at risk. Investigating Post-Quantum Cryptography (PQC) is essential for developing quantum-resistant algorithms that can mitigate these emerging threats. This research explores various PQC methodologies, including lattice-based and hash-based techniques, which demonstrate resilience against quantum attacks.We also assess the cybersecurity sector's readiness for this shift, highlighting the need for proactive measures to protect sensitive information in a quantum-enabled future.

Fig. 1

Objective

- **Impact Assessment:** Evaluate the vulnerabilities of RSA and ECC in the context of quantum computing. This assessment will inform necessary adaptations to existing systems.
- **Risk Analysis:** Investigate the implications of quantum threats on encrypted systems. Understanding these implications is vital for proactive security measures.
- **Development of Post-Quantum Solutions:** Examine the creation and standardization of quantum-resistant cryptographic algorithms. This development is essential for securing data against future quantum attacks.
- **Long-term Research Directions:** Advocate for the transition to quantum-safe systems to ensure future data security.

Outcome

Expected Outcomes: Quantum Computing vs. Encryption

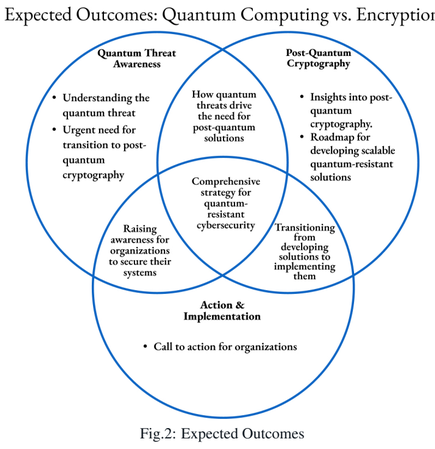


Fig.2: Expected Outcomes

Methodology

Quantum computing threatens encryption methods by utilizing qubits, which can exist in a superposition state represented as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$

This allows quantum algorithms, like Shor's, to factor large integers in polynomial time $O((\log N)^2 \log\log N)$, while classical methods require exponential time $O(e^{(\log N)^{1/3}(\log\log N)^{2/3}})$. Consequently, widely used systems like RSA and ECC, which rely on the difficulty of integer factorization, become vulnerable. The entanglement of qubits enables complex computations that further undermine traditional security protocols.

Bits against Qubits

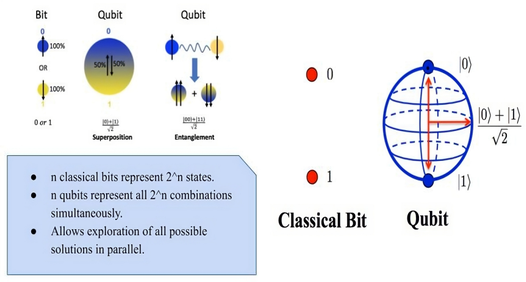


Fig. 3

Evolution

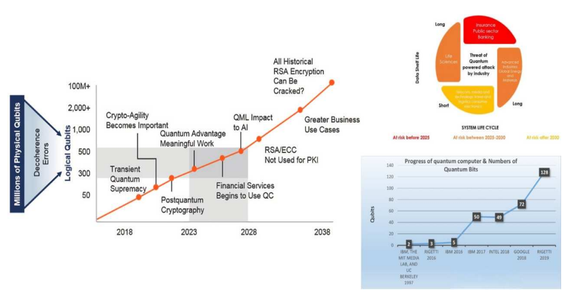


Fig. 4

Existing Encryption Systems and Their Vulnerabilities: Current encryption systems, including RSA and ECC, are vulnerable to quantum computers using Shor's algorithm for factoring large integers and computing discrete logarithms. Symmetric methods like AES are also at risk from Grover's algorithm, which reduces key length and weakens security.

Currently existing Cryptographies

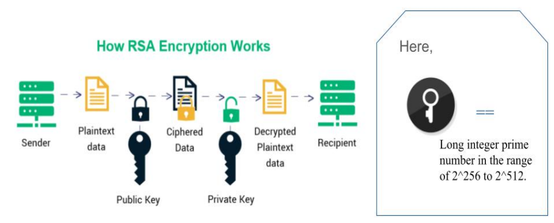


Fig. 5

How it Happens?

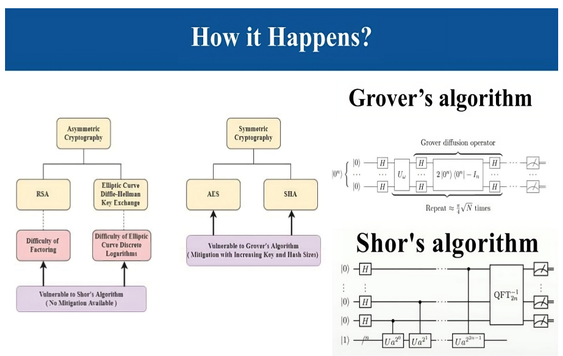


Fig. 6

Navigating Quantum Threats: The concern is addressed by Post-Quantum Cryptography (PQC), which aims to develop algorithms resilient to quantum threats. Key candidates include lattice-based schemes like Kyber and Dilithium, as well as hash-based systems like SPHINCS+. Lattice-based cryptography relies on hard mathematical problems, such as the Learning With Errors (LWE) problem, which poses challenges for quantum algorithms. Given a matrix $A \in \mathbb{Z}_q^{m \times n}$, a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$, and an error distribution χ, the LWE problem involves finding $\mathbf{s}$ given the samples:

$$\mathbf{y}_i = A\mathbf{s} + \mathbf{e}_i \mod q$$

where $\mathbf{e}_i$ is a small error vector from χ, and q is a prime modulus. In the Kyber cryptosystem, the public key pk is computed as:

$$pk = A \cdot \mathbf{s} + \mathbf{e} \mod q$$

Hash-based cryptography uses secure hash functions that exhibit quantum resistance, particularly for digital signatures. In SPHINCS+, the signature σ for a message m is computed as:

$$\sigma = H(m \parallel sk) \mod N$$

where H is a secure hash function, sk is the secret key, and N is a modulus for reduction.
Hash functions must satisfy several security properties:

- **Pre-image Resistance:** For a given hash value h, it should be hard to find m such that $H(m) = h$.
- **Second Pre-image Resistance:** For a given message m_1, it should be hard to find m_2 such that $H(m_1) = H(m_2)$.
- **Collision Resistance:** It should be hard to find distinct messages m_1 and m_2 such that $H(m_1) = H(m_2)$.

Classic Vs PQC?

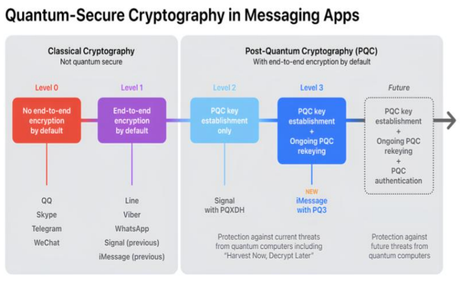
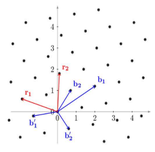


Fig. 9

Lattice-Based Cryptography

A lattice is a grid-like structure that extends infinitely in multiple directions. Cryptographic systems based on lattices rely on hard mathematical problems such as the Shortest Vector Problem (SVP) and Learning with Errors (LWE).



Hash-Based Cryptography

Hash-based schemes use cryptographic hash functions to provide secure digital signatures. The security of these systems depends on the pre-image resistance, collision resistance, and second pre-image resistance of the underlying hash function.

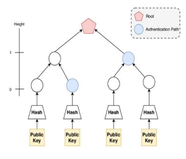


Fig. 10

Comparison

Quantum computers vastly surpass classical counterparts, solving complex problems such as factoring and database searching in minutes rather than years through algorithms like Shor's and Grover's.

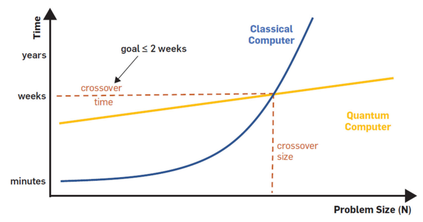


Fig. 11: Quantum Computing Vs. Classical Computing

Feasibility

Quantum advancements could compromise current cryptographic systems, such as RSA, within 10-30 years, making this threat increasingly imminent.

- **Lattice-Based Cryptography:** Supported by strong theoretical foundations, with NIST actively leading standardization efforts, making it feasible for future implementation.
- **Hash-Based Cryptography:** Proven quantum-resistant for digital signatures, though its application to broader encryption is limited.
- Transitioning to post-quantum cryptography (PQC) requires infrastructure updates but is feasible with ongoing research and industry adoption.

Conclusion

To conclude, the rapid advancement of quantum computing presents a significant threat to conventional cryptographic systems, such as RSA. This situation underscores the urgent need for research into quantum-resistant solutions like post-quantum cryptography. As these technologies continue to evolve, they may compromise the security of sensitive data and communications. Therefore, it is essential to enhance cybersecurity measures to mitigate the risks associated with quantum technology, ensuring the protection of critical information in an increasingly digital landscape

References

1. National Institute of Standards and Technology (NIST). Post-Quantum Cryptography Standardization.
2. Shor, Peter. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer." SIAM Journal on Computing.
3. Grover, Lov. "A Fast Quantum Mechanical Algorithm for Database Search." Proceedings of the 28th Annual ACM Symposium on Theory of Computing.
4. Bernstein, Daniel J., et al. "Post-Quantum Cryptography." Springer, 2009.
5. Mosca, Michele. "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" Institute for Quantum Computing.