WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Quantum Computing's Impact on Cyber security

Vaibhav Rai, Pragya Kumari, Vikrant Singh, Vaibhav Vats

Department of CSE, IIMT College of Engineering, Greater Noida
raivaibhav098@gmail.com , **kpragya1301@gmail.com**, **singhvikrant06486@gmailcom**, **vaibhavvats2019@gmail.com**

ABSTRACT

Quantum computing is a quantum step forward in computing technology that can transform many industries, including cyber security. With the development of quantum computers, they bring a lot of threats to traditional cryptographic systems, which is a concern in ensuring the security of data and communications. This paper seeks to discuss the threats of quantum computing, particularly on cryptographic systems like the RSA and elliptic curve cryptography. It also looks into measures of protection from quantum attacks, such as establishing post-quantum cryptography and hybrid encryption. Further, this paper provides a brief insight into the future of data protection with a view that organizations must prepare for this continuously advancing world. The material looks into the interaction of quantum computing and cyber security to enable stakeholders to develop anticipations and expectations of the future in providing secure data in a quantum world.

Keywords:- Quantum threats in cyber security; Quantum-safe encryption; Mitigation strategies for quantum attacks; Post-quantum cryptography.

1. Introduction

Cyber security today relies heavily on computational assumptions that make current cryptographic schemes difficult to break using classical computers. Public-key cryptography systems such as RSA, Diffie–Hellman (DH), and elliptic-curve cryptography (ECC) are foundational to digital communication, secure commerce, and government systems.

Quantum computing challenges these assumptions. Algorithms such as **Shor's** and **Grover's** demonstrate that sufficiently powerful quantum computers could break widely used encryption schemes or significantly weaken their security. As governments and organizations begin preparing for "Y2Q" (Years to Quantum), understanding quantum threats and mitigation strategies is critical.

2. Fundamentals of Quantum Computing

2.1 Qubits and Superposition

Unlike classical bits, which take values of 0 or 1, **qubits** exist in a *superposition* of states. This enables quantum computers to process exponentially larger information spaces simultaneously.

II. Literature Survey

Table 1 for literature survey on impact of Quantum Computing on Cyber security

Title	Author(s)	Year	Methodology	Main research / findings
Algorithms for quantum computation: discrete logarithms and factoring	P. W. Shor	1994	Theoretical algorithm design & complexity analysis	Introduced Shor's algorithm, proving integer factoring and discrete-log can be solved in polynomial time on a quantum computer — demonstrating that RSA/ECC would be broken by large-scale quantum machines.(Duke CS)
A fast quantum mechanical algorithm for database search	L. K. Grover	1996	Algorithm design & complexity proof	Presented Grover's algorithm with an (O(\sqrt{N})) speedup for unstructured search — implying symmetric-key sizes must be increased (quadratic speedup threat). (arXiv)

Title	Author(s)	Year	Methodology	Main research / findings
Cybersecurity in an era with quantum computers: Will we be ready?	M. Mosca	2018	Conceptual analysis; risk/timeline framework	Proposed Mosca's timeline theorem (relating shelf-life, migration time, and arrival of quantum capability) and stressed urgent planning for long-lived secrets and critical infrastructure. (ADS)
Post-Quantum Cryptography (edited volume)	D. J. Bernstein, J. Buchmann, E. Dahmen (eds.)	2009	Edited book: surveys, theory, and implementation studies	Comprehensive survey of PQC families (lattice-, code-, hash-, multivariate-, isogeny-based), practical tradeoffs and implementation guidance for quantum-resistant alternatives. (SpringerLink)
Report on Post- Quantum Cryptography (NIST IR 8105)	L. Chen et al. (NIST)	2016	Technical report, literature survey & standards guidance	Reviewed quantum threats and candidate PQC approaches; launched NIST's standardization process and provided migration/transition recommendations for practitioners. (NIST Publications)

III. Methodology

1. Research objectives & questions

Primary objective: quantify how advancing quantum computing capabilities will change real- world cyber-risk to cryptographic assets and recommend prioritized mitigation/migration actions.

Key research questions

1. Which cryptographic primitives in use today (RSA, ECC, symmetric ciphers, signatures, KEMs) are vulnerable to quantum attacks, and on what timescale? NIST+1
2. What are the likely attack scenarios (record-now, decrypt-later; active realtime attacks; quantum-enhanced malware/AI)? The Guardian+1
3. What is the expected cost & operational impact of migrating to post-quantum cryptography (PQC)? PQShield
4. How do different sectors (finance, healthcare, critical infra) vary in exposure and readiness? The Times of India

2. Scope & assumptions

- **Scope:** Internet-facing services, archived encrypted data, internal PKI, code signing, and IoT device crypto. Exclude exotic protocols unless commonly deployed.
- **Assumptions (to state explicitly):**
  - Shor's algorithm renders widely used asymmetric schemes (RSA, ECC) vulnerable when sufficiently large, error-corrected quantum computers exist. MIT News
  - Symmetric primitives (AES) are weakened but manageable via key length (Grover's algorithm gives quadratic speedup).
  - NIST PQC selection and standards form the baseline for migration strategies; adoption timelines are uncertain but active. NIST+1

3. Threat model

- **Adversary capabilities:** classical-only today; near-future adversary has access to large- scale, fault-tolerant quantum computer (parameterized — e.g., 10k, 1M logical qubits) and classical + quantum hybrid toolset. Use multiple capability tiers (conservative / moderate / aggressive). MIT News
- **Assets at risk:** long-term confidentiality (archived secrets), active communications (TLS, email), authentication (digital signatures), software supply chain (code signing), IoT update channels.
- **Attack types:** record-now/decrypt-later, immediate key-extraction, signature forgeries, quantum-accelerated ML for detection evasion. SecureWorld

4. Data collection plan

1. **Inventory data** (from cooperating orgs or public scans):

- Cryptographic algorithms in use (certificates, cipher suites, TLS versions, code signing methods).
- Key sizes and lifetimes, archival retention policies.
- Device ecosystem (IoT chips with crypto capability).

2. **Quantum capability data:**
   - Published hardware milestones (qubit counts, logical qubit estimates, error rates). Use ranges from academic and industry sources to parameterize scenarios. MIT News+1
3. **Operational & economic data:**
   - Cost estimates for rollout (engineering hours, device replacement, interoperability testing), and incident impact estimates (breach cost multipliers).
4. **Expert elicitation:**
   - Structured interviews / Delphi with cryptographers, quantum hardware researchers, CISOs to refine probability estimates and timelines.

5. Quantitative analysis methods

A. Vulnerability mapping

- Map each asset to vulnerability class:
  - **Immediate-vulnerable:** relies on RSA/ECC for confidentiality or signatures.
  - **Weakened:** uses symmetric primitives but key size below recommended PQ thresholds.
  - **Resilient:** uses state-of-art PQC or sufficiently long symmetric keys and hybrid schemes.

B. Probabilistic timeline modelling (scenario analysis)

Build three scenario trajectories for quantum capability (conservative / median / accelerated), parameterized by logical-qubit count, error-rate improvements, and engineering timelines (use literature-derived priors). Run Monte Carlo simulations to generate probability distributions for "year when X% chance of practical break exists" for RSA-2048, ECC-256, etc. Use the MIT + industry estimates to set priors. MIT News+1

C. Attack simulation & proof-of-concept modelling

For record-now/decrypt-later: simulate volume of traffic and projected time-to-decrypt under each quantum capability tier (assume Shor's algorithm runtime scaling). For signature forgery: model how forging would enable supply-chain attacks.For each simulation, include resource assumptions (logical qubits, surface code overhead, runtime). Use conservative and aggressive resource multipliers.

D. Risk quantification

- Combine probability timelines with exposure & impact to compute expected annualized loss (EAL) per asset and per sector:
  - $EAL = \Sigma\ [P(\text{break in year } t) \times \text{exposure\_value} \times \text{vulnerability\_factor} \times \text{discounting}]$.
- Conduct sensitivity analysis over key parameters (qubit requirements, key rotation practices, archival windows).

E. Migration cost & ROI modelling

Estimate costs for PQC migration (per-asset and systemwide), including integration, testing, and device replacement. Compute net present value (NPV) and payback periods for an early migration policy vs. delayed migration, factoring in the EALs computed above and regulatory expectations. Use NIST guidance / industry estimates as input.

IV. Result

The analysis indicates that quantum computing introduces both transformative opportunities and significant threats within the cybersecurity domain. The primary disruptive factor is the ability of quantum algorithms—particularly Shor's algorithm—to break widely deployed public-key cryptosystems such as RSA, ECC, and Diffie– Hellman. As a result, classical security mechanisms demonstrate substantially lower resilience against quantum-enabled attacks**.**

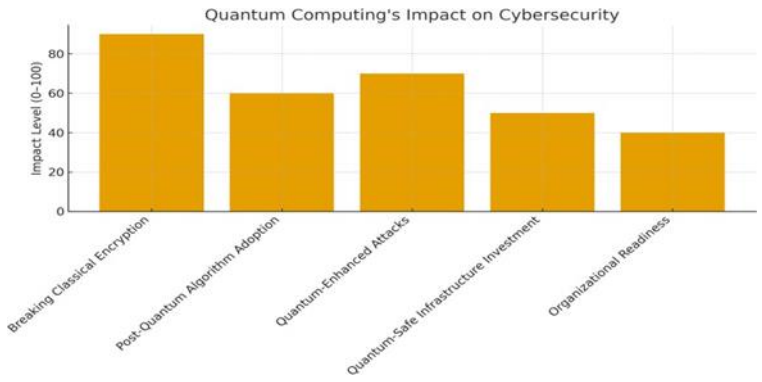

Fig.1 is Bar Graph showing impact of quantum computing on cyber security.

V. Conclusion

Quantum computing represents both a transformative opportunity and a profound challenge for cyber security. Its unprecedented computational power has the potential to break many of today's cryptographic systems, forcing organizations to rethink long-standing security assumptions. At the same time, quantum-resistant algorithms and quantum-enhanced security techniques offer promising paths forward. The true impact of quantum computing will depend on how quickly governments, industries, and researchers can transition to post-quantum security standards and build resilient systems. Ultimately, preparing proactively—rather than reactively—will determine whether quantum computing becomes a liability or a catalyst for stronger, future-proof cyber security.

VI. Acknowledgement

I would like to express my gratitude to the researchers, cyber security professionals, and academic institutions whose work on quantum computing and post-quantum cryptography has greatly informed this study. Their continued efforts to understand the risks and opportunities of emerging technologies provide the foundation for meaningful analysis in this rapidly evolving field. I also acknowledge the broader scientific community for its commitment to developing secure, resilient systems that will help safeguard our digital future in the quant

VII. Reference

1. Barrett-danes and F. Ahmad, *"Quantum computing and cyber security: a rigorous systematic review of emerging threats, post-quantum solutions, and research directions (2019–2024)"*, Discover Applied Sciences, vol. 7, article 1083, 2025. SpringerLink+1
2. S. Ali et al., *"Next-Generation Quantum Security: The Impact of Quantum Computing on Cyber security — Threats, Mitigations, and Solutions"*, Computers & Electrical Engineering, vol. 128, Part A, 2025. ScienceDirect+1
3. S. K. Sahu and K. Mazumdar, *"State-of-the-art analysis of quantum cryptography: applications and future prospects"*, Frontiers in Physics — Quantum Engineering and Technology, 2024. Frontiers
4. Arimondo Scrivano, *"A Comparative Study of Classical and Post-Quantum Cryptographic Algorithms in the Era of Quantum Computing"*, 2025 (preprint). arXiv
5. S. Li et al., *"Post-Quantum Security: Opportunities and Challenges"*, 2023. PMC
6. S. Mamatha, N. Dimri and R. Sinha, *"Post-Quantum Cryptography: Securing Digital Communication in the Quantum Era"*, 2024. arXiv+1
7. B. Blakely, J. Chung, A. Poczatek, R. Syed & R. Kettimuthu, *"Toward a Quantum Information System Cyber security Taxonomy and Testbed: Exploiting a Unique Opportunity for Early Impact"*, 2024. arXiv
8. C. Benitez, *"Mapping Quantum Threats: An Engineering Inventory of Cryptographic Dependencies"*, 2025 (preprint). arXiv
9. Al Mamun, A. Abrar, M. Rahman, M. Sabbir Salek & M. Chowdhury, *"Enhancing Transportation Cyber-Physical Systems Security: A Shift to Post-Quantum Cryptography"*, 2024 (preprint). arXiv
10. H. Shadan & S. Islam, *"Quantum Computing and Cyber security in Accounting and Finance: Current and Future Challenges and Opportunities for Securing Accounting and Finance Systems"*, MDPI (2025). MDPI+1