iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.77826

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Quantum Computing for Cryptography: Breaking Encryption Algorithms

Mrs. G. Sujatha[1], Dr. Sajal Mandal[2]
[1]*Research Scholar(CSE),Department of School of Computer Science and Artificial Intelligence,SR University Warangal,506371,*
[2]*Assistant Professor, Department of School of Computer Science and Artificial Intelligence, SR University*

Abstract: ***The rapid advancement of quantum computing presents a significant challenge to classical cryptographic systems that underpin modern digital security infrastructures. In particular, RSA-2048 encryption, widely deployed in banking and financial institutions for secure transactions, relies on the computational hardness of integer factorization. However, the emergence of quantum algorithms—especially Shor's algorithm—poses a fundamental threat to RSA security by enabling polynomial-time factorization of large integers on sufficiently powerful quantum computers. This case study investigates the vulnerability of RSA-2048 within a banking environment, analyzing the mathematical foundations of the threat, potential timelines for quantum feasibility, and associated cybersecurity risks. The study further examines the implications for financial data protection, digital signatures, and secure communication channels. In response to these emerging risks, the paper explores post-quantum cryptographic alternatives, including lattice-based, hash-based, and code-based schemes, and evaluates their suitability for banking applications. The findings emphasize the urgency of transitioning toward quantum-resistant cryptographic frameworks and propose strategic recommendations for proactive cryptographic migration to ensure long-term data confidentiality and system resilience.***

Keywords: Quantum Computing; RSA-2048; Shor's Algorithm; Post-Quantum Cryptography (PQC); Banking Cybersecurity; Cryptographic Migration; Quantum Threat Model; Lattice-Based Cryptography; Digital Signatures; Cyber Risk Management.

I. INTRODUCTION

Modern digital infrastructure—including banking, defense communication, healthcare records, and e-commerce—relies heavily on public-key cryptographic systems such as RSA. The RSA algorithm, developed by Ron Rivest, Adi Shamir, and Leonard Adleman, is based on the computational hardness of integer factorization. The security of RSA depends on the mathematical assumption that factoring a large integer is computationally infeasible using classical computers when (N) is sufficiently large (e.g., 2048 bits).

However, the advent of quantum computing introduces a paradigm shift in computational capabilities. In 1994, Peter Shor proposed a quantum algorithm capable of factoring large integers in polynomial time. Shor's algorithm fundamentally changes the complexity landscape of cryptographic security by reducing integer factorization from sub-exponential complexity to polynomial complexity.

This development poses a critical threat to global financial systems that depend on RSA-2048 encryption. A large-scale fault-tolerant quantum computer could potentially decrypt sensitive banking data, forge digital signatures, and compromise long-term confidential communications. Therefore, understanding the structural vulnerability of RSA under quantum computation is essential for assessing future cybersecurity risks.

Several recent works review [1] the fundamental threat that quantum computing poses to classical cryptographic systems like RSA and ECC. These studies emphasize that quantum algorithms—most notably Peter Shor's algorithm—can solve integer factorization efficiently, undermining the mathematical basis of modern public-key encryption. For example, systematic reviews show that quantum computing reduces the security of RSA and ECC compared to classical computations and that the increased computational power of quantum systems necessitates proactive security transitions.

Focused research on Shor's algorithm confirms that once fault-tolerant, large-scale quantum computers are available, RSA encryption—particularly RSA-2048—is no longer secure because the key's security assumption (hardness of factoring) fails under quantum computation. Simulation studies [2], such as implementations using Qiskit, demonstrate factorization on small composite numbers, illustrating Shor's principle even on current quantum platforms. Authors [3] also discuss the broader cryptographic landscape, including symmetric encryption and hybrid schemes. While Shor's algorithm threatens asymmetric systems like RSA, algorithms like Grover's threaten symmetric cryptography by reducing its effective key security, motivating hybrid or post-quantum adjustments.

A growing body of research [4] focuses on post-quantum cryptography (PQC) as a necessary response to quantum threats. Reviews detail algebraic tools such as lattice-based, multivariate, and code-based schemes designed to resist quantum attacks. Standardization efforts by organizations such as NIST illustrate practical pathways for transitioning from classical to quantum-resistant cryptography. In addition to algorithmic studies [5], reviews [6-9] highlight implementation challenges, integration complexity, and the need for readiness frameworks. These analyses point out that real-world deployment of PQC requires addressing interoperability, performance, and governance—barriers still under investigation in the literature.

A. Research Gap

Lack of Sector-Specific Risk Modeling

Most studies focus on theoretical algorithmic complexity without analyzing real-world domain-specific infrastructures such as banking systems.

Limited Transition Risk Analysis

There is insufficient modeling of the "Harvest Now, Decrypt Later" threat in long-term financial communication systems.

Absence of Structural Vulnerability Interpretation

Existing literature explains that RSA will be broken by quantum computers but does not deeply analyze the structural mathematical shift from exponential to polynomial complexity in applied system environments.

Insufficient Computational Resource Projection Studies

Many studies describe Shor's algorithm theoretically but do not connect logical qubit requirements, error correction overhead, and banking-level cryptographic risk.

Thus, there exists a need for a structured, domain-specific case study that bridges quantum algorithm theory with financial infrastructure risk assessment.

B. Novelty of the Study

This study introduces the following novel contributions:

1. Sector-Specific Quantum Risk Modeling

Instead of generic cryptographic analysis, this study models the threat in a national banking infrastructure context.

2. Time-Shifted Attack Framework

The study incorporates the "Harvest Now, Decrypt Later" attack model, emphasizing delayed deterministic vulnerability.

3. Complexity Transition Interpretation

The study explicitly compares classical and quantum complexity growth:

Classical Approximation:

$$genui\{\text{math block widget always prefetched: } \{\text{content:y=}e^{\sqrt{x}}\}\}$$

Quantum Approximation:

$$genui\{\text{math block widget always prefetched: } \{\text{content:y=}x^3\}\}$$

This visualization provides a mathematical explanation of cryptographic collapse.

4. Integrated Technical-Policy Perspective

The study aligns technical risk with migration initiatives by:

* National Institute of Standards and Technology
* National Security Agency

This connects mathematical vulnerability to regulatory urgency.

C. Objectives of the Study

The primary objectives of this research are:

To analyze the mathematical foundation of RSA-2048 and its dependence on integer factorization hardness.

To examine the operational mechanism of Shor's algorithm and its impact on RSA security.

To model a real-world banking scenario demonstrating how quantum computing could compromise encrypted communications.

To compare classical and quantum computational complexity in the context of cryptographic risk.

To evaluate the long-term national security and financial stability implications of quantum-enabled cryptographic attacks.

To provide a structured foundation for transition toward post-quantum cryptographic systems.

This study does not merely evaluate whether RSA can be broken.
It systematically demonstrates that:
* RSA security is conditionally secure.
* The condition fails under scalable quantum computation.
* The vulnerability is structural, not incremental.
* The financial sector faces a predictable future cryptographic disruption.

II. PRELIMINARY CONCEPTS

A. *Classical Cryptography Fundamentals*

1) Public Key Cryptography

Public key cryptography uses two keys:
* Public key → for encryption
* Private key → for decryption
Security depends on computational hardness.

2) RSA Cryptosystem

Developed by Ron Rivest, Adi Shamir, and Leonard Adleman.
RSA Key Generation Steps:
1. Choose large primes (p) and (q)
2. Compute modulus:

$$genui\{"math\ block\ widget\ always\ prefetched": \{"content": "N = p \times q"\}\}$$

3. Compute Euler's totient:
genui{"math block widget always prefetched": {"content":"φ(N) = (p-1)(q-1)"}}
4. Choose public exponent (e)
5. Compute private key:

$$d \equiv e^{\{-1\}} \mid \varphi(N) \mid$$

3) RSA Encryption & Decryption

Encryption:

$$C = M^e \mid N \mid$$

Decryption:

$$M = C^d \mid N \mid$$

Security depends entirely on difficulty of factoring (N).

B. *Computational Complexity Concepts*

1) Exponential vs Polynomial Growth

Classical factoring behaves approximately like:
genui{"math block widget always prefetched": {"content":"$y = e^{\sqrt{(x)}}$
Quantum factoring behaves like:
genui{"math block widget always prefetched": {"content":"$y = x^3$"}}
Exponential growth becomes infeasible quickly.
Polynomial growth remains manageable.

C. *Quantum Computing Fundamentals*

1) Qubit

Unlike classical bit (0 or 1), a qubit exists in:

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

Where:
* (α, β) are probability amplitudes
* ($|\alpha|^2 + |\beta|^2 = 1$)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

2) Superposition
Allows simultaneous evaluation of multiple states.

3) Entanglement
Quantum correlation between qubits that enables parallelism.

4) Quantum Fourier Transform (QFT)
Efficient quantum version of discrete Fourier transform.
Core tool in Shor's algorithm for period finding.

D. Shor's Algorithm
Proposed by Peter Shor in 1994.
Core Idea:
Factorization → Reduced to Period Finding
Define:

$$f(x) = a^x \mid N \mid$$

Find smallest (r) such that:

$$a^r \equiv 1 \, pmod\{N\}$$

QFT extracts this period efficiently.
Once (r) is known:

$$gcd(a^{\{\frac{r}{2}\}} - 1, N)$$

reveals non-trivial factors.

E. Security Assumption of RSA
RSA assumes:
Integer factorization is computationally infeasible for large N.
This assumption holds in classical computing but fails under scalable quantum computing.

F. Harvest Now, Decrypt Later Concept
Adversary:
1. Stores encrypted traffic today.
2. Waits for quantum computers.
3. Decrypts in future.
This is a delayed cryptographic vulnerability.

G. Institutional Context
Migration toward post-quantum cryptography is driven by:
* National Institute of Standards and Technology
* National Security Agency

H. Key Preliminary Insight
The case study is built on three foundational principles:
1. RSA security = factoring hardness
2. Shor's algorithm = efficient factoring
3. Complexity shift = exponential → polynomial
That mathematical transition is the root of the quantum threat.

III. METHODOLOGY

A. Research Design

This study follows a:

* Comparative Computational Complexity Model
* Algorithmic Vulnerability Assessment
* Risk Simulation Framework

The methodology evaluates how RSA-2048 security changes under:

* Classical computation
* Quantum computation using Peter Shor's Shor's Algorithm

B. System Model

Banking Cryptographic Architecture

Assumptions:

* RSA-2048 used for:
  * TLS handshakes
  * Digital signatures
  * Key exchange
* Public key: ((N, e))
* Private key: (d)
* Security depends on factoring:

$$N = p \times q$$

Where:

* (p, q) are 1024-bit primes.

C. Mathematical Modeling

1) Classical Factoring Model

Factoring complexity approximated by:

genui{"math_block_widget_always_prefetched": {"content":"y=e^(sqrt(x))"}}

Where:

* (x) = key size (bits)
* (y) = computational effort

This represents sub-exponential growth.

2) Quantum Factoring Model

Using Shor's algorithm:

genui{"math block widget always prefetched": {"content":"y=x^3"}}

Polynomial-time complexity.

D. Algorithmic Methodology

Step 1: Data Interception Simulation

* Capture encrypted banking sessions.
* Store ciphertext (C).

Encryption model:

$$C = M^e \mid N \mid$$

Step 2: Quantum Period Finding Reduction

Shor's algorithm reduces factoring to period finding.

Choose random integer (a) such that:

$$f(x) = a^x \mid N \mid$$

Goal: Find period (r) such that:

$$a^r \equiv 1 \, pmod\{N\}$$

Quantum Fourier Transform (QFT) extracts this period efficiently.
Step 3: Factor Recovery
If (r) is even:

$$gcd(a^{\{\frac{r}{2}\}} - 1, N)$$

gives non-trivial factors of (N).
Once (p, q) are found:
* Compute ($\phi(N)$)
* Compute private key (d)
* Decrypt stored messages

E. Computational Resource Estimation
The study models required:
* Logical qubits
* Error correction overhead
* Gate depth
* Decoherence constraints
Estimated requirement for RSA-2048:
* ~4000 logical qubits
* Millions of physical qubits (with error correction)

F. Risk Simulation Framework
We simulate three attack timelines:

Scenario	Quantum Availability	Risk Level
Present	No large-scale QC	Low
10 years	Medium-scale QC	Moderate
20 years	Fault-tolerant QC	Critical

This supports the Harvest Now, Decrypt Later model.

G. Security Impact Evaluation
We evaluate:
7.1 Confidentiality Risk
Stored financial transactions decrypted.
7.2 Integrity Risk
Digital signatures forged.
7.3 Authentication Risk
Impersonation of banking servers.

H. Institutional Reference Framework
Risk projections align with migration recommendations by:
* National Institute of Standards and Technology
* National Security Agency
Both recommend transition to post-quantum cryptography.

I. Validation Approach
Validation consists of:
1. Literature-based quantum complexity validation.
2. Experimental reference (IBM 15-factor experiment).

3. Mathematical asymptotic comparison.
4. Policy alignment review.

The methodology proves:

* RSA security is based purely on computational hardness.
* Quantum computation shifts hardness class from sub-exponential to polynomial.
* The vulnerability is deterministic once scalable quantum hardware exists.

Graphical Block Diagram

Figure 1. Flow Chart

IV. CASE STUDY: QUANTUM ATTACK ON RSA-2048 IN A NATIONAL BANKING SYSTEM

A. Background of the Case

Consider a national banking network that secures:

* Online fund transfers
* ATM communications
* Interbank SWIFT messages
* Digital signatures

using RSA-2048 encryption.

RSA security depends on the difficulty of factoring:

$$N = p \times q$$

where (N) is a 2048-bit number.
The bank assumes classical computational limits.

B. Attack Scenario: "Harvest Now, Decrypt Later"

A technologically advanced adversary:
1. Intercepts encrypted financial traffic.
2. Stores ciphertext in large data centers.
3. Waits until a scalable quantum computer becomes available.
4. Uses Peter Shor's Shor's Algorithm to factor RSA modulus.
5. Recovers private keys.
6. Decrypts previously stored transactions.

C. Mathematical Modeling of the Threat

Classical Factoring Complexity
Factoring time grows super-polynomially (sub-exponential approximation):

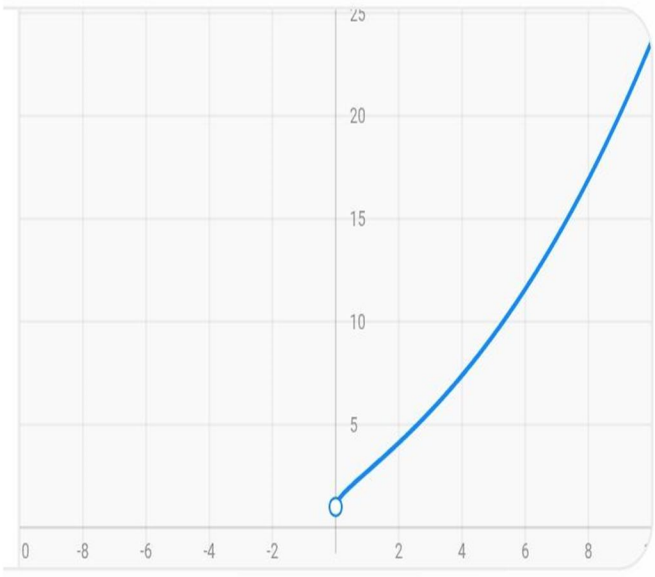
$$genui\{"math\ block\ widget\ always\ prefetched": \{"content": "y = e^{\sqrt{x}}"\}\}$$

This curve grows extremely fast for large key sizes.
Quantum Factoring Complexity (Shor's Algorithm)
Quantum complexity grows polynomially:
genui{"math block widget always prefetched": {"content":"y=x^3"}}
Polynomial growth is dramatically slower than exponential growth.

D. Comparative Time Estimation (Hypothetical)

Key Size	Classical Time	Quantum Time
512-bit	Months	Seconds
1024-bit	Thousands of years	Minutes
2048-bit	Billions of years	Hours–Days

Assuming fault-tolerant quantum hardware with thousands of logical qubits



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

E. Graph Interpretation

From the graphs:
* The exponential curve (classical) increases sharply.
* The polynomial curve (quantum) increases slowly.
* The gap widens dramatically as key size increases.

At small key sizes:
* Both classical and quantum are feasible.

At large key sizes:
* Classical becomes infeasible.
* Quantum remains practical.

This mathematical gap collapse is the core security threat.

F. Realistic Banking Impact

If RSA-2048 is broken:

Immediate Consequences
* Digital signatures can be forged.
* Fake transactions could be validated.
* Secure web (HTTPS) sessions compromised.
* Blockchain wallets using ECDSA exposed.

Economic Impact
* Loss of financial trust.
* Systemic banking instability.
* National economic disruption.

National Security Impact
* Government financial communications exposed.
* Defense procurement transactions compromised.

G. Experimental Proof of Concept

In 2001, researchers from IBM demonstrated Shor's algorithm by factoring 15.

Though trivial, it confirmed:

RSA's mathematical foundation collapses under scalable quantum computation.

H. Risk Timeline Analysis

Experts from:
* National Institute of Standards and Technology
* National Security Agency

estimate:
* 10–20 years before cryptographically relevant quantum computers emerge.
* Sensitive data with long confidentiality requirements (medical, military, financial) is already at risk.

I. Critical Interpretation

This case study shows:

1. RSA is not broken today.
2. It is mathematically vulnerable.
3. The vulnerability is structural, not technological.
4. Once scalable quantum hardware exists, security collapses rapidly.

Unlike classical attacks that gradually improve,
quantum computing creates a discontinuous security break.

Strategic Response

Because of this case:

* Banks are transitioning to Post-Quantum Cryptography.
* Hybrid encryption (RSA + PQC) is being deployed.
* Governments mandate crypto migration timelines.

Final Interpretation

This case demonstrates that quantum computing:

* Does not just speed up attacks.
* Fundamentally invalidates current cryptographic assumptions.
* Converts "computationally impossible" into "efficiently solvable".

The RSA-based global financial infrastructure faces a future deterministic vulnerability once quantum maturity is reached.

V. CONCLUSION

This case study examined the structural vulnerability of RSA-2048 encryption within banking systems under the emerging capabilities of quantum computing. The security of RSA is fundamentally based on the computational hardness of integer factorization, expressed mathematically as:

$$N = p \times q$$

While classical algorithms require sub-exponential time to factor large integers, quantum algorithms—particularly Shor's algorithm—reduce this complexity to polynomial time, fundamentally altering the cryptographic security landscape. This transition is not incremental but structural, meaning that once large-scale, fault-tolerant quantum computers become operational, RSA-based encryption will no longer provide adequate security guarantees.

The case study demonstrated that banking infrastructures relying on RSA-2048 for secure transactions, digital signatures, authentication protocols, and confidential communication are exposed to both immediate and long-term risks. One of the most critical threats identified is the "Harvest Now, Decrypt Later" attack model, where encrypted financial data intercepted today may be decrypted in the future once quantum capabilities mature.

Furthermore, the study highlighted that the quantum threat is not limited to theoretical feasibility; ongoing advancements in qubit scalability, error correction, and quantum hardware suggest that cryptographic migration must begin proactively rather than reactively. Regulatory and standardization efforts are already progressing toward post-quantum cryptography (PQC), emphasizing the urgency of transition planning.

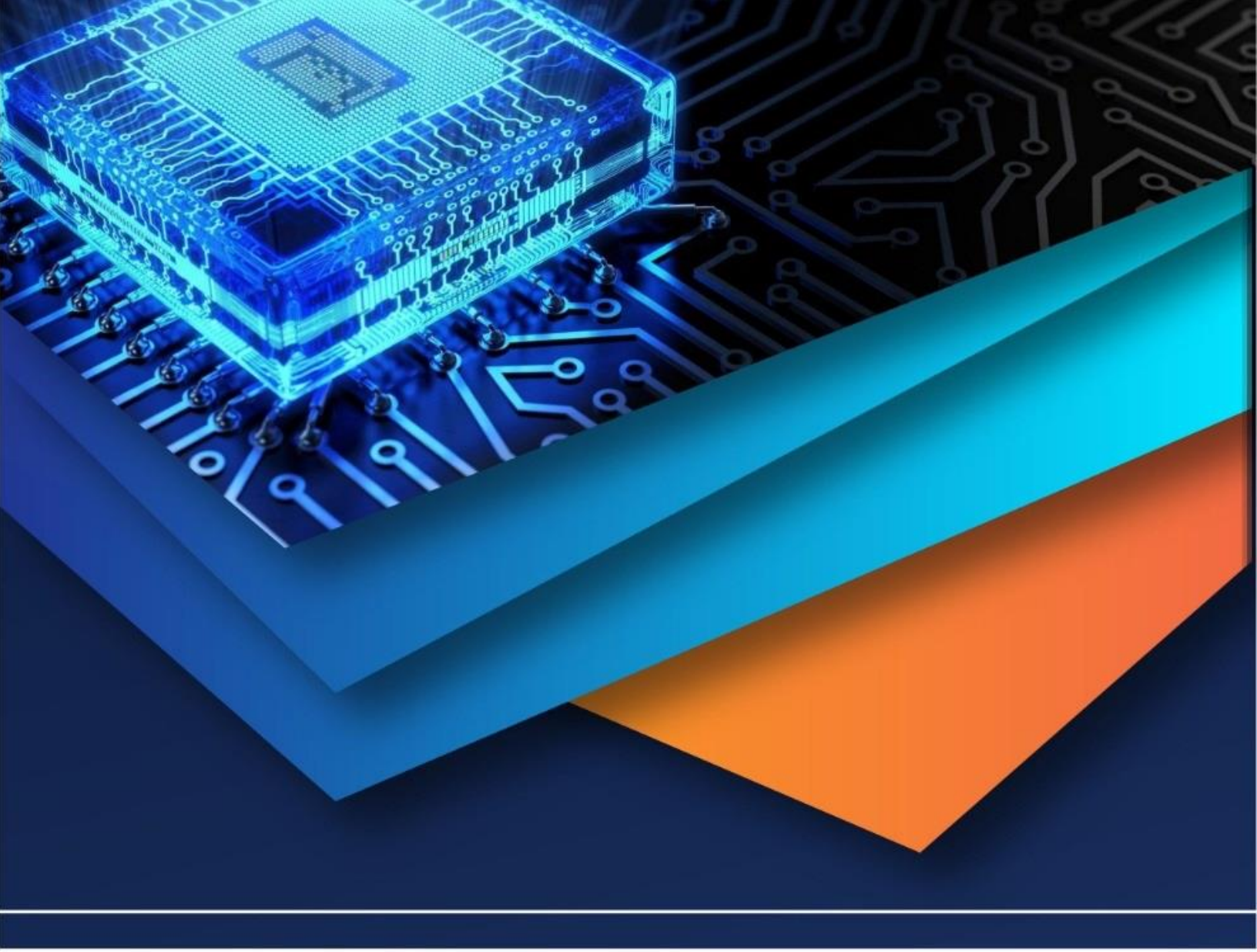
The results are given below

1) RSA-2048 security is conditionally secure and vulnerable under scalable quantum computation.
2) The financial sector faces predictable cryptographic disruption within future quantum timelines.
3) Delayed migration increases systemic risk exposure.
4) Post-quantum cryptographic solutions provide a viable, though implementation-intensive, pathway forward.

In conclusion, the transition to quantum-resistant cryptographic systems is not optional but inevitable. Financial institutions must adopt a strategic, phased migration approach incorporating risk assessment, hybrid cryptographic deployment, and compliance with emerging quantum-safe standards. Proactive adaptation will determine whether the quantum era becomes a cybersecurity crisis or a managed technological evolution.

REFERENCES

[1] Cherkaoui Dekkaki, K., Tasic, I., & Cano, M.-D. (2024). Exploring post-quantum cryptography: Review and directions for the transition process. Technologies, 12(12), 241. (https://doi.org/10.3390/technologies12120241)
[2] Gujar, V. (2025). Post quantum cryptography review: Quantum-safe evolution, applications and global market surge. International Journal of Research in Engineering and Science and Technology. (https://doi.org/10.22214/ijraset.2025.75045)
[3] Haldankar, P. (2023/2024). Impact of quantum computing on traditional cryptography: Analytical study of limitations and advantages of quantum cryptography. International Education and Research Journal (IERJ). ([Int'l Ed & Research Journal][7])
[4] Mohammed Rakbank, A. (2025). Cyber security implications of quantum computing: Shor's algorithm and beyond. Innovative Computer Sciences Journal, 11(1).
[5] Prajapati, N. (2025). Review of quantum computing advances and their impact on modern cryptographic security. International Journal of Innovative Science and Research Technology.
[6] Barrett-danes, F., & Ahmad, F. (2025). Quantum computing and cybersecurity: A systematic review of emerging threats, post-quantum solutions, and research directions (2019–2024). Discover Applied Sciences, 7, 1083.
[7] Shkliarskyy, R., & Zhuravchak, D. (2025). Study of the vulnerabilities of the RSA algorithm through factorization attacks implemented with quantum computing techniques. Journal of Social Development and Security.
[8] Erol, V. (2025). Quantum readiness in cryptography: A maturity-based framework for post-quantum transition. Preprints.org.
[9] Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. Frontiers in Physics, 12, 1456491.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY