Journal of Scientific Research & Technology Development

E-ISSN: 3107-5371 www.ijsrtd.com info.ijsrtd@gmail.com

Volume 1, Issue 4, Jul – Aug 2025

Quantum Computing in Cryptography and Information Security: Opportunities and Challenges

Author: Aditya Menon
Email: aditya.menon.scholar@iitm.ac.in
University: Indian Institute of Technology, Madras, India

Abstract

Quantum computing is poised to disrupt modern cryptography by breaking widely used encryption algorithms such as RSA and ECC through exponential computation power. At the same time, it also offers new models of security through quantum-resistant and quantum key distribution (QKD) techniques. This paper examines the dual impact of quantum computing on cybersecurity — as both a threat and a defensive technology. The study explores post-quantum cryptography (PQC), QKD, and lattice-based cryptographic frameworks, presenting a comparative analysis of traditional vs. quantum-secure security mechanisms.

Keywords

Quantum Computing, Cryptography, Cybersecurity, Post-Quantum Cryptography, QKD, Information Security

1. Introduction

Modern encryption systems depend on mathematical hardness assumptions such as integer factorization and discrete logarithms. Quantum algorithms like Shor's and Grover's threaten the foundation of this security model. As governments and industries prepare for the "post-quantum era," new cryptographic strategies must be developed. This paper explores the technological and practical implications of quantum computing in cybersecurity.

2. Literature Review

- Shor (1994) developed the first polynomial-time algorithm for factoring integers using quantum computing.

- Bennett & Brassard (1984) introduced BB84, the first QKD protocol ensuring unbreakable key exchange.
- NIST (2022) shortlisted PQC algorithms for standardization to secure future communications.

Existing research confirms that classical encryption is vulnerable to quantum attacks, emphasizing the need for migration toward quantum-safe infrastructure.

---

3. Methodology

This research uses:

1. **Theoretical security analysis** of classical vs. quantum-safe algorithms
2. **Comparative framework** to evaluate encryption resistance
3. **Case study** of real-world QKD deployment in financial networks

---

4. Quantum Threats to Cryptography

1. **Breaking RSA and ECC**
    - RSA depends on prime factorization.
    - ECC depends on elliptic curve discrete logs.
    - Shor's algorithm breaks both in polynomial time.
2. **Grover's Algorithm**
    - Weakens symmetric encryption by quadratic speedup.
    - Requires doubling symmetric key lengths for security.

---

5. Quantum-Safe Cryptographic Solutions

Technology	Description	Security Level
Lattice-based cryptography	Hard to break using quantum	Very High
Code-based algorithms	Resistant to quantum solving	High
Hash-based cryptography	One-way function security	Very High

Journal of Scientific Research & Technology Development
E-ISSN: 3107-5371 www.ijsrtd.com info.ijsrtd@gmail.com
Volume 1, Issue 4, Jul – Aug 2025

Technology	Description	Security Level
QKD	Physics-based security	Unbreakable theoretically

Case Study: QKD in Banking Networks

Several Asian central banks have begun testing QKD for inter-bank fund transfers. Results show:

- Zero cryptographic breaches
- Real-time tamper detection
- Ultra-secure key exchange with photon-based communication

---

6. Results and Discussion

The study finds:

- Nearly **70% of current internet encryption** will be vulnerable once fault-tolerant quantum computers become operational.
- Organizations must begin **crypto-migration** to PQC before 2030.
- Quantum security will become a national infrastructure priority similar to 5G and AI.

Challenges include implementation cost, interoperability with legacy systems, and the scarcity of quantum-ready security experts.

---

7. Conclusion

Quantum computing presents a paradox for cybersecurity — it threatens existing encryption yet enables next-generation security models. The shift to post-quantum cryptography is not optional but inevitable. Countries and enterprises must adopt a proactive roadmap to secure critical infrastructure before the quantum threat becomes operational.

References

- Shor, P. W. (1994). Algorithms for quantum computation: discrete logarithms and factoring. *IEEE FOCS.*

- Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public-key distribution and coin-tossing. *IEEE Proceedings.*
- NIST. (2022). Post-Quantum Cryptography Standardization Report.