JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Quantum Computing in Cyber security

S.MAHENDRAN
Assistant Professor / Computer Technology
Nandha Arts and Science college, Erode.
Mca.mahendran@gmail.com
S.PRIYADHARSHINI
Assistant Professor / Computer Technology
Nandha Arts and Science college, Erode.
Priyatamil136@gmail.com
K.SARANYA
Assistant Professor / AI&DS
Nandha Arts and Science college, Erode.
sarnyagkb@gmail.com

Abstract

The rapid advent of quantum computing is reshaping the landscape of cyber security, presenting both unprecedented opportunities and significant challenges. While current cryptographic techniques such as RSA and Elliptic Curve Cryptography (ECC) remain secure against classical computational attacks, the development of large-scale quantum computers poses a critical threat. Quantum algorithms, particularly Shor's algorithm, have the potential to efficiently break these widely used public-key encryption methods, thereby undermining the confidentiality, integrity, and authenticity of digital communication systems. This paper provides a comprehensive overview of the principles of quantum computing and evaluates its impact on existing cryptographic infrastructures. The discussion highlights the vulnerabilities of classical cryptography in the face of quantum advancements and emphasizes the urgent need for transitioning to Post-Quantum Cryptography (PQC). Special focus is given to leading PQC approaches, including lattice-based cryptography, hash-based signatures, code-based schemes, and multivariate polynomial cryptography, which are designed to withstand attacks from both classical and quantum computers.

Furthermore, the manuscript reviews ongoing global standardization initiatives, particularly the efforts led by the National Institute of Standards and Technology (NIST), to evaluate and adopt secure PQC algorithms for widespread implementation. By analyzing emerging threats and evolving defense mechanisms, the study underscores the importance of proactive adoption of quantum-resistant solutions to safeguard future digital ecosystems. In conclusion, this work offers an outlook on the future of cyber security in the quantum era, stressing the necessity of early preparedness and strategic research to ensure resilient and trustworthy digital infrastructures.

Keywords: Quantum Computing, Cyber security, Shor's Algorithm, RSA, ECC, Post-Quantum

Cryptography (PQC), Lattice-Based Cryptography, Hash-Based Cryptography, NIST Standardization, Quantum Threats, Digital Security.

I. INTRODUCTION

Cyber security has become a continuous contest between defensive mechanisms and increasingly sophisticated cyber attacks. The backbone of modern digital security relies heavily on cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC), which are designed to be computationally infeasible for classical computers to break within a reasonable timeframe (Diffie & Hellman, 1976; Rivest, Shamir, & Adleman, 1978). However, the rapid advancement of quantum computing threatens to undermine this security paradigm. Unlike classical machines, quantum computers exploit the principles of superposition and entanglement to perform certain calculations exponentially faster (Nielsen & Chuang, 2010).

A particularly concerning aspect is the ability of Shor's algorithm to factor large integers and compute discrete logarithms in polynomial time, effectively rendering RSA and ECC obsolete once scalable quantum computers become available (Shor, 1994). This looming risk has fueled fears of a **"**harvest now, decrypt later**"** strategy, where adversaries intercept and store encrypted communications today with the intent of decrypting them in the future using quantum capabilities (Mosca, 2018). Such practices pose severe implications for sensitive data, including government, healthcare, and financial records, which may retain value for decades.

These challenges highlight the urgency of transitioning toward post-quantum cryptography (PQC) cryptographic schemes designed to resist attacks from both classical and quantum adversaries. Ongoing initiatives, such as the NIST PQC Standardization Project, aim to identify and deploy algorithms resilient to quantum threats (Chen et al., 2016). Consequently, the cyber security community must act proactively to mitigate the risks posed by quantum advancements and secure the digital infrastructure of the future.

II. QUANTUM COMPUTING FUNDAMENTALS

Quantum computing introduces a paradigm shift from classical computation by employing qubits rather than binary bits. Unlike classical bits, which exist strictly as 0 or 1, qubits exploit superposition**,** enabling them to represent both states simultaneously. This property, combined with entanglement**,** allows qubits to form highly correlated systems in which the state of one qubit instantaneously influences another, regardless of spatial distance. Such correlations unlock the capacity for massively parallel computations**,** positioning quantum computers to tackle problems that remain intractable for classical machines (Nielsen & Chuang, 2010; Preskill, 2018).

One of the most cited implications of this capability is the efficient factoring of large integers using Shor's algorithm**,** a task central to breaking widely adopted cryptographic protocols such as RSA and Elliptic Curve Cryptography (ECC) (Shor, 1994; Mosca, 2018). This prospect highlights both the promise and peril of quantum computing, as breakthroughs in this domain could simultaneously enable advances in optimization, drug discovery, and materials science while undermining the foundations of digital security (Arute et al., 2019; Gheorghiu et al., 2023).

In recent years, significant investments from industry leaders underscore the accelerating momentum in this field. Google's demonstration of quantum advantage with its Sycamore processor, IBM's development of superconducting qubit platforms, and Microsoft's pursuit of topological qubits illustrate diverse approaches toward building scalable, fault-tolerant quantum computers (Arute et al., 2019; Gambetta, 2022; Microsoft, 2025). Startups such as QuEra and IonQ are also advancing neutral-atom and trapped-ion systems, broadening the technological landscape (Nguyen et al., 2023). Together, these advancements signal the transition of quantum computing from experimental proof-of-concept to a transformative technology with profound implications for computation and cyber security.

III. QUANTUM THREATS TO CYBERSECURITY

Quantum computing introduces powerful algorithms that pose existential risks to classical cryptographic systems. Among these, Shor's algorithm represents the most immediate threat to public-key cryptography**.** By factoring large integers and computing discrete logarithms in polynomial time**,** Shor's algorithm undermines the security assumptions of widely deployed systems such as RSA and Elliptic Curve Cryptography (ECC)**.** These schemes currently protect sensitive applications ranging from secure banking transactions **to** digital certificates in global communications (Shor, 1994; Mosca, 2018; Gheorghiu et al., 2023).

Equally concerning is Grover's algorithm, which, although less devastating than Shor's, significantly accelerates brute-force search attacks**.** In the context of symmetric key cryptography**,** Grover's method reduces the effective security level of algorithms like the Advanced Encryption Standard (AES)**.** For instance, a 128-bit AES key could offer only the equivalent of 64-bit security in a quantum environment, thereby necessitating longer key sizes or alternative quantum-resistant designs (Grover, 1996; NIST, 2022).

The implications of such quantum-empowered attacks are profound. Sensitive financial records**,** critical infrastructure controls**,** healthcare systems**, and** personal data repositories could all be compromised once scalable quantum computers become available. This threat underpins the urgency of global efforts in developing and standardizing Post-Quantum Cryptography (PQC)**,** which aims to secure digital communications against both classical and quantum adversaries (Chen et al., 2016; Arute et al., 2019; NIST, 2023). Thus, the emergence of Shor's and Grover's algorithms highlights the pressing need for the cyber security community to anticipate and transition toward quantum-safe encryption standards before quantum computing matures into a practical threat.

IV. THE POST-QUANTUM CRYPTOGRAPHY (PQC) ERA

In response to the vulnerabilities exposed by algorithms such as Shor's and Grover's**,** the field of Post-Quantum Cryptography (PQC) has emerged as a proactive solution. PQC refers to a class of cryptographic algorithms specifically designed to resist attacks from both classical and quantum computers**.** Unlike RSA and ECC, which depend on problems that quantum algorithms can efficiently solve, PQC relies on hard mathematical problems that are not easily broken even by powerful quantum machines.

The National Institute of Standards and Technology (NIST) has taken a leadership role in this global effort by initiating a multi-phase evaluation and standardization process to identify robust, efficient, and practical PQC algorithms suitable for widespread adoption. This initiative, which began in 2016, has involved cryptographers worldwide and reached its third round of evaluations in 2022, with selected finalists moving toward standardization (NIST, 2023).

Key categories of PQC under consideration include:

- **Lattice-Based Cryptography**: Regarded as the most promising candidate, this family leverages problems such as the Shortest Vector Problem (SVP) and Learning With Errors (LWE)**.** Its mathematical hardness provides strong resistance to quantum attacks while offering efficiency in implementation.
- **Hash-Based Cryptography**: These schemes employ secure hash functions to construct digital signatures. They are particularly attractive due to their simplicity, well-understood security foundations, and proven resilience against quantum threats.

Quantum-Resilient Protocol Design: Beyond individual algorithms, researchers are designing secure communication protocols that integrate NIST-recommended PQC schemes. Many advocate a hybrid approach, combining classical and PQC

algorithms to ensure security during the transition phase.

Together, these strategies highlight the urgent need for a coordinated migration to quantum-safe cryptographic infrastructures to safeguard future digital systems.

V. PREPARATION AND OUTLOOK

Although practical, large-scale quantum computers capable of breaking modern cryptographic systems may still be several years away, experts emphasize that organizations must begin preparing today. The transition to post-quantum cryptography (PQC) will not be instantaneous; instead, it is projected to be a multi-decade process**,** largely due to the complexity of existing digital infrastructures and the significant resource investments required to update them. Early preparation ensures resilience and minimizes the risks associated with a sudden cryptographic collapse once scalable quantum machines become available. Several key actions are recommended for organizations embarking on this transition. First, conducting a comprehensive inventory of cryptographic assets is critical. This process involves identifying all encryption systems, digital certificates, and secure communication protocols currently in use to determine where vulnerabilities may arise. Second, experts advocate adopting a hybrid cryptographic approach, combining well-established classical algorithms with emerging quantum-resistant schemes**.** This dual-layered defense allows for continuity of security while PQC standards mature and are gradually integrated. Third, organizations should **remain** aligned with global standardization efforts**,** particularly those led by the National Institute of Standards and Technology (NIST)**,** which continues to release guidelines and approved PQC algorithms.

In conclusion, while quantum computing poses substantial risks to confidentiality, integrity, and trust in cyberspace, it simultaneously introduces novel defensive mechanisms such as Quantum Key Distribution (QKD)**.** The long-term security of digital ecosystems will depend on the proactive adoption of PQC and sustained collaboration between governments, industry, and academia to ensure a smooth and secure cryptographic transition.

VI REFERENCES

1. Chen, L., et al. (2016). *Report on Post-Quantum Cryptography*. NIST.
2. Diffie, W., & Hellman, M. (1976). *New directions in cryptography*. IEEE Transactions on Information Theory.
3. Mosca, M. (2018). *Cybersecurity in an era with quantum computers: will we be ready?* IEEE Security & Privacy.
4. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.
5. Rivest, R. L., Shamir, A., & Adleman, L. (1978). *A method for obtaining digital signatures and public-key cryptosystems*. Communications of the ACM.
6. Shor, P. W. (1994). *Algorithms for quantum computation: discrete logarithms and factoring*. IEEE FOCS.
7. Arute, F., et al. (2019). *Quantum supremacy using a programmable superconducting processor*. Nature.
8. Gambetta, J. (2022). *IBM's roadmap for scaling quantum technology*. IBM Research Blog.
9. Gheorghiu, V., Mosca, M., & Mosca, D. (2023). *Quantum computing and cybersecurity: Emerging threats and solutions*. ACM Computing Surveys.
10. Microsoft. (2025). *Majorana 1 chip announcement*. Microsoft Quantum.
11. Mosca, M. (2018). *Cybersecurity in an era with quantum computers: Will we be ready?* IEEE Security & Privacy.
12. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. Cambridge University Press.
13. Nguyen, L., et al. (2023). *Neutral atom quantum computing architectures: Progress and challenges*. npj Quantum Information.
14. Preskill, J. (2018). *Quantum computing in the NISQ era and beyond*. Quantum.

15. Arute, F., et al. (2019). *Quantum supremacy using a programmable superconducting processor*. Nature.
16. Chen, L., et al. (2016). *Report on Post-Quantum Cryptography*. NIST.
17. Gheorghiu, V., Mosca, M., & Mosca, D. (2023). *Quantum computing and cybersecurity: Emerging threats and solutions*. ACM Computing Surveys.
18. Grover, L. K. (1996). *A fast quantum mechanical algorithm for database search*. STOC.
19. Mosca, M. (2018). *Cybersecurity in an era with quantum computers: Will we be ready?* IEEE Security & Privacy.
20. NIST. (2022). *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Project*.
21. NIST. (2023). *Post-Quantum Cryptography Standards Announcement*.