American Journal of Applied Science and Technology

VOLUME Vol.05 Issue 11 2025
PAGE NO. 118-121
DOI 10.37547/ajast/Volume05Issue11-23

Security Challenges In The Era Of Cryptography And Quantum Technologies

Nuriddin Safoev

Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

Received: 27 September 2025; **Accepted:** 19 October 2025; **Published:** 23 November 2025

Abstract: This article analyzes the profound impact of quantum computing on modern cryptographic systems. It explores the computational complexity theory framework to assess the vulnerability of current cryptographic mechanisms, which rely on complex mathematical problems. The analysis confirms that symmetric cryptography and hash functions remain relatively secure against quantum attacks, primarily threatened by Grover's algorithm. In contrast, widely used public-key cryptosystems are critically vulnerable to Shor's algorithm. The study concludes by examining the transition to post-quantum cryptography, highlighting the challenges of efficiency, trust, and usability that must be overcome before these new algorithms can be widely deployed.

Keywords: Cryptography, Quantum Computing, Shor’s Algorithm, Grover’s Algorithm, Post-Quantum Cryptography, AES, RSA.

1. INTRODUCTION:

The advent of quantum computing represents a paradigm shift in computational capability, posing a significant threat to the foundations of modern information security. Current cryptographic systems rely on the computational difficulty of problems like integer factorization and discrete logarithms, which are intractable for classical computers. However, quantum algorithms, leveraging principles like superposition and entanglement, can solve these problems in polynomial time, rendering many existing cryptographic protocols obsolete. This paper examines the specific threats quantum computers pose to both symmetric and asymmetric cryptography, the timeline of this threat, and the ongoing global effort to standardize quantum-resistant algorithms.

To understand the quantum threat, one must consider computational complexity theory, which classifies problems based on the resources required to solve them [1]. The two primary resources are:

- Time Complexity: The number of computational steps needed.
- Space Complexity: The amount of memory required.

This work focuses on time complexity:

- P (Polynomial Time): Problems solvable by a classical computer in polynomial time. These are considered efficiently solvable.
- NP (Nondeterministic Polynomial Time): Problems whose solutions can be verified in polynomial time, but finding the solution is believed to be hard. The Traveling Salesman Problem is a classic NP-Complete problem.
- BQP (Bounded-error Quantum Polynomial Time): Problems solvable by a quantum computer in polynomial time with a bounded probability of error. This class includes all of P and some of NP. Shor's algorithm, which factors large integers, is the most famous BQP algorithm [2, 3].

Crucially, quantum computers are not believed to be able to solve all NP-Complete problems efficiently, which directs the practical focus of quantum threats towards specific mathematical problems underpinning current cryptography.

2. Impact of Quantum Computers on Existing Cryptosystems

The emergence of large-scale quantum computers poses differing levels of risk to today’s cryptographic systems. Not all algorithms are affected equally.

Public-key cryptosystems, such as RSA and ECC, are the most vulnerable because Shor's algorithm can efficiently solve the mathematical problems—integer factorization and discrete logarithms—on which these systems rely. This means that once a sufficiently powerful quantum computer is built, these schemes can be completely broken.

In contrast, symmetric-key algorithms (e.g., AES) and cryptographic hash functions (e.g., SHA-256) experience only a partial reduction in security due to Grover's algorithm, which offers a quadratic speedup for brute-force search. These systems can remain secure simply by doubling key lengths or using larger hash outputs.

Because the degree of vulnerability varies across cryptographic families, Table 1 provides a summarized comparison of how different existing cryptosystems withstand quantum attacks. This helps highlight which algorithms require urgent replacement, which need strengthening, and which remain relatively secure in the post-quantum era.

Table 1: Impact of Quantum Computers on Existing Cryptosystems

Cryptoalgorithm	Type	Purpose	Impact from Quantum Computers
AES-256	Symmetric	Encryption	Secure
SHA-256, SHA-3	Hash Function	Data Integrity	Secure
RSA	Public Key	Digital Signature, Encryption	Not Secure
ECDSA, ECDH	Public Key	Digital Signature, Key Exchange	Not Secure

2.1. The Threat to Public-Key Cryptography (PKC)

The most significant threat to modern public-key cryptography arises from Shor's algorithm, which is capable of solving the integer factorization problem (thereby breaking RSA) and the discrete logarithm problem (breaking ECC) in polynomial time [8]. Current projections indicate a non-negligible likelihood that a cryptographically relevant quantum computer (CRQC) could be built between 2026 and 2031 [5, 6].

Given this risk, the transition to quantum-safe (post-quantum) algorithms has become urgent. Mosca's theorem provides a simple but powerful model to quantify this urgency using three variables [7]:

- X – the duration for which the data must remain confidential,
- Y – the time required to migrate systems to post-quantum cryptography,
- Z – the estimated time until quantum computers can break current PKC schemes.

If X + Y ≥ Z, then immediate action is required, as sensitive information encrypted today may be decrypted in the future once quantum capabilities mature.

The U.S. National Institute of Standards and Technology (NIST) is currently leading an international effort to standardize post-quantum cryptographic algorithms—a multi-year process that is expected to deliver finalized draft standards in the near future [5].

Shor's algorithm efficiently determines the period of the function

$$f(x) = a^x \, mod(n)$$

and this period enables the factorization of the composite number nnn. The key quantum component that provides an exponential speed-up is the Quantum Fourier Transform (QFT), defined as:

$$QFT_N \mid j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{jk} \mid k\rangle$$

The algorithm proceeds by preparing quantum registers, applying Hadamard gates, performing modular exponentiation through an oracle U_f, and then applying the QFT before measurement to extract the period with high probability.

The overall time complexity for factoring an integer n using Shor's algorithm is:

$$O((log\, n)^4)$$

which is exponentially faster than the best known classical algorithms.

2.2. The Impact on Symmetric Cryptography and Hash Functions

The quantum threat to symmetric cryptographic systems is significantly less severe compared to public-key cryptography. The primary quantum algorithm of concern is Grover's algorithm, which offers a quadratic speedup for unstructured search problems, including brute-force key searches [11].

For a symmetric key of length nnn bits, a classical brute-force attack requires

$$O(2^n)$$

operations. Grover's algorithm reduces this complexity to

$$O(2^{\frac{n}{2}})$$

effectively halving the security level. As a result, AES-128, which traditionally provides 128 bits of classical security, offers only 64 bits of quantum security.

Mitigation strategies for symmetric cryptography are relatively simple: increase key sizes. For example, AES-256, with its 256-bit key, retains approximately 128 bits of security against quantum adversaries—considered adequate for the foreseeable future [4].

Hash functions are impacted in a similar manner. Grover's algorithm, when combined with the classical birthday paradox, further reduces their effective security levels. To maintain b bits of quantum security, a hash function must have an output length of at least 3b bits. Consequently, legacy algorithms such as MD5 and SHA-1 are considered completely insecure, while modern alternatives like SHA-256 and SHA-3 remain strong and quantum-resilient options [8, 12].

3. The Path Forward: Post-Quantum and Quantum Cryptography

3.1. Post-Quantum Cryptography (PQC)

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to remain secure against both classical and quantum computer attacks. The central challenge is not merely identifying quantum-resistant algorithms, but ensuring that they are practical, efficient, and deployable at scale. The key hurdles include:

- Efficiency: Many PQC candidates—such as the McEliece cryptosystem—suffer from large key sizes, high memory usage, or significant computational overhead. Achieving acceptable performance while maintaining strong security guarantees remains a major research focus [14].
- Trust and Maturity: Classical cryptographic standards (e.g., RSA, ECC, AES) have earned trust through decades of public scrutiny and cryptanalysis. In contrast, newly proposed PQC algorithms lack long-term validation. They must undergo extensive peer review, formal security proofs, and real-world testing before they can be confidently deployed on a global scale.
- Usability and Integration: Integrating PQC into existing protocols, networks, and hardware requires careful engineering. PQC schemes often demand specialized handling of randomization, padding, message formatting, and key derivation. Additionally, implementations must be rigorously protected against side-channel attacks, which remain a practical threat even to quantum-resistant algorithms [15].

A promising and widely recommended transitional solution is the hybrid approach—combining a classical cryptographic algorithm (such as RSA or ECC) with a post-quantum counterpart. This strategy ensures that security is preserved even if one algorithm is later compromised, offering defense-in-depth during the migration period to fully quantum-safe systems [14].

3.2. Quantum Cryptography

Quantum cryptography—distinct from post-quantum cryptography (PQC)—leverages the fundamental principles of quantum mechanics to secure communication. The most prominent example is Quantum Key Distribution (QKD), such as the well-known BB84 protocol [16]. Unlike classical or PQC algorithms, the security of QKD does not rely on computational hardness assumptions; instead, it is guaranteed by physical laws, including the no-cloning theorem and the disturbance caused by measurement.

Despite its strong theoretical security, QKD faces several practical limitations:

- It requires specialized quantum hardware, including single-photon sources and detectors.
- QKD typically depends on dedicated optical fiber links or line-of-sight free-space channels, which limits scalability.
- These requirements make QKD incompatible with existing classical internet infrastructure, preventing seamless global deployment.

As a result, while quantum cryptography represents a promising long-term research direction, its integration into large-scale communication systems remains constrained by engineering challenges, cost, and the need for new physical infrastructure.

CONCLUSIONS

The rise of quantum computing necessitates a proactive and strategic transition in the field of cryptography. While symmetric algorithms and hash functions can be fortified with larger parameters, the public-key cryptography that underpins modern digital trust must be entirely replaced. The global standardization of post-quantum cryptography is a critical step, but its success depends on overcoming significant challenges in efficiency, establishing trust in new algorithms, and ensuring seamless integration into existing systems. The time to prepare for this post-quantum future is now, as the transition will be complex and time-consuming.

REFERENCES

1. C.-L. Wu and C.-H. Hu, "Computational Complexity Theoretical Analyses on Cryptographic Algorithms for Computer Security Application," in 2012 Third International

Conference on Innovations in Bio-Inspired Computing and Applications, IEEE, Sep. 2012, pp. 307–311. doi: 10.1109/IBICA.2012.9.

2. P. W. Shor, "Progress in Quantum Algorithms," Quantum Inf Process, vol. 3, no. 1–5, pp. 5–13, Oct. 2004, doi: 10.1007/s11128-004-3878-2.
3. Scott Aaronson, "THE LIMITS OF Quantum," Sci Am, vol. 298, no. 3, pp. 62–69, 2008.
4. V. Mavroeidis, K. Vishi, M. D., and A. Jøsang, "The Impact of Quantum Computing on Present Cryptography," International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, 2018, doi: 10.14569/IJACSA.2018.090354.
5. Dustin Moody, "The ship has sailed: The NIST Post-Quantum Crypto 'Competition,'" 2017.
6. M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," IEEE Secur Priv, vol. 16, no. 5, pp. 38–41, Sep. 2018, doi: 10.1109/MSP.2018.3761723.
7. M. Mosca, "Setting the Scene for the ETSI Quantum-safe Cryptography Workshop," in eproceedings of 1st Quantum-Safe-Crypto Workshop, Sophia Antipolis, 2013.
8. V. Mavroeidis, K. Vishi, M. D., and A. Jøsang, "The Impact of Quantum Computing on Present Cryptography," International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, 2018, doi: 10.14569/IJACSA.2018.090354.
9. Zach Kirsch and Ming Chow, "Quantum Computing: The Risk to Existing Encryption Methods," Tufts University, Computer Systems Security, 2015.
10. John Proos and Christof Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," arXiv preprint quant-ph/0301141, 2003.
11. L. K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack," Phys Rev Lett, vol. 79, no. 2, pp. 325–328, Jul. 1997, doi: 10.1103/PhysRevLett.79.325.
12. G. Brassard, P. Høyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions," ACM SIGACT News, vol. 28, no. 2, pp. 14–19, Jun. 1997, doi: 10.1145/261342.261346.
13. D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, no. 7671, pp. 188–194, Sep. 2017, doi: 10.1038/nature23461.
14. Ruben Niederhagen and Michael Waidner, "Practical Post-Quantum Cryptography," White Paper of Fraunhofer SIT, 2017.
15. D. J. Bernstein, "Post-quantum Cryptography," in Encyclopedia of Cryptography, Security and Privacy, Cham: Springer Nature Switzerland, 2025, pp. 1846–1847. doi: 10.1007/978-3-030-71522-9_386.
16. S. Fehr, "Quantum Cryptography," Found Phys, vol. 40, no. 5, pp. 494–531, May 2010, doi: 10.1007/s10701-010-9408-4.