International Journal of Research in Engineering, Science and Management
Volume 8, Issue 5, May 2025
https://www.ijresm.com | ISSN (Online): 2581-5792

Quantum Threats to Classical Cryptography: A Mathematical and Algorithmic Perspective

Aman Shajee*
Private Researcher, Singapore

***Abstract*: Quantum computing offers transformative computational power by harnessing phenomena such as superposition and entanglement. Yet, this potential simultaneously poses severe risks to classical cryptographic systems. In this paper, we explore how quantum algorithms, most notably Shor's algorithm for integer factorization and Grover's algorithm for unstructured search, could break widely deployed cryptographic schemes. We present a rigorous mathematical analysis of these quantum algorithms, compare their complexity with classical methods, and examine their impact on public-key and symmetric cryptography. Finally, we discuss potential countermeasures, including post-quantum cryptographic solutions, to safeguard data in the quantum era.**

***Keywords*: Quantum computing, Cryptanalysis, Shor's algorithm, Grover's algorithm, Post-quantum cryptography.**

1. Introduction

The rapid development of quantum computing introduces a dual-edged sword for cryptography. On one hand, quantum systems promise exponential speed-ups in solving problems that are intractable for classical computers. On the other hand, these same advances threaten the security of many cryptographic protocols that underpin modern digital communications. Classical public-key algorithms such as RSA and elliptic curve cryptography (ECC) rely on the computational difficulty of problems like integer factorization and discrete logarithms. Shor's algorithm, however, can factor large numbers and compute discrete logarithms in polynomial time, rendering these systems vulnerable.

Symmetric ciphers and hash functions, while more resilient, are still affected by Grover's algorithm, which provides a quadratic speedup for brute-force searches. This reduction in complexity implies that key sizes must be doubled to achieve classical security levels. The urgent need for post-quantum cryptography has prompted extensive research into new algorithms resistant to quantum attacks. This paper examines the mathematical foundations of these quantum algorithms and assesses their implications for cryptography.

2. Background

A. Quantum Computing Fundamentals

Quantum computers use qubits, which unlike classical bits, can exist in superpositions of states. A single qubit is represented by:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, with\ |\alpha|^2 + |\beta|^2 = 1 \quad (1)$$

The ability to represent 2^n states with n qubits, combined with entanglement and interference, enables quantum algorithms to process information in fundamentally new ways. Quantum gates, represented by unitary matrices, manipulate these qubit states. The performance of quantum algorithms relies heavily on maintaining coherence and minimizing errors through techniques such as quantum error correction.

B. Classical Cryptographic Primitives

Modern cryptographic systems generally fall into two categories:

- *Public-Key Cryptography*: Systems like RSA and ECC are based on the hardness of problems such as integer factorization and discrete logarithms.
- *Symmetric-Key Cryptography*: Algorithms such as AES rely on key lengths and complex permutation–substitution networks to ensure security. Hash functions provide data integrity by generating fixed-length digests from variable-length inputs.

The security of these systems rests on the assumption that certain mathematical problems are computationally infeasible to solve on classical machines, a premise that quantum computing directly challenges.

3. Quantum Algorithms for Cryptanalysis

A. Shor's Algorithm

Shor's algorithm represents a ground-breaking approach to integer factorization. For a given composite number N (with bit-length n), the algorithm operates as follows:

- Random Selection: Choose an integer a such that gcd(a,N) = 1
- Period Finding: Define the function $f(x) = a^x \bmod N$
- *Factor Extraction*: If r is even and $a^{\frac{r}{2}} \not\equiv$ -1(mod N), then compute gcd $(a^{\frac{r}{2}} \pm 1, N)$ to obtain non-trivial factors of N.

The quantum component of the algorithm, dominated by the

*Corresponding author: amanshajee1234@gmail.com

QFT, runs in $O(2^n)$ time, making it exponentially faster than the best-known classical factoring algorithms. This polynomial-time solution threatens the security of RSA and ECC, both of which depend on the intractability of factorization and discrete logarithm problems.

B. Grover's Algorithm

Grover's algorithm offers a quadratic speedup for searching unsorted databases. In classical terms, finding a specific item in a database of N items requires $O\sqrt{N}$ iterations.

For symmetric cryptography, the algorithm implies that a brute-force key search on a n-bit key can be performed in roughly $O(2^{\frac{n}{2}})$ steps, rather than $O(2^n)$. This significant reduction in complexity means that symmetric algorithms such as AES-128, which are considered secure against classical attacks, may be compromised by quantum adversaries unless key lengths are doubled (e.g., using AES-256).

Mathematically, the success probability after k iterations is given by:

$$P(k) = \sin^2((2k+1)\theta) \tag{2}$$

With $\theta = \arcsin\left(\frac{1}{\sqrt{N}}\right)$. The optimal number of iterations is approximately:

$$k \approx \frac{\pi}{4}\sqrt{N}$$

4. Mathematical Analysis and Complexity, Calculations

A. Complexity Analysis of Shor's Algorithm

Consider an integer N with n = $log_2 N$ bits. The quantum complexity of Shor's algorithm is primarily determined by the quantum Fourier transform, which requires about $O(n^2)$ quantum operations. Including overhead for error correction, the overall procedure remains polynomial in n, demonstrating that RSA, which requires super-polynomial effort to break classically, is fundamentally vulnerable in the quantum regime.

B. Impact of Grover's Algorithm on Symmetric Cryptography

For a symmetric cipher with a key length of n bits, the classical brute-force complexity is 2^n. With Grover's algorithm, this is reduced to:

$$T_{quantum}(n) \approx \frac{\pi}{4}2^{\frac{n}{2}} \tag{3}$$

For example, AES-128's effective complexity falls from 2^128 to approximately 2^{64} operations under quantum attack. This quadratic speedup necessitates larger key sizes (such as AES-256) to maintain equivalent security levels.

5. Quantum Impact on Cryptographic Primitives

A. Vulnerability of Public-Key Systems

Public-key systems such as RSA and ECC derive their security from problems that are hard for classical computers but become tractable with quantum algorithms. Shor's algorithm, by efficiently factorizing large numbers and computing discrete logarithms, effectively nullifies the security assumptions of these systems. This vulnerability necessitates a rapid transition to quantum-resistant alternatives.

B. Symmetric Ciphers and the Role of Grover's Algorithm

Although symmetric cryptography is more resilient, Grover's algorithm significantly reduces the effective key length by providing a quadratic speedup for exhaustive searches. As a result, doubling the key size is required to counteract this reduction. This requirement underscores the importance of reassessing key length recommendations in the context of emerging quantum technologies.

6. Countermeasures and Post-Quantum Cryptography

In anticipation of quantum attacks, researchers have been developing post-quantum cryptographic schemes. These include:

- *Lattice-Based Cryptography*: Algorithms based on the hardness of lattice problems are promising candidates for quantum-resistant cryptography.
- *Code-Based Cryptography*: Systems such as the McEliece cryptosystem leverage error-correcting codes to provide security.
- *Hash-Based Signatures*: These digital signature schemes rely solely on the strength of cryptographic hash functions and are inherently resistant to quantum attacks.

A. Lattice-Based Cryptography

Lattice-based schemes derive their security from the worst-case hardness of certain lattice problems, most notably the Shortest Vector Problem and the Learning with Errors problem. A lattice $\mathcal{L} \subset \mathbb{R}^n$ is the integer span of basis vectors B= $[b_1, \ldots, b_2]$. The SVP asks for a nonzero lattice vector $v \in \mathcal{L}$ minimizing $\|v\|$. Best classical algorithms run in time roughly $2^{O(n)}$, and quantum improvements are bounded by a subexponential factor, far from the polynomial.

B. Learning with Errors

Let q be a prime modulus, n the dimension, and χ an "error" distribution $\mathbb{Z}_q$ (eg. A discrete Gaussian $\mathcal{D}_{aq}$). An LWE sample is $(a, b =< a, s + e \ mod \ q >)$ where $\overset{\$}{\leftarrow} \mathbb{Z}_q^n$, secret s ∈ $\mathbb{Z}_q^n$, and e $\overset{\$}{\leftarrow} x$. The basic LWE decision problem is reducible in quantum polynomial time to GapSVP in the worst case. The best known quantum solvers for LWE require time $2^{O(n)}$ as well, with improvements only in constants or sub-exponential factors

Parameter selection. To achieve 2^λ quantum security, choose

$$n = O(\lambda), q = poly(n), \alpha = O\left(\frac{1}{\sqrt{n \ logq}}\right) \tag{4}$$

For instance, for $\lambda = 128: n \approx 512, q \approx 2^{13}, and \ \alpha q \approx 3$.. Under these parameters, any quantum accelerated lattice reduction still takes time $\approx 2^{1.8n/(k+1)}$ for block size k≈ 40,

which is infeasible.

C. Code-Based Cryptography

Code-based cryptosystems rely on the NP-hardness of decoding a random linear code. The canonical example is the McEliece cryptosystem, based on the structural difficulty of syndrome decoding.

McEliece setup. Let $G \in \mathbb{F}_2^{k\,x\,n}$ generate a binary Goppa code of length n, dimension k, and error-correcting capability t. The public key is G′ = SGP where S is an invertible k×k matrix and P is a n×n permutation matrix. The private key is (S,G,P). Encryption of message m $\mathbb{F}_2^k$ adds a random vector e of hamming weight t:

$$c = mG' + e \tag{5}$$

Decryption uses P^{-1} to permute c back, then applies efficient Goppa-code decoders to correct up to t errors and recovers m=uS^{-1}.

Syndrome decoding hardness. Given $\mathbb{HF}_2^{(n-k)n}$ and syndrome s = He^T, finding any e of weight t such that $He^T = s$ is NP- complete. Best classical information-set decoding (ISD) algorithms cost roughly,

$$\binom{n}{t} / \binom{k}{t} \approx 2^{\gamma n} \tag{6}$$

Where $\gamma \approx 0.12$ for recommended parameters (n=3488, k=2720, t=64). Quantum enhancements using Grover's algorithm yield only a quadratic speedup, $2^{\frac{\gamma n}{2}}$„ still infeasible for $\frac{\gamma n}{2} \approx 209$.

Concrete parameters. The NIST-Round 3 Classic McEliece uses (n=3488, k=2720, t=64), giving classical security ≈256 bits and quantum security ≈128 bits. The code rate k/n≈0.78 ensures efficient transmission, and the well-studied algebraic structure of Goppa codes resists structural attacks.

Resistance to quantum attacks. Because the core problem, decoding a random linear code, is NP-hard and admits only brute-force or ISD-based attacks, quantum computers offer at best Grover-speedups. No subexponential quantum algorithm is known for general decoding. The public-key size (≈1 MB) is a trade-off for long-term security, but the extremely high estimated quantum work factor renders code-based schemes a cornerstone of post-quantum cryptography.

D. Hash-Based Signatures

Hash-based signature schemes (e.g., XMSS, SPHINCS+) leverage the provable security of cryptographic hash functions and Merkle trees. Their security reduces to collision and pre-image resistance,properties believed to withstand quantum adversaries beyond Grover's speed-ups.

The Lamport One Time Signatures uses two pairs of random n-bit values $(X_{i,0}, X_{i,1})$ for each bit I of the message. The public key is $\{h(X_{i,0}), h(X_{i,1})\}$. To sign a message m =$(m_1, \ldots, m_l)$ reveal X_{i,m_1}. Verification recomputes hashes and matches against the public key. Security against an attacker forging a second message requires breaking pre-image resistance in ℓ instances, each cost ≈2n classically and ≈$2^{\frac{n}{2}}$quantumly. Thus, achieving λ −bit quantum security requires hash outputs of length 2λ.

Stateless hash-based (SPHINCS+) builds multiple layers of few-time signature trees (Winternitz OTS) and a top-layer hash tree, avoiding state-management challenges. Parameters (e.g., Winternitz parameter w=16 balance signature size vs. signing speed. Total security analysis still reduces to repeated Grover-style attacks costing $2^{\frac{n}{2}}$. If n = 512, quantum effort per collision is 2^{256}, providing 256-bit security. For a hash function H: $\{0,1\}^* \rightarrow \{0,1\}^n$, quantum pre image resistance implies any adversary's success probability in inverting one instance is bounded by,

$$P_{invert} \leq \frac{Q^2}{2^n} \tag{7}$$

Where Q quantum queries to H are made. By choosing n =2 λ, even Q=2^{λ} yields negligible success probability because hash-based schemes rest solely on hash security, and quantum computers only grant quadratic speed-ups, they remain a robust and mathematically transparent option for post-quantum signatures.

7. Conclusion

Modern cryptography systems face both an incredible opportunity and an existential threat from the rapidly developing field of quantum computing. Quantum algorithms like Shor's and Grover's can challenge the fundamental hardness assumptions that underpin classical cryptography, as shown by thorough mathematical study. Once thought to be computationally safe, public-key systems like RSA and ECC are made ineffective by polynomial-time quantum attacks. Despite its greater resilience, even symmetric-key cryptography has a quadratic security degradation, requiring more robust designs and longer key lengths.

The cryptographic community has made great progress in creating post-quantum algorithms that are safe from attackers using massive quantum computers in response to these difficulties. A mathematically complex and adaptable framework based on worst-case hardness assumptions, lattice-based encryption is thought to be impervious to both classical and quantum attacks. Code-based cryptographic systems, exemplified by the McEliece scheme, leverage the enduring complexity of syndrome decoding and continue to demonstrate formidable resilience even under Grover-accelerated adversaries. Hash-based signatures, on the other hand, rely only on the preimage and collision resistance of cryptographic hash functions to offer sophisticated, stateless solutions with transparent and understandable security reductions.

The prompt adoption of these post-quantum cryptographic primitives is essential to the future of secure digital communication. Although there are still issues with performance trade-offs, key sizes, and standardisation, post-quantum cryptography has solid theoretical foundations. Our

cryptography infrastructure has to advance along with quantum capabilities. To prevent the vulnerabilities of the upcoming computational paradigm, governments, institutions, and the commercial sector must start implementing and integrating quantum-safe protocols widely. In the quantum era, we can only guarantee the confidentiality, integrity, and validity of data by taking a proactive, mathematically based approach.

References

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science*, vol. 35, no. 1, pp. 124–134, Nov. 1994.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, vol. 28, no. 1, pp. 212–219, May 1996.

[3] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM*, vol. 56, no. 6, pp. 1–40, Sept. 2009.

[4] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *DSN Progress Report*, vol. 42-44, no. 1, pp. 114–116, Jan. 1978.

[5] J. Buchmann, E. Dahmen, and M. Schneider, "Hash-based digital signature schemes," *Post-Quantum Cryptography*, vol. 2, no. 1, pp. 35–93, Mar. 2008.