Journal of Computer Science

Review Article

A Comprehensive Review of Post-Quantum Cryptography Algorithms

Samandeep Kaur and Jaswinder Singh

Department of Computer Science and Engineering, Punjabi University, Patiala, India

Article history
Received: 24-02-2025
Revised: 14-05-2026
Accepted: 21-07-2026

Corresponding Author:
Samandeep Kaur
Department of Computer Science and Engineering, Punjabi University, Patiala, India
Email: samandeepphd@gmail.com

Abstract: The development of quantum computing has been rapid, and an existential threat to computational hardness assumptions that underlie today's public-key cryptography has been encountered. This manuscript is a complete and thoroughly organized review of Post-Quantum Cryptography (PQC), discussing the mathematical concepts, complexity, and mechanisms of the algorithms that underpin quantum-safe security infrastructures. Rather than the principles of quantum mechanics, the analysis mathematically defines the basic principles of qubits, superposition, and entanglement, and clarifies common misunderstandings of the theory of parallelism in quantum mechanics. The research places cryptographic problems into the Bounded-Error Quantum Polynomial-Time (BQP) complexity class, thus highlighting the exact defects of classical algorithms. The quantum gate complexity of Shor's algorithm is compared to classical bounds as in Pollard's rho algorithm for the Elliptic Curve Discrete Logarithm Problem (ECDLP), for a detailed comparative cryptanalysis. The comparison highlights a very important "quantum security inversion" in that Elliptic Curve Cryptography (ECC) is much more susceptible to the early-stage fault-tolerant quantum computer as compared to the approach used today in RSA. It unfolds the architectural dependency of quantum algorithms, one by one, from the Quantum Fourier Transform (QFT) to Quantum Phase Estimation (QPE) and Shor's algorithm to Grover's algorithm. Last but not least, the manuscript examines emerging attack primitives such as lattice-based, code-based, and hash-based cryptography, their security models, side channel vulnerabilities, and the recently finalised Federal Information Processing Standards (FIPS 205, 203, and 204) that have been published by the National Institute of Standards and Technology (NIST).

Keywords: Quantum Computing, Post-Quantum Cryptography (PQC), Classical Computing, Shor's Algorithm, Grover's Algorithm

Introduction

For decades, classical cryptographic schemes have been the foundation of secure communication, digital identity, and data protection. Since quantum computers are being developed and are even maturing at such a great speed, the inherent assumptions of computational hardness used in many current public key cryptography protocols like RSA, DH, and Elliptic Curve Cryptography (ECC) built thereon become problematic (Shor, 1997). Quantum computing replaces the binary logic of classical processors with the principles of quantum mechanics, enabling fundamentally different modes of computation (Sahu and Mazumdar, 2024). The discovery of Shor's algorithm in 1994 provided a polynomial-time quantum solution for both integer factorization and the discrete logarithm problem, effectively guaranteeing the eventual obsolescence of virtually all currently deployed public-key cryptographic protocols (Shor, 1997; Sahu and Mazumdar, 2024). Furthermore, Grover's algorithm demonstrated a quadratic speedup for unstructured search tasks, halving the effective security margins of symmetric-key encryption algorithms such as the Advanced Encryption Standard (AES) (Shor, 1997; Kikuchi, 2024).

The need to develop, standardise, and implement Post-Quantum Cryptography (PQC) cryptographic primitives that are capable of working securely on classical computers but are also mathematically hard to break by classical and quantum adversaries cannot be overstated. To ensure

migration of the global digital infrastructure to quantum-resistant standards, an exhaustive understanding of quantum algorithmic capabilities, the complexity classes that define computational hardness, and the precise resource estimates needed to execute quantum attacks is required. In this review, the authors cover the theoretical approaches, algorithmic techniques, and recent advances in the standardization of PQC that are required to protect digital communications in the post-quantum era.

Fundamental Principles of Quantum Information Theory

Before understanding how quantum computers can break classical cryptographic systems, a mathematical framework of quantum information processing must be developed. The vulnerability of classical cryptography is not due to the speed-up in processing, but rather it is due to a change in the basic model of computation (Shor, 1997; Jazaeri et al., 2019).

The Mathematical Definition of a Qubit

Classical computing uses binary digits (bits), which are physical entities with a definite state of either zero or one, and are mutually exclusive (Jazaeri et al., 2019; Jozsa, 1997). The basic element of quantum information, in contrast, is the quantum bit (qubit). A qubit is a two-level quantum mechanical system, rather than being in one of two fixed states. Superposition mathematically is a linear combination of the computational basis states $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ (Rigetti, 2009).

Here α and β are complex probability amplitudes. According to the principles of quantum mechanics the quantum state should be normalized, that is, the sum of the squared moduli of these amplitudes should be

Exactly one ($|\alpha|^2+|\beta|^2=1$) (Rigetti, 2009; Jozsa, 1999). One of the basic characteristics of this system is that it is not possible to observe it without changing its condition. When the superposition is measured in the computational basis, it collapses irrevocably, with a probability of $|\alpha|^2$ to the outcome $|0\rangle$, and a probability of $|\beta|^2$ to the outcome $|1\rangle$ (Rigetti, 2009; Epstein, 2019).

Correcting Superposition Misconceptions

A prevalent misconception in popularized accounts of quantum computing and a critical error in assessing cryptographic vulnerabilities is the assertion that a qubit in superposition literally exists as both zero and one simultaneously, leading to the erroneous conclusion that quantum computers solve complex problems by evaluating all possible combinations at once (Shor and Preskill, 2000; Chong and Hwang, 2010). If quantum computers operated as massively parallel classical machines capable of instantaneous exhaustive search, all cryptographic systems, including symmetric ciphers and hash functions, would be broken in 0 (1) time.

In reality, it is a popular misconception that a quantum computer finds all solutions at once; rather, the true power of quantum algorithms lies in orchestrating quantum interference (Shor and Preskill, 2000). A unitary transformation orchestrates the probability amplitudes such that the computational paths leading to incorrect answers undergo destructive interference (cancelling each other out), while the paths leading to the correct answer undergo constructive interference (amplifying their probability) (Kumar and Pattnaik, 2020; Fernandez-Carames and Fraga-Lamas, 2020). By the conclusion of the algorithm, the system has been manipulated so that a measurement yields the correct solution with an overwhelmingly high probability (Kumar and Pattnaik, 2020; Bagirovs et al., 2024).

Entanglement and Decoherence

Entanglement is a crucial aspect of quantum computation, apart from superposition. Entanglement is a purely quantum phenomenon in which two or more qubits become inseparably correlated (Shor, 1997; Bennett et al., 1992). The entangled state of a group of qubits cannot be expressed as the product of the qubits' states. One of the two qubits is measured, and the result immediately determines the state of the other qubit, both of which are separated in space (Shor, 1997; Mavroeidis et al., 2018). Entanglement can be used to implement multi-qubit quantum logic gates that perform conditional operations, which are crucial for creating intricate computational paths (Shor, 1997; Bennett, 1992). The fragile nature of superposition and entanglement, however, presents many engineering challenges.

Quantum states are highly susceptible to decoherence, a process where interactions with external environmental noise (such as thermal fluctuations or electromagnetic radiation) cause the quantum system to leak information, collapsing the superposition prematurely and introducing computational errors (Shor, 1997; Bos et al., 2009). To execute deep cryptographic algorithms, systems cannot rely on fragile physical qubits. Instead, they must employ Quantum Error Correction (QEC) protocols, such as surface codes, which spread the information of a single abstract logical qubit across hundreds or thousands of redundant physical qubits (Shor, 1997; Bos et al., 2009; Chailloux et al., 2017). Consequently, an algorithm requiring a few thousand logical qubits to break an encryption key may demand a hardware footprint of millions of physical qubits (Fehr, 2018; Bernstein and Lange, 2017).

Quantum Computational Complexity and Cryptographic Hardness

Cryptographic security is entirely dependent on computational complexity theory. A cryptographic

primitive is deemed secure if breaking it requires computational resources that scale exponentially with the size of the key, rendering attacks physically impossible within human timescales (Nejatollahi et al., 2017; Micciancio and Regev, 2009). The advent of quantum computing requires a rigorous remapping of these complexity classifications to understand precisely which cryptographic foundations are vulnerable.

Classical Complexity Classes: P, NP, and PSPACE

In classical complexity theory, problems are categorized based on the time and memory resources required by a deterministic or nondeterministic Turing machine to solve them (Hoffstein et al., 1998). The class P (Polynomial Time) encompasses decision problems that can be solved by a deterministic Turing machine efficiently, with execution times bounded by a polynomial function of the input size (Hoffstein et al., 1998; Bernstein, 2016). The class NP (Nondeterministic Polynomial Time) includes problems for which a proposed solution (a witness) can be verified in polynomial time, even if finding that solution requires exponential time (Hoffstein et al., 1998; Bernstein, 2016).

Public-key cryptography relies on problems that are strongly believed to reside within NP but strictly outside of P. For example, verifying that two prime numbers multiply to a specific composite product is trivial (in P), but finding those prime factors from the composite product is presumed to be computationally intractable for classical machines. Furthermore, the class PSPACE (Polynomial Space) encompasses all problems solvable using a polynomial amount of memory, regardless of the time required. The fundamental Hierarchy is established as $P \subseteq NP \subseteq PSPACE$ (Hoffstein et al., 1998).

The Quantum Complexity Class BQP

The computational domain of a quantum computer is formally defined by the complexity class BQP (Bounded-Error Quantum Polynomial-Time), as formalized by Bernstein and Vazirani. BQP represents the set of decision problems solvable by a quantum circuit of polynomial size, with the probability of an incorrect output strictly bounded to at most 1/3 (Ducas et al., 2018; Wang et al., 2023). Because quantum outputs are probabilistic, achieving arbitrary certainty simply requires running the polynomial-time algorithm multiple times and taking a majority vote (Wang et al., 2023).

The relationship between BQP and classical complexity classes dictates the future of cryptography. It is a proven theorem that $BQP \subseteq PSPACE$, as quantum state evolution can be simulated classically using polynomial space, albeit requiring exponential time (Gidney and Ekerå, 2021). Furthermore, since quantum computers can leverage classical randomness, the relationship is formally understood as $P \subseteq BPP \subseteq BQP \subseteq PSPACE$ (Gidney and Ekerå, 2021).

However, the intersection of BQP and NP is the fulcrum of the quantum threat. It is universally conjectured by complexity theorists that $NP \not\subset BQP$ (Ravi et al., 2020; Alaoui, 2013). This implies that quantum computers are not a panacea for all hard computational problems; they cannot solve NP-complete problems efficiently (Bagirovs et al., 2024; Sendrier and Overbeck, 2009). Therefore, symmetric encryption algorithms like AES, which rely on unstructured search spaces rather than specific algebraic structures, are not fully broken by quantum computers. Grover's algorithm provides only a quadratic speedup for these unstructured problems, meaning that upgrading from AES-128 to AES-256 fully restores post-quantum security (Shor, 1997; Kikuchi, 2024; Bagirovs et al., 2024).

The existential crisis for public-key cryptography arises because specific mathematical vulnerabilities namely integer factorization and the discrete logarithm problem contain hidden Abelian subgroup structures (Fehr, 2019). These structures map perfectly onto the Quantum Fourier Transform, placing them firmly inside the BQP complexity class (Fehr, 2018; Bernstein and Lange, 2017). Consequently, RSA, Diffie-Hellman, and ECC exist in the narrow theoretical space of problems that are hard for classical computers but fundamentally easy for quantum computers.

Cryptanalysis: Classical Bounds vs. Quantum Gate Complexity

To fully articulate the threat model against modern cryptography, one must quantitatively contrast the operational limits of classical algorithms against the quantum gate complexity of Shor's algorithm. This comparison highlights a significant paradigm shift, particularly regarding the relative security of RSA versus Elliptic Curve Cryptography (ECC).

Classical Cryptanalysis: The Limits of Pollard's Rho

In the classical computing paradigm, the Elliptic Curve Discrete Logarithm Problem (ECDLP) is significantly harder to solve than the Integer Factorization Problem (IFP) used in RSA. To break RSA, classical adversaries utilize the General Number Field Sieve (GNFS), an algorithm that operates in subexponential time (Fehr, 2018; Tang and Zhang, 2017). Because the time required to break RSA grows sub-exponentially, cryptographic key sizes must be disproportionately massive to maintain security margins; an RSA key must be 3072 bits long to achieve a classical security level of 128 bits (Song et al., 2019).

Conversely, no sub-exponential algorithm exists to solve the ECDLP for standard, safely chosen elliptic curves (Alagic et al., 2019). The most efficient generic attack is Pollard's rho method, which uses a polynomial modulo *n* to generate a pseudorandom sequence to find collisions. For an elliptic curve defined over a prime field of size *P*, Pollard's rho requires $O(\sqrt{p})$ group operations. If the cryptographic key is *n* bits long, the field size is *P* approximately 2^n. Therefore, the computational complexity is strictly bounded by:

$$O(\sqrt{2^n})=O(2^{n/2})$$

This demonstrates that Pollard's rho operates in fully exponential time relative to the bit-length of the input (Alagic et al., 2019). As a direct result, an ECC key requires only 256 bits to achieve the exact same 128-bit classical security level that requires 3072 bits in RSA (Song et al., 2019).

Quantum Cryptanalysis: Shor's Gate Complexity and the Security Inversion

Shor's algorithm obliterates the classical hierarchy by solving both integer factorization and the ECDLP in polynomial time (Fehr, 2018). The complexity of quantum algorithms is not measured in classical clock cycles, but rather in logical qubit width (memory space) and total gate complexity (circuit depth and the number of fault-tolerant operations, particularly non-Clifford gates like the Toffoli gate) (Alagic et al., 2019; Apon et al., 2020).

For integer factorization, Shor's algorithm exhibits an asymptotic quantum gate complexity of $O((\log N)^2(\log\log N)(\log\log\log N))$ (Shor, 1997; Fehr, 2018). When adapted for the ECDLP, the space complexity of the quantum circuit is heavily dictated by the modular inversion operation during point addition. Using length registers and location-controlled arithmetic, a space-efficient reversible modular inversion algorithm reduces requirements to $3n+4\lfloor \log_2 n \rfloor+O(1)$ logical qubits and $204n^2\log_2 n+O(n^2)$ Toffoli gates.

This shift from exponential classical time to polynomial quantum gate complexity creates a phenomenon known as the "quantum security inversion" (Song et al., 2019). Because the resource requirements for Shor's algorithm scale proportionally with the bit length of the modulus or curve rather than the classical hardness of the underlying mathematical problem ECC becomes significantly more vulnerable to quantum attacks than RSA (Shor, 1997; Song et al., 2019; Kuang et al. 2022; Umana, 2011).

As detailed in Table 1, breaking an RSA-2048 key requires 6190 logical qubits, whereas breaking an ECC256 key requires only 2619 logical qubits (Alagic et al., 2019). While RSA has a higher logical qubit requirement, the significantly lower qubit width required for ECC makes it a highly accessible target for early-generation fault-tolerant quantum computers (Song et al., 2019). Therefore, the modern cryptographic reliance on compact elliptic curves inadvertently lowers the barrier to entry for Harvest-Now-Decrypt-Later (HNDL) quantum adversaries (Song et al., 2019).

Architectural Taxonomy of Quantum Algorithms

Quantum algorithms are hierarchical assemblies composed of fundamental quantum subroutines. To accurately assess their capabilities, these algorithms must be examined in their logical order of dependency, beginning with phase-encoding mechanisms and concluding with period-finding and amplitude amplification (Fernandez-Carames and Fraga-Lamas, 2020).

The Quantum Fourier Transform (QFT)

The Quantum Fourier Transform is the foundational engine underlying the exponential speedups observed in quantum cryptography (Sun et al., 2020; Sivasubramanian, 2020). It is the quantum analogue of the classical discrete Fourier transform, designed to map a quantum state from the computational basis into the Fourier (or phase) basis (Shor, 1997).

Mathematically, its action on a basis state $|x\rangle$ is defined as:

$$QFT|x\rangle=\frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}e^{\frac{2\pi ixy}{N}}|y\rangle$$

While calculating a discrete Fourier transform over $N = 2^n$ data points using the classical Fast Fourier Transform (FFT) requires *O(N log N)* operations, the QFT requires only quantum gates (Mozaffari-Kermani and Azarderakhsh, 2015).

Table 1: Comparison of Classical Security Levels and Quantum Resource Requirements for RSA and ECC

Cryptographic Target	Classical Security Level	Minimum Logical Qubits	Estimated Toffoli Gate Complexity	Overall Cost (Mega qubitdays)
ECC P-256	128 bits	2619	1.26×10^{11}	0.89
RSA-2048	112 bits	6190	2.6×10^{9}	0.34
RSA-3072	128 bits	9288	1.86×10^{13}	1.14

The QFT converts information encoded in the computational states of individual qubits into global phase relationships, revealing hidden periodicities and structural patterns within massive datasets without directly measuring the data (Sivasubramanian, 2020; Bao et al., 2022).

Quantum Phase Estimation (QPE)

Building directly upon the capabilities of the QFT is the Quantum Phase Estimation algorithm, a subroutine critical for extracting eigenphase information from a unitary operator with exponential precision (Sivasubramanian, 2020).

Given a unitary operator *U*, and an associated eigenvector ψ the application of the operator results in a phase shift defined by $U|\psi\rangle=e^{2\pi i\theta}|\psi\rangle$. The objective of QPE is to determine the precise value of the phase (Bao et al., 2022).

The QPE circuit utilizes two qubit registers. A sequence of controlled-*U* operations is applied, systematically kicking back the phase information into the Fourier basis of the first register. Crucially, the algorithm concludes by applying the inverse Quantum Fourier Transform (QFT^{-1}) to the first register, converting the abstract phase data back into the computational basis where it can be directly measured as a binary fraction representing θ (Fernandez-Carames and Fraga-Lamas, 2020; Sivasubramanian, 2020; Bao et al., 2022).

Shor's Algorithm

Shor's algorithm, discovered in 1994, is a direct application of Quantum Phase Estimation engineered to solve the period-finding (Shor, 1997; Fernandez-Carames and Fraga-Lamas, 2020). To factor a large composite integer *N*, classical number theory reduces the factorization problem to finding the period *r* of the modular exponentiation function $f(x)=a^x \pmod N$, where a is a randomly chosen integer coprime to *N* (Shor, 1997; Fernandez-Carames and Fraga-Lamas, 2020).

Shor's algorithm executes this period-finding task exponentially faster than classical methods by orchestrating a massive quantum interference pattern. The algorithm evaluates the modular exponentiation function across a full superposition of inputs, temporarily entangling the input and output registers (Kumar and Pattnaik, 2020; Aumasson, 2019). By subsequently applying the inverse QFT to the input register, the algorithm causes the probability amplitudes of all non-periodic states to destructively interfere. Concurrently, the amplitudes that correspond to integer multiples of the fundamental frequency (N/r) constructively interfere (Kumar and Pattnaik, 2020; Aumasson, 2019). Upon measurement, the system collapses to yield a value from which the precise period *r* can be efficiently calculated using classical continued fractions (Kumar and Pattnaik, 2020).

Grover's Algorithm

Distinct from the QFT-dependent algorithms is Grover's algorithm, which addresses the fundamentally different challenge of unstructured database search and function inversion (Shor, 1997; Sun et al., 2020). If a classical computer must locate a specific target within an unsorted list of *N* elements, it must perform an exhaustive search requiring an average of $N/2$ queries and a worst-case of *N* queries ($O(N)$) (Bagirovs et al., 2024).

Grover's algorithm achieves a quadratic speedup, locating the target in precisely $O(\sqrt{N})$ queries (Bagirovs et al., 2024). It accomplishes this through a geometric process known as amplitude amplification. The algorithm initializes the system in a uniform superposition of all possible states. An "oracle" operator is applied, which identifies the target state and flips its quantum phase from positive to negative (Fernandez-Carames and Fraga-Lamas, 2020; Bagirovs et al., 2024). Following the oracle, a diffusion operator is applied, which inverts the amplitudes of all states around the mean amplitude of the system (Bagirovs et al., 2024). Because the target state's amplitude was mathematically lowered by the phase flip, inverting around the mean dramatically increases its positive probability amplitude while suppressing all other incorrect states (Fernandez-Carames and Fraga-Lamas, 2020; Bagirovs et al., 2024). While this does not break symmetric cryptography entirely, it halves the effective bit-strength, mandating the transition to larger key sizes (e.g., AES-256) (Shor, 1997; Kikuchi, 2024).

Post-Quantum Cryptographic Primitives

The existential vulnerabilities inherent in RSA and ECC necessitate an immediate transition toward Post Quantum Cryptography (PQC). PQC primitives are cryptographic systems built upon novel mathematical foundations that are strictly outside the BQP complexity class, ensuring they remain intractable for both classical and quantum adversaries while operating efficiently on classical hardware (Shor, 1997; Li et al., 2023). The principal families of post-quantum cryptographic primitives are illustrated in Fig. 1, including lattice-based, code-based, multivariate, hash-based, and isogeny-based approaches. These families rely on different computational hardness assumptions and provide alternative mechanisms for achieving quantum-resistant security.

This transition is heavily coordinated by international standards organizations. Recently, the National Institute of Standards and Technology (NIST) published three finalized Federal Information Processing Standards (FIPS) to protect against quantum-enabled attacks: FIPS 203, FIPS 204, and FIPS 205.

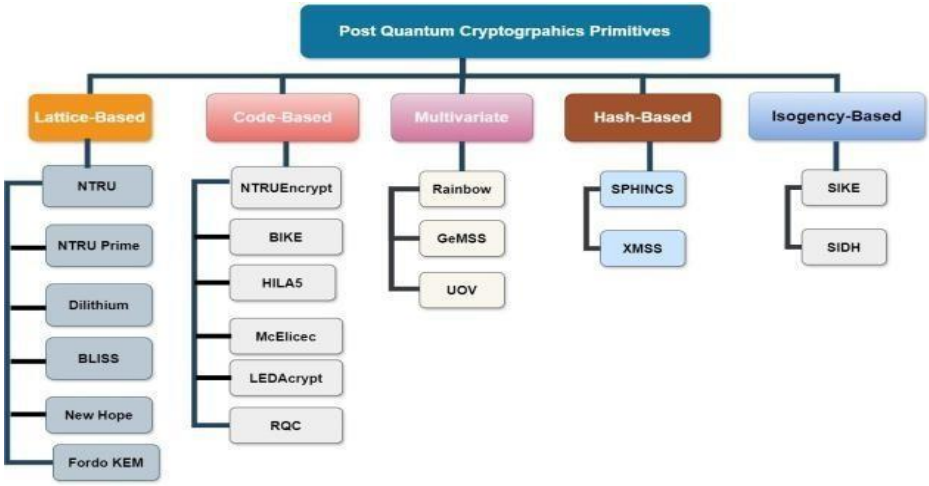

Fig. 1: Post-Quantum Cryptographic Primitives

Lattice-Based Cryptography (FIPS 203 & FIPS 204)

Lattice-based cryptography is the most prominent family within the PQC ecosystem. A mathematical lattice is an infinite grid of points residing in high-dimensional space. The security of these systems is predicated on the hardness of high-dimensional geometric challenges, such as the Shortest Vector Problem (SVP) or the Closest Vector Problem (CVP) (Shor, 1997; Buchmann et al., 2011). Figure 2 provides a geometric illustration of a lattice generated by basis vectors, demonstrating the structured arrangement of lattice points that underlies lattice-based cryptographic constructions.

Modern implementations predominantly rely on the Module Learning With Errors (MLWE) paradigm, which injects mathematically bounded random noise into polynomial equations. Distinguishing the underlying lattice structure from the random noise is believed to be computationally intractable for quantum algorithms (Shor, 1997; Bernstein, 2017).

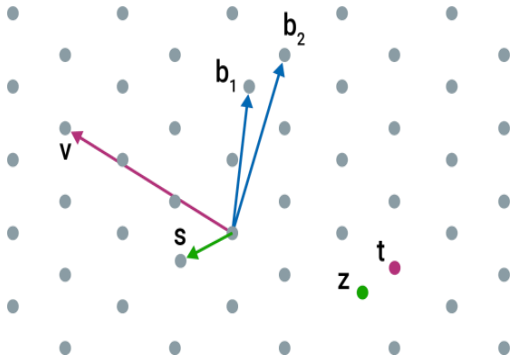

Fig. 2: Lattice pattern

NIST has formalized these structures in two primary standards:

- FIPS 203 (ML-KEM): Derived from CRYSTALS-Kyber, the Module-Lattice-Based Key-
- Encapsulation Mechanism specifies parameters like ML-KEM-512, ML-KEM-768, and ML-KEM1024, providing quantum-safe data encryption mechanisms alongside classical symmetric algorithms
- FIPS 204 (ML-DSA): Derived from CRYSTALS-Dilithium, the Module-Lattice-Based Digital Signature Standard enables authentication and non-repudiation, functioning as the primary standard for protecting digital signatures

Hash Based Cryptography (FIPS 205)

All of the digital signature generation algorithms in hash-based cryptography provide some of the highest theoretical security guarantees in the PQC space (Shor, 1997; Soni et al., 2021). These schemes are not based on mathematical hardness assumptions but are based on the collision and pre-image resistance of well-known cryptographic hash functions (like SHA-3 or BLAKE) (Shor, 1997; Li et al., 2023). NIST recently completed the Stateless Hash-Based Digital Signature Standard (FIPS 205, SLH-DSA), which is based on SPHINCS+. It is a stateless algorithm, which avoids the severe operational limitations of state management in the older hash-based schemes, and is a good fallback option in case of cryptanalytical breakthroughs of lattice-based schemes in the future.

Code Based and Multivariate Cryptography

While not currently finalized as FIPS standards, code-based and multivariate cryptography remain highly active research areas. Code-based cryptography, rooted in the theory of error-correcting codes, relies on the hardness of

decoding random linear codes in the presence of noise (e.g., the McEliece cryptosystem) (Shor, 1997; Bernstein, 2017). Multivariate cryptography relies on the NP-hard problem of solving systems of multivariate polynomial equations over finite fields, offering rapid signature verification at the cost of complex parameter tuning (Shor, 1997; Bernstein, 2017).

Security Models and Algorithmic Countermeasures

The theoretical resistance of a PQC algorithm to Shor's algorithm represents only one dimension of cryptographic security. Algorithms must be proven secure against active, adaptive adversaries operating within formalized cryptographic security models. In the context of post-quantum systems, security proofs must be elevated to the Quantum Random Oracle Model (QROM). Unlike classical models, where an adversary queries a hash function normally, the QROM assumes the adversary possesses a quantum computer and can query the cryptographic hash function in a state of quantum superposition, demanding much tighter mathematical security reductions.

Side-Channel Attacks and Physical Implementation

Although a post-quantum algorithm may be mathematically impenetrable, there are still side-channel attacks (SCAs) that could be implemented. SCAs exploit the physical leakage of the processor running the cryptography without going through the mathematical difficulty of the algorithm (Shor, 1997; Song et al., 2019). The lattice-based schemes such as ML-KEM and MLDSA have complex polynomial sampling, matrix multiplication, and rejection sampling, which gives them unique physical signatures (Shor, 1997). Adversaries can track small changes in power consumption, electromagnetic radiation or time of operation (Shor, 1997). These weaknesses are addressed by careful software engineering, such as programming in constant time and algorithmic masking to hide the power signature (Shor, 1997; Song et al., 2019).

The Standardization and Future Integration

The shift to post-quantum cryptography is a challenge on a scale never before seen in the history of cryptography. The formalisation of FIPS 203, 204 and 205 is driving enterprise environments to shift towards integration phases.

Hybrid Cloud Deployments

One highly recommended approach for the transition period is by implementing hybrid cryptographic architectures. Hybrid systems use a classical asymmetric algorithm with a post-quantum algorithm, since the newly standardized PQC algorithms might have undetected mathematical flaws (Shor, 1997; Li et al., 2023). One notable example is the support of hybrid key exchange in TLS 1.3, where endpoints can be able to negotiate with multiple key exchange algorithms at once (e.g., classical ECDHE in combination with ML-KEM). The key material is generated independently in both the classical and quantum safe channel during a TLS handshake, which makes the communication totally secure against retroactive decryption if the adversary is able to break the classical elliptic curve and the lattice scheme (Li et al., 2023; Song et al., 2019).

Conclusion

One of the biggest security challenges in the modern digital age is the combination of quantum computing and modern cryptography. This review proves that the problem is fundamentally related to the structure of the Bounded-Error Quantum Polynomial-Time (BQP) complexity class, which in particular encompasses the integer factorization and discrete logarithm problems that are the basis of RSA and Elliptic Curve Cryptography. A careful analysis of the security parameters of the two approaches reveals the serious consequences of the quantum security inversion: The classical security properties of ECC are excellent, based on the exponential bound of Pollard's rho algorithm, but the small key sizes require a much smaller number of logical qubits and Toffoli gates to break with Shor's algorithm, making it very susceptible to near-term quantum adversaries. Knowing exactly how the algorithm is supposed to work, from the power of the Quantum Fourier Transform to the period-finding execution of Shor's algorithm, is critical to designing secure systems. Through a concerted effort to deploy the new standardised FIPS 203, 204, and 205 postquantum primitives, as well as hybrid integration protocols. Through proactive efforts to deploy the recently standardised FIPS 203, 204, and 205 postquantum primitives and hybrid integration protocols. Together with TLS 1.3, the cryptographic community can adequately protect digital infrastructures around the world from the coming age of fault-tolerant quantum computers.

Acknowledgment

Thank you to the publisher for their support in the publication of this research article. We are grateful for the resources and platform provided by the publisher, which have enabled us to share our findings with a wider audience. We appreciate the efforts of the editorial team in reviewing and editing our work, and we are thankful for the opportunity to contribute to the field of research through this publication.

Funding Information

The authors have not received any financial support or

funding to report.

Authors Contributions

Both authors contributed equally to this study.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

Availability of Data and Materials

This is a review of existing literature; therefore, no new data were generated or analyzed in this study. All referenced data and materials are available from the cited sources, and further information on these can be accessed through the relevant publications listed in the reference section.

On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2019). *Status report on the first round of the NIST post-quantum cryptography standardization process*. https://doi.org/10.6028/nist.ir.8240

Alaoui, S. M. E. (2013). Code-Based Identification and Signature Schemes in Software. *Lecture Notes in Computer Science*, 122–136. https://doi.org/10.1007/978-3-642-40588-4_9

Apon, D., Perlner, R., Robinson, A., & Santini, P. (2020). Cryptanalysis of ledacrypt. *Annual Int. Cryptol. Conf*, 389–418. https://doi.org/10.1007/978-3-030-56877-1_14

Aumasson, J.-P. (2019). *SPHINCS*.

Bagirovs, E., Provodin, G., Sipola, T., & Hautamäki, J. (2024). Applications of Post-quantum Cryptography. *Computer Science > Cryptography and Security*, 1–17. https://doi.org/10.34190/eccws.23.1.2247

Bao, Z., Guo, J., Li, S., & Pham, P. (2022). Evaluating the Security of Merkle-Damgård Hash Functions and Combiners in Quantum Settings. *Network and System Security*, *13787*, 687–711. https://doi.org/10.1007/978-3-031-23020-2_39

Bennett, C. H., Brassard, G., & Ekert, A. K. (1992). Quantum Cryptography. *Scientific American*, *267*(4), 50–57. https://doi.org/10.1038/scientificamerican1092-50

Bernstein, D. J. (2016). NTRU Prime. *IACR Cryptol. EPrint Arch*, *10719*, 235–260.

Bernstein, D. J. (2017). *Sphincs*.

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188–194. https://doi.org/10.1038/nature23461

Bos, J., Kaihara, M., & Kleinjung, T. (2009). *On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography*.

Buchmann, J., Dahmen, E., & Hülsing, A. (2011). *XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions*. 117–129. https://doi.org/10.1007/978-3-642-25405-5_8

Chailloux, A., Naya-Plasencia, M., & Schrottenloher, A. (2017). An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography. *Advances in Cryptology – ASIACRYPT 2017*, *10625*, 211–240. https://doi.org/10.1007/978-3-319-70697-9_8

Chong, S.-K., & Hwang, T. (2010). Quantum key agreement protocol based on BB84. *Optics Communications*, *283*(6), 1192–1195. https://doi.org/10.1016/j.optcom.2009.11.007

Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS-Dilithium: Digital Signatures from Module Lattices. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2018*(1), 238–268.

Epstein, S. (2019). Algorithmic No-Cloning Theorem. *IEEE Transactions on Information Theory*, *65*(9), 5925–5930. https://doi.org/10.1109/tit.2019.2910562

Fehr, S. (2018). Classical Proofs for the Quantum Collapsing Property of Classical Hash Functions. *Theory of Cryptography*, *11240*, 315–338. https://doi.org/10.1007/978-3-030-03810-6_12

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access*, *8*, 21091–21116. https://doi.org/10.1109/access.2020.2968985

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*, 433. https://doi.org/10.22331/q-2021-04-15-433

Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. *Algorithmic Number Theory*, *1423*, 267–288. https://doi.org/10.1007/bfb0054868

Jazaeri, F., Beckers, A., Tajalli, A., & Sallese, J.-M. (2019). A Review on Quantum Computing: From Qubits to Front-end Electronics and Cryogenic MOSFET Physics. *2019 MIXDES - 26th International Conference "Mixed Design of Integrated Circuits and Systems,"* 15–25. https://doi.org/10.23919/mixdes.2019.8787164

Jozsa, R. (1997). Entanglement and quantum computation. *Quantum Physics*, 1–11. https://doi.org/10.48550/arXiv.quant-ph/9707034

Jozsa, R. (1999). Searching in Grover's algorithm. *Quantum Physics*, 1–17. https://doi.org/10.48550/arXiv.quant-ph/9901021

Kikuchi, T. (2024). Towards A Post-Quantum Cryptography in Blockchain 1: Basic Review on Theoretical Cryptography and Quantum Information Theory. *Computer Science > Cryptography and Security*, 1–32. https://doi.org/10.48550/arXiv.2407.18966

Kuang, R., Perepechaenko, M., & Barbeau, M. (2022). A new post-quantum multivariate polynomial public key encapsulation algorithm. *Quantum Information Processing*, *21*(10), 360. https://doi.org/10.1007/s11128-022-03712-5

Kumar, M., & Pattnaik, P. (2020). Post Quantum Cryptography (PQC)-An overview: (Invited Paper). *2020 IEEE High Performance Extreme Computing Conference (HPEC)*, 1–9. https://doi.org/10.1109/hpec43674.2020.9286147

Li, S., Chen, Y., Chen, L., Kuang, C., Li, K., & Liang, W. (2023). Post-Quantum Security: Opportunities and Challenges. *Sensors*, *23*(21), 8744. https://doi.org/10.3390/s23218744

Mavroeidis, V., Vishi, Kamer, Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *Computer Science > Cryptography and Security*, *9*(3), 405–414. https://doi.org/10.14569/IJACSA.2018.090354

Micciancio, D., & Regev, O. (2009). Lattice-based Cryptography. *Post-Quantum Cryptography*, *7*, 147–191. https://doi.org/10.1007/978-3-540-88702-7_5

Mozaffari-Kermani, M., & Azarderakhsh, R. (2015). Reliable hash trees for post-quantum stateless cryptographic hash-based signatures. *2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*, 103–108. https://doi.org/10.1109/dft.2015.7315144

Nejatollahi, H., Dutt, N., & Cammarota, R. (2017). Trends, challenges and needs for lattice-based cryptography implementations. *Proceedings of the Twelfth IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis Companion*, 1–3. https://doi.org/10.1145/3125502.3125559

Ravi, P., Roy, S. S., Chattopadhyay, A., & Bhasin, S. (2020). Generic Side-channel attacks on CCA-secure lattice-based PKE and KEMs. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2020*(3), 307–335. https://doi.org/10.46586/tches.v2020.i3.307-335

Rigetti, C. T. (2009). *Quantum gates for superconducting qubits*.

Sahu, S. K., & Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: applications and future prospects. *Frontiers in Physics*, *12*, 1456491. https://doi.org/10.3389/fphy.2024.1456491

Sendrier, N., & Overbeck, R. (2009). Code-Based Cryptography. *Springer Nature Link*, 95–145.

Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, *26*(5), 1484–1509. https://doi.org/10.1137/s0097539795293172

Shor, P. W., & Preskill, J. (2000). Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, *85*(2), 441–444. https://doi.org/10.1103/physrevlett.85.441

Sivasubramanian, K. S. (2020). *A comparative analysis of PostQuantum Hash-based Signature Algorithm*.

Song, Y., Huang, X., Mu, Y., & Wu, W. (2019). A new code-based signature scheme with shorter public key. *Cryptol. EPrint Arch*, *2015*(2), 345–360.

Soni, D., Basu, K., Nabeel, M., Aaraj, N., Manzano, M., & Karri, R. (2021). SPHINCS+. *Springer Nature*, *9*, 141–162. https://doi.org/10.1007/978-3-030-57682-0_9

Sun, S., Zhang, R., & Ma, H. (2020). Efficient Parallelism of Post-Quantum Signature Scheme SPHINCS. *IEEE Transactions on Parallel and Distributed Systems*, *31*(11), 2542–2555. https://doi.org/10.1109/tpds.2020.2995562

Tang, J., & Zhang, F. (2017). A new code-based encryption scheme and its applications. *Int. J. High Perform. Comput. Netw*, *10*(6), 515-523,. https://doi.org/10.1504/IJHPCN.2017.087469

Umana, V. G. (2011). *Post-quantum cryptography*. 156.

Wang, A., Xiao, D., & Yu, Y. (2023). Lattice-based cryptosystems in standardisation processes: A survey. *IET Information Security*, *17*(2), 227–243. https://doi.org/10.1049/ise2.12101