Chapter

Post-Quantum Cryptography: Number Theoretic Foundations and Future-Proof Protocols

Kelvin Tafadzwa Mpofu and Patience Mthunzi-Kufa

Abstract

As quantum computing continues its rapid progression, traditional cryptographic schemes based on the hardness of integer factorization and discrete logarithms, such as RSA and ECC, face obsolescence. This chapter explores the number theoretic underpinnings of Post-Quantum Cryptography (PQC), surveying emerging quantum-resistant protocols including lattice-based, code-based, multivariate polynomial, and isogeny-based cryptography. We analyze the mathematical assumptions behind their security, the role of hard problems in number theory (e.g., shortest vector problem, syndrome decoding, supersingular isogeny graphs), and the computational implications of these approaches. Furthermore, the chapter discusses the transition from classical cryptography to PQC within the NIST standardization process and how these cryptographic primitives align with the modern number theoretic and algorithmic challenges. Designed for both researchers and educators, this chapter aims to bridge theory and practice while emphasizing the continuing centrality of number theory in shaping the future of secure communication in the quantum era.

Keywords: post-quantum cryptography, lattice-based cryptography, isogeny-based cryptography, code-based cryptography, multivariate cryptography, quantum-resistant algorithms, number theory, quantum computing, cryptanalysis, computational hardness, public-key infrastructure (PKI), Shor's algorithm, NIST standardization

1. Introduction

Cryptography is the mathematical discipline concerned with securing information in the presence of adversaries [1]. Its central goals include confidentiality (preventing unauthorized disclosure of information), integrity (ensuring information is not altered), authentication (verifying the identity of communicating parties), and non-repudiation (preventing denial of communication or transactions) [2]. These objectives are achieved by encoding information using algorithms whose security relies on computational hardness assumptions. Modern cryptography can broadly be divided into two categories [3]:

Symmetric-key cryptography [4]: In symmetric systems, the same secret key is used for both encryption and decryption. Examples include the Advanced Encryption

Standard (AES) and block cipher modes of operation that enable large-scale secure communication. The main challenge in symmetric cryptography is secure key distribution, although its efficiency makes it indispensable for practical data protection.

The concept of public-key systems, first introduced by Diffie and Hellman in 1976 [5], makes use of a mathematically related key pair: One key is openly shared for encryption, while the other remains private for decryption. The security of these protocols depends on the number theoretic problems that are considered infeasible to solve efficiently with classical algorithms. For instance, RSA relies on the presumed hardness of factoring large integers, whereas Elliptic Curve Cryptography (ECC) draws its security from the difficulty of computing discrete logarithms on elliptic curves [6–8]. Both RSA and ECC have become foundational to modern digital security, providing the cryptographic basis for secure web communication, electronic signatures, and the wider Public Key Infrastructure (PKI). A comparison between symmetric-key and public-key paradigms is presented in **Table 1**, highlighting their strengths, weaknesses, and how their security assumptions are challenged in the quantum computing era [8].

The strength of classical public-key systems rests on the assumption that these problems cannot be solved efficiently by classical algorithms [9]. The best known method for factoring large integers on conventional machines, the Number Field Sieve, still requires super-polynomial resources, making RSA with sufficiently large keys practically secure [10]. Similarly, solving discrete logarithms on elliptic curves is infeasible for appropriately chosen curve parameters. However, this security paradigm is being fundamentally reshaped by advances in quantum computing. Shor's algorithm [11] demonstrates that both integer factorization and discrete logarithms can be solved in polynomial time on a sufficiently powerful quantum computer, rendering RSA and ECC insecure [12]. Even symmetric schemes face challenges, as Grover's algorithm provides a quadratic speedup for brute-force key searches, motivating longer key sizes [13].

The emergence of quantum computing underscores the urgent need for Post-Quantum Cryptography (PQC), a field dedicated to creating algorithms that remain secure even when confronted by adversaries with quantum capabilities [14]. The objective of PQC extends beyond protecting confidentiality and authenticity; it also

Feature	Symmetric-key cryptography	Asymmetric (public-key) cryptography
Key usage	Same key for encryption and decryption	Public key for encryption, private key for decryption
Examples	AES, DES, ChaCha20	RSA, ECC, Diffie–Hellman
Performance	Fast and efficient for bulk data encryption	Slower, higher computational cost
Security basis	Relies on secrecy of the shared key	Based on hardness of number theoretic problems (factorization, discrete logarithm)
Key distribution	Requires a secure channel to exchange keys	Public key can be distributed openly
Main limitation	Key exchange problem	Vulnerable to quantum algorithms such as Shor's algorithm

Table 1.
Comparison between symmetric-key and asymmetric (public-key) cryptography.

seeks to guarantee the long-term reliability of essential cryptographic services such as digital signatures, key exchange mechanisms, and encrypted data storage. A solid grasp of the mathematical underpinnings of conventional cryptography is therefore essential, both to understand the weaknesses revealed by quantum algorithms and to appreciate the quantum-resistant approaches that are explored in this chapter. The transition toward practical quantum computers represents one of the most profound turning points in information security since the original development of public-key cryptography [15]. Established schemes like RSA and Elliptic Curve Cryptography (ECC) derive their strength from the assumed hardness of number theoretic problems such as factoring large integers and solving discrete logarithms. Yet Shor's algorithm demonstrates that these problems can be solved in polynomial time on a sufficiently advanced quantum machine, creating an immediate imperative for the design of protocols capable of withstanding quantum-enabled attacks.

Post-Quantum Cryptography is a rapidly evolving field that seeks to design cryptographic systems resistant to quantum attacks while remaining compatible with existing classical infrastructure. This chapter explores the number theoretic foundations of PQC, elucidates the mathematical hardness assumptions that underpin quantum-resistant protocols, and maps the current transition process being overseen by standardization bodies such as National Institute of Standards and Technology (NIST).

2. Description of post-quantum cryptography

Post-Quantum Cryptography encompasses cryptographic methods built to remain secure against adversaries equipped with either classical or quantum computing power. Current standards such as RSA and ECC depend on the presumed difficulty of tasks like factoring large integers and solving discrete logarithms, challenges that are infeasible for traditional computers. However, once scalable quantum machines are available, these underlying assumptions no longer hold. Shor's algorithm would enable efficient factoring and discrete log computations, while Grover's algorithm accelerates brute-force searches, together threatening the security of nearly all existing public-key systems. PQC aims to counter this looming threat by building security on mathematical problems that are believed to be resistant to both classical and quantum adversaries. Rather than discarding traditional cryptography altogether, PQC replaces the underlying hard problems with alternatives such as structured lattices, error-correcting codes, multivariate polynomial equations, and isogenies of elliptic curves. Of these, structured lattice problems (e.g., Learning With Errors) and hash-based constructions currently dominate the field, with several algorithms selected for standardization. The U.S. NIST has led a global effort to evaluate and standardize PQC algorithms. Initiated in 2016, this open process invited worldwide cryptographers to submit the candidate schemes and subjected them to extensive cryptanalysis. From the original pool of 69 submissions, NIST has finalized a first set of PQC standards in 2024 [16]. These include lattice-based schemes for key encapsulation and digital signatures, alongside a hash-based signature scheme. By providing multiple families of algorithms, the standards are designed to ensure resilience even if one mathematical assumption is later weakened. The urgency of PQC arises not only from the eventuality of a "cryptographically relevant" quantum computer, but also from the risk of so-called "harvest now, decrypt later" attacks, in which encrypted data is collected today with the expectation that it can be decrypted once quantum computers mature.

Because the migration to new standards can take a decade or more, organizations must prepare now by inventorying cryptographic dependencies and planning for replacement. PQC therefore represents both a research frontier in mathematics and computer science and an immediate engineering challenge for securing global communications. Finally, it is important to distinguish PQC from quantum cryptography. Although the names are similar, PQC is purely mathematical and designed for deployment on conventional digital hardware. Quantum cryptography, by contrast, exploits the physical principles of quantum mechanics (such as the no-cloning theorem) to create fundamentally new secure communication protocols. Both approaches are expected to play complementary roles in the post-quantum era, but PQC has the practical advantage of compatibility with the existing network infrastructures [17].

3. Quantum computing and quantum cryptography

Quantum computing marks a fundamental departure from the classical model of computation, utilizing quantum mechanical principles to handle information in novel ways [18]. Whereas conventional machines process binary digits (bits) that take values strictly of 0 or 1, quantum computers rely on quantum bits (qubits). A qubit leverages two distinctive quantum properties, the first being superposition—allowing it to exist as a linear combination of $|0\rangle$ and $|1\rangle$, and thereby encode an exponentially large set of states simultaneously. A single qubit can be expressed as a superposition of the computational basis states:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where $\alpha, \beta \in \mathbb{C}$ and the normalization condition holds:

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2}$$

For example, applying the Hadamard gate to $|0\rangle$ produces an equal superposition:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle). \tag{3}$$

Extending this to two qubits, applying Hadamard gates to both $|0\rangle$ states yields:

$$|\psi\rangle = H|0\rangle \otimes H|0\rangle = \frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle). \tag{4}$$

Another useful property of quantum technologies is entanglement which are correlations between qubits that cannot be described classically, allowing the distributed systems of qubits to exhibit non-local behavior and enabling quantum parallelism [12]. As shown in **Figure 1**, the circuit applies a Hadamard gate to the first qubit followed by a CNOT, creating the maximally entangled Bell state $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$. The evolution of a quantum state is governed by unitary transformations, which is implemented in practice as quantum gates. Collections of gates form quantum circuits, analogous to logic circuits in classical computing. Measurement collapses the quantum state, yielding classical outcomes with probabilities determined by the amplitudes of the superposition.

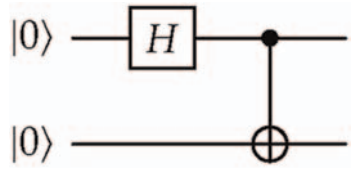

Figure 1.
Bell-state preparation: H on the first qubit, then $\mathrm{CNOT}_{1\to 2}$.

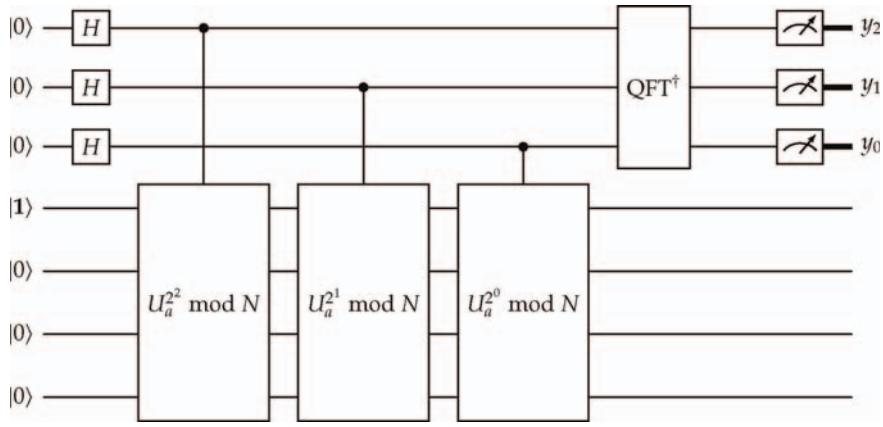

Figure 2.
High-level circuit for Shor's period-finding subroutine. The top t-qubit register (here, $t = 3$*) undergoes Hadamards and then controls three modular-exponentiation unitaries* $U_a^{2^k} \mathrm{mod} N$ *on the n-qubit target register (here* $n = 4$*). Finally, an inverse QFT is applied to the control register and the outcomes* $y_2 y_1 y_0$ *are processed (continued fractions) to estimate the period r.*

The advantage of quantum computing lies in its ability to tackle problems that are considered infeasible for conventional algorithms. Two well-known quantum algorithms highlight this strength: Shor's algorithm demonstrates that large integer factorization and discrete logarithms can be solved in polynomial time, thereby undermining the security assumptions of RSA and ECC, while Grover's algorithm offers a quadratic acceleration for exhaustive search tasks, effectively lowering the security margin of symmetric-key cryptography. Although practical, large-scale fault-tolerant quantum processors are still under construction, continuous advances in hardware development and error-correction techniques make the eventual compromise of classical cryptosystems an increasingly realistic concern. This anticipated breakthrough forms the driving force behind PQC, whose goal is to develop primitives that remain robust even against quantum-enabled adversaries. **Figure 2** depicts the schematic of Shor's period-finding routine, the key component of the factoring algorithm. In this circuit, the upper t-qubit register, initialized as $|0\rangle^{\otimes t}$, is transformed into a superposition through Hadamard operations and then used to control modular exponentiation gates $U_a^{2^k} \mathrm{mod} N$ applied to an n-qubit target register. The target register, starting in the state $|1\rangle$, evolves coherently under these controlled unitaries, embedding the periodic structure of $a^x \mathrm{mod} N$ into the phase of the control qubits. An inverse Quantum Fourier Transform ($\mathrm{QFT}^\dagger$) is applied to the control register, and measurement produces the outcome (y_2, y_1, y_0). Using the continued fractions algorithm, this outcome allows one to estimate the period r, illustrating how Shor's method achieves its exponential speedup compared with the classical factoring approaches.

3.1 Quantum Fourier transform and phase estimation: Introduction to the quantum Fourier transform

Currently, the best classical algorithm for factoring an n-bit integer is the Number Field Sieve, which requires approximately $\exp\left(\theta n^{1/3}(\log n)^{2/3}\right)$ operations. The parameter θ depends on the variation of the method used:

- $\theta \approx 1.52$ when factoring numbers near a large power,
- $\theta \approx 1.92$ for general odd positive integers, and
- $\theta \approx 1.90$ using multipolynomial variants [12].

Due to this exponential complexity, classical factorization becomes intractable for large n. In contrast, a quantum computer can factor an n-bit number in roughly $O(n^2 \log n \log\log n)$ operations [12]. At the heart of Shor's algorithm and several other quantum algorithms lies the *Quantum Fourier Transform* (QFT), a quantum analogue of the discrete Fourier transform (DFT). While it does not accelerate the classical computation of DFTs, QFT enables efficient solutions to problems like order-finding, period estimation, and ultimately, integer factorization.

3.2 The quantum Fourier transform

The classical discrete Fourier transform of a vector $\vec{a} = (a_0, a_1, \ldots, a_{N-1})$ produces a new vector $\vec{b} = (b_0, b_1, \ldots, b_{N-1})$ given by:

$$b_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j \exp\left(\frac{2\pi i j k}{N}\right). \tag{5}$$

The QFT acts on quantum states. Given the orthonormal basis $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$, the QFT is a linear operator defined by:

$$|j\rangle \overset{\text{QFT}}{\rightarrow} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(\frac{2\pi i j k}{N}\right) |k\rangle. \tag{6}$$

For an arbitrary quantum state $\sum_{j=0}^{N-1} x_j |j\rangle$, the QFT yields:

$$\sum_{j=0}^{N-1} x_j |j\rangle \overset{\text{QFT}}{\rightarrow} \sum_{k=0}^{N-1} y_k |k\rangle, \tag{7}$$

where the amplitudes y_k correspond to the classical DFT of the input amplitudes x_j. The QFT is a unitary transformation (**Figure 3**), and its inverse is used in quantum algorithms such as phase estimation. **Figure 3** shows a typical QFT quantum circuit (excluding final SWAP gates).

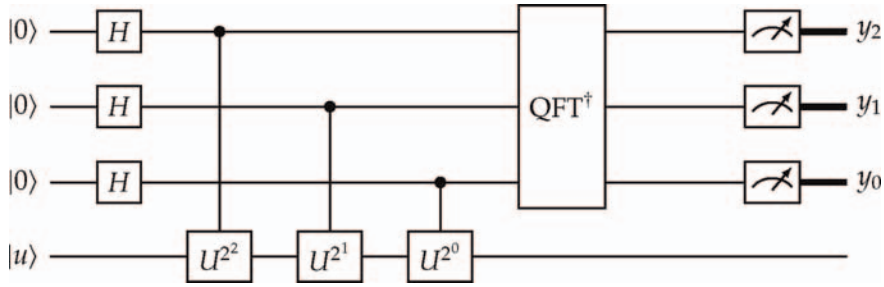

Figure 3.
Quantum circuit for the phase estimation algorithm. The control register undergoes Hadamard gates, controlled unitary operations U^{2^k}, and an inverse QFT before measurement.

3.3 Phase estimation algorithm

The phase estimation algorithm determines the phase ψ in the eigenvalue $e^{2\pi i\psi}$ of a unitary operator U, given access to an eigenstate $|u\rangle$ such that:

$$U|u\rangle = e^{2\pi i\psi}|u\rangle. \tag{8}$$

The algorithm uses t control qubits and one target register initialized as:

$$|0\rangle^{\otimes t} \otimes |u\rangle. \tag{9}$$

Applying Hadamard gates on the control qubits creates a superposition:

$$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|u\rangle. \tag{10}$$

Controlled-U^{2^j} gates are then applied, encoding the phase ψ into the control register:

$$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i\psi j}|j\rangle|u\rangle. \tag{11}$$

Applying the inverse QFT on the control register transforms the phase into a binary approximation $\overline{\psi}$. Measurement yields $\overline{\psi}$ with probability close to 1 provided the phase is close to a binary fraction. **Figure 3** illustrates the complete phase estimation circuit.

3.4 Probability of successful estimation

Let $\overline{\psi}$ be the n-bit approximation of $2^t\psi$. The measurement outcome is accurate to within δ if:

$$2^t\psi = \overline{\psi} + \delta, \quad \text{with} \quad 0 \le \delta < \frac{1}{2^{t+1}}. \tag{12}$$

The final measurement in the computational basis yields $\overline{\psi}$ with probability:

$$\Pr(\overline{\psi}) = \begin{cases} 1 & \text{if } \delta = 0, \\ \left| \frac{1 - e^{2\pi i 2^t \delta}}{2^t (1 - e^{2\pi i \delta})} \right|^2 & \text{if } \delta \neq 0. \end{cases} \tag{13}$$

This shows the phase estimation algorithm succeeds with high probability, especially as t increases.

3.5 Computational complexity

The phase estimation algorithm requires:

- $O(t^2)$quantum gates for inverse QFT,
- One application of the unitary U raised to powers of two,
- $t = n + [\log(2+1/2\epsilon)]$ qubits to achieve n-bit precision with error ϵ.

Detailed complexity analysis is presented in Nielsen and Chuang's foundational text [12].

4. Cryptographic vulnerabilities in the quantum era

The transition from classical to quantum computing has profound implications for the security assumptions that underpin modern cryptographic systems. While conventional cryptography relies on the presumed intractability of certain mathematical problems, quantum algorithms directly target these hardness assumptions, rendering once-secure schemes vulnerable. This section examines the most critical threats posed by quantum algorithms and their broader consequences for public-key infrastructures (PKIs) and digital security as a whole.

4.1 The threat of quantum algorithms

The central challenge posed by quantum computing to modern cryptography stems from its ability to address problems that remain infeasible for classical methods. The clearest illustration is Shor's algorithm, which shows that integer factorization and the discrete logarithm problem can both be resolved in polynomial time once a sufficiently powerful quantum computer is available. This breakthrough directly compromises the foundations of widely used public-key mechanisms, including RSA, Diffie–Hellman key exchange, and elliptic curve cryptography (ECC). To illustrate, RSA relies on the classical difficulty of factoring the product of two large primes, a task that requires sub-exponential resources with the fastest known conventional technique, the Number Field Sieve. Shor's approach, however, reduces this task to $\mathcal{O}(n^3)$ operations with $\mathcal{O}(n^2)$ memory, where n represents the modulus size in bits. Likewise, the elliptic curve discrete logarithm problem (ECDLP), which secures ECC, can also be efficiently broken under Shor's framework. As a result, many of the core primitives supporting digital security would fail once scalable quantum machines become available.

In addition to Shor's algorithm, Grover's algorithm introduces additional challenges, particularly for symmetric key cryptography. Although symmetric ciphers such as AES and hash functions remain more robust to quantum attacks than their public-key counterparts, Grover's algorithm provides a quadratic speedup for brute-force key search and preimage attacks. This effectively reduces the security strength of symmetric systems: a k-bit key offers only $k/2$ bits of quantum security. For example, AES-128, which provides 128-bit classical security, is reduced to 64-bit security against a quantum adversary, which is insufficient for long-term protection. To maintain the adequate post-quantum security levels, symmetric key sizes must therefore be doubled (e.g., AES-256). While this adjustment preserves the viability of symmetric encryption, it emphasizes the disruptive asymmetry of the quantum threat: Public-key primitives are fundamentally broken, while symmetric schemes require only parameter adjustments.

4.2 Collapse of traditional public-key infrastructure (PKI)

The vulnerabilities exposed by quantum algorithms extend far beyond encryption and key exchange. Public-key cryptography also underpins essential services such as digital signatures, authentication protocols, and certificate-based infrastructures. If adversaries equipped with quantum computers can efficiently forge digital signatures, impersonate entities, or retroactively decrypt stored ciphertexts, the trust model of the internet collapses. This scenario is often described as the "quantum apocalypse," the sudden obsolescence of the global PKI [19].

In practical terms, the collapse of PKI would disrupt secure web browsing (TLS/SSL), and secure email protocols (PGP, S/MIME), blockchain and cryptocurrency systems, and virtually all digital identity management systems. Certificates signed with RSA or ECC would no longer be trustworthy, and adversaries could both impersonate legitimate servers and decrypt historical communications that were recorded in encrypted form (a phenomenon known as "store now, decrypt later"). The risk is therefore not merely prospective but also retrospective, threatening the confidentiality of data already transmitted under classical schemes.

To mitigate these risks, a fundamental redesign of PKI is required, integrating quantum-safe primitives that remain secure against both classical and quantum adversaries. Post-Quantum Cryptography offers candidate algorithms, such as lattice-based schemes (e.g., Kyber, Dilithium), code-based encryption (e.g., Classic McEliece), and hash-based signatures (e.g., SPHINCS+), that can replace RSA and ECC while maintaining compatibility with the existing network protocols. Transitioning to such primitives is a complex socio-technical challenge, involving standardization (e.g., the NIST PQC project), software and hardware integration, and widespread migration across critical infrastructure. Nonetheless, this transition is essential to ensure the resilience of digital security in the quantum era.

5. Mathematical foundations of post-quantum cryptography

Post-Quantum Cryptography is grounded in mathematical problems that are believed to resist both classical and quantum attacks. Unlike RSA and ECC, which rely on factorization and discrete logarithms, PQC schemes are built upon problems for which no efficient quantum algorithms are known. This section surveys the main families of post-quantum cryptographic constructions and the mathematical assumptions that support their security.

5.1 Lattice-based cryptography

At the forefront of PQC research is lattice-based cryptography [20], widely regarded as the most versatile and efficient class of quantum-resistant systems. Lattices are discrete periodic structures in $\mathbb{R}^n$, and their complexity arises from the difficulty of finding short or close vectors within these grids. The most important hard problems include:

- *Shortest vector problem (SVP) and closest vector problem (CVP)*: Given a lattice basis, finding the shortest non-zero vector or the closest lattice vector to a target point is conjectured to remain hard even for quantum computers [21].
- *Learning with errors (LWE) and ring-LWE*: These problems introduce noise into linear equations over modular arithmetic, making recovery of the secret vector computationally infeasible [22]. They provide the security foundation for leading NIST candidates such as *CRYSTALS-Dilithium* (digital signatures) and *Kyber* (key encapsulation).

Lattice-based cryptography offers strong worst-case to average-case reductions, meaning that breaking one random instance is as hard as solving the hardest case of the underlying lattice problem [23]. Moreover, structured variants such as Ring-LWE allow efficient implementations, making these schemes well-suited for practical deployment.

5.2 Code-based cryptography

Code-based cryptography, first proposed by McEliece in 1978 [24], builds security on the hardness of decoding random linear codes. The fundamental assumption is the Syndrome Decoding Problem; given a parity-check matrix and a noisy codeword, recovering the original message is computationally hard. Prominent candidates in this category include *Classic McEliece*, which is highly resistant to quantum attacks, and *BIKE*, which leverages structured codes for efficiency. Code-based schemes benefit from decades of cryptanalytic scrutiny and remain strong contenders for long-term security. Their main drawback is the large size of public keys, though modern variants have improved compactness [25].

5.3 Multivariate polynomial cryptography

Multivariate cryptography constructs schemes from systems of quadratic equations over finite fields [26]. Solving such systems, known as the MQ problem, is NP-hard, providing the basis for security. These schemes are particularly attractive for digital signatures, with *Rainbow* being a notable NIST candidate [27]. The strengths of multivariate systems lie in their efficient signing operations and mathematical simplicity. However, they often suffer from very large public key sizes and occasional structural weaknesses discovered through algebraic cryptanalysis, which has led to the deprecation of some candidates during the NIST process.

5.4 Isogeny-based cryptography

Isogeny-based cryptography is the most recent family of PQC constructions, relying on the difficulty of computing isogenies (structure-preserving maps) between

elliptic curves [28]. Supersingular isogeny graphs provide a rich algebraic structure believed to be resistant to both classical and quantum attacks.

- Supersingular Isogeny Diffie–Hellman (SIDH) [29]: Once considered a leading candidate, SIDH was broken by powerful algebraic attacks (Castryck–Decru, 2022).
- CSIDH and other variants [30]: These aim to retain the compact key sizes and unique algebraic features of isogeny-based schemes while improving resilience against cryptanalysis.

Despite recent setbacks, isogeny-based cryptography remains of research interest due to its potential for extremely small key sizes and novel algebraic foundations.

5.4.1 Algebraic number theory in isogeny-based cryptography

Isogeny-based cryptography exploits maps between elliptic curves defined over finite fields. An *isogeny* is a non-constant rational morphism $\varphi : E_1 \to E_2$ that preserves the group law. The security of schemes such as CSIDH and SQISign relies on the presumed hardness of computing paths in supersingular isogeny graphs. From a number theoretic perspective, these constructions are deeply tied to class groups of quadratic fields and quaternion algebras. For instance, the CSIDH protocol uses the action of the ideal class group of $\mathbb{Q}(\sqrt{-p})$ on elliptic curve isomorphism classes, embedding algebraic number theory directly into cryptographic key exchange. The unresolved problem of computing endomorphism rings efficiently for supersingular curves illustrates how open number theoretic questions directly translate into cryptographic assumptions.

5.5 Cyclotomic fields and ring-LWE

A key structural ingredient in lattice-based post-quantum cryptography is the use of *cyclotomic fields* and their associated rings of integers. Recall that the n-th cyclotomic polynomial is defined as

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(x - e^{2\pi i k/n}\right). \tag{14}$$

For n a power of two, $\Phi_n(x) = x^{n/2} + 1$, yielding highly structured rings

$$R_q = \mathbb{Z}_q[x]/(\Phi_n(x)), \tag{15}$$

which form the algebraic backbone of Ring-LWE and Module-LWE schemes. This structure enables efficient arithmetic *via* the Number Theoretic Transform (NTT), while simultaneously connecting security to deep problems in algebraic number theory. In particular, the hardness of Ring-LWE is linked to the difficulty of finding short vectors in ideal lattices associated with cyclotomic fields. This interplay between efficient computation and provable reductions highlights why cyclotomic fields are central to modern PQC.

6. Role of number theory in PQC

Modern PQC schemes continue to draw heavily from classical number theory and algebra. For example:

- Modular arithmetic underpins lattice- and code-based systems, where modular reductions and linear algebraic operations dominate computations [31].
- Algebraic number fields and quaternion algebras provide the structural backbone of isogeny-based schemes [28].
- Cyclotomic fields and polynomial rings are used to optimize structured lattice schemes, enabling efficient implementations of Ring-LWE and Module-LWE systems [32].

This interplay between algebra, geometry, and arithmetic highlights the enduring centrality of number theory in cryptographic design. The same mathematical traditions that enabled RSA and ECC now guide the construction of secure alternatives in the quantum era.

7. NIST standardization process and practical transition

7.1 Overview of the NIST PQC project

In 2016, the U.S. National Institute of Standards and Technology (NIST) initiated an open competition to identify and standardize quantum-resistant cryptographic primitives. The evaluation process emphasized [33]:

- *Provable security*, grounded in hard, well-studied mathematical problems.
- *Implementation efficiency*, ensuring suitability for a wide range of classical hardware platforms.
- *Resilience to side-channel attacks*, ensuring practical security in real-world systems.

7.2 Finalists and selected algorithms

In 2022, NIST announced its first selections for standardization. *Kyber* was chosen as the primary algorithm for public-key encryption and key encapsulation, while *CRYSTALS-Dilithium* was selected for digital signatures. Additional recommendations include *Falcon* (a lattice-based signature scheme) and *SPHINCS+* (a hash-based signature scheme). These selections reflect a balance between mathematical soundness, efficiency, and maturity under cryptanalysis.

7.3 Migration challenges

Transitioning from classical public-key systems to PQC presents significant challenges. Integration into protocols such as TLS and VPNs, and secure email requires careful consideration of:

- *Backward compatibility* with existing infrastructure, ensuring continuity of secure communications during migration.
- *Implementation audits*, including side-channel resistance, memory usage, and performance under constrained devices.

The migration to PQC will likely be gradual, with hybrid schemes (combining classical and quantum-resistant algorithms) deployed during the transition phase. Nevertheless, the urgency of preparing digital infrastructures for the quantum era cannot be overstated.

8. Open research problems and future directions

Despite rapid advances in PQC, several open questions remain:

- *Lattice problems:* Are there sub-exponential quantum algorithms for Ring-LWE or Module-LWE using hidden subgroup techniques?
- *Isogenies:* Can new class-group-based constructions avoid the vulnerabilities that broke SIDH, while retaining compact key sizes?
- *Code-based systems:* How can key sizes be further reduced without compromising security?
- *Multivariate systems:* Can we design trapdoor functions that resist algebraic cryptanalysis while remaining efficient?
- *Global adoption:* Beyond NIST, how will regions such as Africa approach PQC migration, especially in lightweight IoT and mobile environments?

These challenges underscore the continuing dialog between number theory, algebraic geometry, and cryptography. The frontier of PQC is therefore not only an engineering problem but also a fertile ground for pure mathematical research.

Toy problems serve as simplified illustrations of otherwise intractable cryptographic challenges, allowing readers to build intuition before engaging with the full mathematical complexity. For example, the Shortest Vector Problem (SVP) can be introduced using a two-dimensional lattice generated by simple basis vectors, where identifying the shortest vector is straightforward, yet the same task becomes computationally infeasible in high dimensions. Similarly, the syndrome decoding problem may be demonstrated with a small parity-check matrix and a single error, showing how easy cases contrast with the hardness underlying code-based cryptography. Even in quantum algorithms, period finding for small modular functions (e.g., $f(x) = 2^x \bmod 15$) offers a concrete stepping stone toward understanding Shor's algorithm. These illustrative exercises not only demystify abstract problems but also highlight why their large-scale versions provide the foundation for post-quantum security.

9. Conclusion

The advent of large-scale quantum computing poses an unprecedented challenge to the security foundations of modern cryptography. The Shor and Grover algorithms

demonstrate that RSA, ECC, and even symmetric primitives cannot remain unaltered in the quantum era. Post-quantum cryptography offers a spectrum of alternatives, lattice-based, code-based, multivariate, and isogeny-based schemes grounded in hard mathematical problems that resist both classical and quantum attacks. A recurring theme throughout this chapter is the enduring role of number theory, which not only shaped the foundations of RSA and ECC but also guides the construction of quantum-resistant protocols. The NIST standardization process has accelerated the transition from theoretical constructs to practical deployment, with algorithms like Kyber and Dilithium now positioned as future cornerstones of global security infrastructures. However, migration to PQC presents both technical and organizational challenges, from ensuring backward compatibility to defending against implementation-level vulnerabilities. As research continues, hybrid models and further cryptanalytic scrutiny will be vital in guaranteeing the long-term robustness of quantum-safe primitives. Ultimately, the future of secure communication will rely on the successful integration of these post-quantum tools, ensuring resilience in the face of quantum adversaries.

Acknowledgements

The authors acknowledge the Council for Scientific and Industrial Research (CSIR) and the Department of Science and Innovation (DSI) for the grant of funding for this research. K.M. was also supported by the South African Quantum Technology Initiative (SAQuTi) and South African Medical Research Council (SAMRC).

Conflict of interest

The authors declare no conflict of interest.

Nomenclature

AES	advanced encryption standard
CVP	closest vector problem
ECDLP	elliptic curve discrete logarithm problem
ECC	elliptic curve cryptography
KEM	key encapsulation mechanism
LWE	learning with errors
NIST	National Institute of Standards and Technology
NTRU	N-th degree truncated polynomial ring units
PKI	public-key infrastructure
PQC	post-quantum cryptography
QFT	quantum Fourier transform
RSA	Rivest–Shamir–Adleman cryptosystem
SIDH	supersingular isogeny Diffie–Hellman
SPHINCS+	stateless practical Hash-based incredibly nice cryptographic signature
SVP	shortest vector problem

Author details

Kelvin Tafadzwa Mpofu[1*†] and Patience Mthunzi-Kufa[1,2,3†]

1 Biophotonics, Photonic Centre, Manufacturing, Council of Scientific and Industrial Research (CSIR), Pretoria, South Africa

2 Molecular and Cell Biology Department, University of Cape Town, South Africa

3 School of Interdisciplinary Research and Graduate Studies (UNESCO), College of Graduate Studies, University of South Africa, Pretoria, South Africa

*Address all correspondence to: kmpofu@csir.co.za

† These authors contributed equally.

IntechOpen

References

[1] Pachghare V. Cryptography and Information Security. 3rd ed. New Delhi, India: PHI Learning Pvt. Ltd.; 2019

[2] Halpin H. The adversary: The philosophy of cryptography. Journal of Cybersecurity. 2025;**11**(1):tyaf006

[3] Easttom C. Modern Cryptography: Applied Mathematics for Encryption and Information Security. Cham, Switzerland: Springer; 2015

[4] Delfs H, Knebl H. Symmetric-key cryptography. In: Introduction to Cryptography: Principles and Applications. 3rd ed. Berlin, Heidelberg: Springer; 2015. pp. 11-48

[5] Merkle RC. Secure communications over insecure channels. Communications of the ACM. 1978;**21**(4):294-299

[6] Saho NJG, Ezin EC. Comparative study on the performance of elliptic curve cryptography algorithms with cryptography through rsa algorithm. In: Watson B, Badouel E, Niang O, editors. Proceedings of CARI 2020 – Colloque Africain sur la Recherche en Informatique et en Mathématiques Appliquées. Thiés, Senegal: École Polytechnique de Thiés, October 2020, hAL Id: hal-02926106. [Online]. Available from: https://hal.science/hal-02926106

[7] Koblitz N. A Course in Number Theory and Cryptography, 2nd ed., ser. Graduate Texts in Mathematics. Vol. 114. New York, NY, USA: Springer; 1994

[8] Abdullah K. Comparison between the Rsa Cryptosystem and Elliptic Curve Cryptography [Ph.D. dissertation]. Hamilton, New Zealand: The University of Waikato; 2010

[9] Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Reviews of Modern Physics. 2002;**74**(1): 145

[10] Portmann C, Renner R. Security in quantum cryptography. Reviews of Modern Physics. 2022;**94**(2):025008

[11] Shor PW. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science (FOCS). Los Alamitos, CA, USA: IEEE Computer Society; 1994. pp. 124-134

[12] Nielsen MA, Chuang IL. Quantum Computation and Quantum Information. 10th ed. Cambridge, United Kingdom: Cambridge University Press; 2010

[13] Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC). New York, NY, USA: Association for Computing Machinery; 1996. pp. 212-219

[14] Bagirovs E, Provodin G, Sipola T, Hautamäki J. Applications of post-quantum cryptography. Vol. 1. arXiv preprint arXiv:2406.13258. 2024. pp. 1-15. [Online]. Available: https://arxiv.org/abs/2406.13258. 2024

[15] Sahu SK, Mazumdar K. State-of-the-art analysis of quantum cryptography: Applications and future prospects. Frontiers in Physics. 2024;**12**:1456491

[16] Moody D. Nist PQC Standardization Update. In: National Institute of Standards and Technology (NIST), 2021, presented at the NIST PQC Standardization Conference. Oct 2021. [Online]. Available from: https://csrc.nist.gov/Presentations/2021/pqc-standardization-update-2021

[17] Bavdekar R, Chopde EJ, Agrawal A, Bhatia A, Tiwari K. Post quantum cryptography: A review of techniques, challenges and standardizations. In: 2023 International Conference on Information Networking (ICOIN). Bangkok, Thailand: IEEE; 2023. pp. 146-151

[18] Steane A. Quantum computing. Reports on Progress in Physics. 1998; **61**(2):117

[19] Bene F, Kiss A. Public key infrastructure in the post-quantum era. In: 2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI). Timisoara, Romania: IEEE; 2023. pp. 000077-000082

[20] Nejatollahi H, Dutt N, Ray S, Regazzoni F, Banerjee I, Cammarota R. Post-quantum lattice-based cryptography implementations: A survey. ACM Computing Surveys (CSUR). 2019;**51**(6):1-41

[21] Voulgaris P. Algorithms for the Closest and Shortest Vector Problems on General Lattices [Ph.D. Thesis]. San Diego, La Jolla, CA, USA: University of California; 2011

[22] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. In: In Advances in Cryptology – EUROCRYPT 2010, ser. Lecture Notes in Computer Science. Vol. 6110. Berlin, Heidelberg: Springer; 2010. pp. 1-23

[23] Zhang J, Zhang Z. Lattice-Based Cryptosystems, ser SpringerBriefs in Computer Science. Singapore: Springer; 2020

[24] McEliece RJ. A public-key cryptosystem based on algebraic. Coding Thv. 1978;**4244**(1978):114-116

[25] Nguyen V. Code-based cryptography: Attacking and constructing cryptographic systems. [Doctoral thesis]. Lund, Sweden: Lund University; May 2025. series of Licentiate and Doctoral Theses No. 186, ISSN 1654-790X-186

[26] Wolf C. Multivariate quadratic polynomials in public key cryptography. In: Cryptology ePrint Archive. Vol. 1. 2005. pp. 1-20. [Online]. Available from: https://eprint.iacr.org/2005/393

[27] Shajahan R, Jain K, Krishnan P. A survey on nist 3 rd round post quantum digital signature algorithms. In: 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI). Pune, India: IEEE; 2024. pp. 132-140

[28] De Feo L. Mathematics of isogeny based cryptography. arXiv preprint arXiv:1711.04062. 2017. pp. 1-35

[29] Costello C, Longa P, Naehrig M. Efficient algorithms for supersingular isogeny diffie-hellman. In: Annual International Cryptology Conference. Berlin, Heidelberg: Springer; 2016. pp. 572-601

[30] Kutas P, Martindale C, Panny L, Petit C, Stange KE. Weak instances of sidh variants under improved torsion-point attacks. IACR Cryptology ePrint Archive. 2020;**633**:1-20

[31] Ganesh MAD. Recent advances and innovations in algebraic structures and their applications. Mathematical Innovation. 2025;**1**:1

[32] Washington LC. Introduction to Cyclotomic Fields. Vol. 83. New York, NY, USA: Springer Science and Business Media; 2012

[33] Plan NPA. National institute of standards and technology (nist)