**FMDB** *Transactions on Sustainable Computer Letters*

# Quantum Computing and the Future of Cryptography: From Shor's Algorithm to Post-Quantum Security

**Jouma Ali Al-Mohamad[1,*], Ghefar Alaa Aldeen Alrefai[2], Karthikeyan Sivanandi[3], Premanand Jothilingam[4], Sayyed Khawar Abbas[5], Ijaz Ahad[6]**

[1]Department of Computer and Mobile Communication Engineering, Faculty of Information Engineering, Al-Shahbaa Private University, Aleppo, Aleppo Governorate, Syria.
[2]Department of Informatics and Communications Engineering, Faculty of Engineering, EBLA Private University, Saraqeb, Idlib Governorate, Syria.
[3]Department of Research and Development, Infra Secure AI LLC, Casper, Wyoming, United States of America.
[4]Department of Life Cycle Service, Yokogawa Corporation of America, Sugar Land, Texas, United States of America.
[5]Department of Information Systems, Corvinus University of Budapest, Budapest, Hungary.
[6]Department of Computer Systems Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan, China.
jalmohamad@su.edu.sy[1], ghefar.refai@ebla.edu.sy[2], admin@infrasecureai.com[3], premanand.j@yokogawa.com[4], sayyedkhawar.abbas@uni-corvinus.hu[5], ijazahad1@gmail.com[6]

**Abstract:** The advent of large-scale quantum computing represents a paradigm shift in computational capabilities, with profound implications for modern cryptography. This paper provides a comprehensive analysis of Shor's algorithm—a quantum algorithm that can factor integers in polynomial time—and its existential threat to widely deployed public-key cryptosystems such as RSA and Elliptic Curve Cryptography (ECC). Researchers examine the fundamental principles of quantum computation, including superposition, entanglement, and the quantum Fourier transform that underpin Shor's algorithm. Building on this analysis, researchers survey the emerging landscape of post-quantum cryptography (PQC), evaluating leading candidate families including lattice-based, code-based, multivariate, and hash-based schemes. Additionally, researchers explore quantum cryptography as a complementary approach, particularly quantum key distribution (QKD) and its information-theoretic security guarantees. Researchers conclude with an assessment of the current state of quantum hardware, projected timelines for cryptographically relevant quantum computers, and recommendations for organizations preparing for the post-quantum transition.

**Keywords:** Quantum Computing; Shor's Algorithm; Post-Quantum Cryptography; Quantum Key Distribution; Quantum Fourier Transform; Quantum Key Distribution.

**Received on:** 03/09/2025, **Revised on:** 30/11/2025, **Accepted on:** 07/01/2026, **Published on:** 11/11/2026

**Journal Homepage:** https://www.fmdbpub.com/user/journals/details/FTSCL

**DOI:** https://doi.org/10.69888/FTSCL.2026.000842

**Cite as:** J. A. Al-Mohamad, G. A. A. Alrefai, K. Sivanandi, P. Jothilingam, S. K. Abbas, and I. Ahad, "Quantum Computing and the Future of Cryptography: From Shor's Algorithm to Post-Quantum Security," *FMDB Transactions on Sustainable Computer Letters*, vol. 4, no. 4, pp. 213–226, 2026.

**Copyright** © 2026 J. A. Al-Mohamad *et al.,* licensed to Fernando Martins De Bulhão (FMDB) Publishing Company. This is an open access article distributed under CC BY-NC-SA 4.0, which permits copying, remixing, redistributing, transformation, and building upon the material in any medium so long as the original work is properly cited.

[*]Corresponding author.

## 1. Introduction

Since Rivest, Shamir, and Adleman developed the RSA cryptosystem in 1977, public-key cryptography has underpinned digital security, enabling secure communications, digital signatures, and authentication across the internet [9]. For nearly five decades, this cryptographic infrastructure has protected everything from online banking transactions and email communications to national security secrets and critical infrastructure control systems [10]. The security of these systems rests on the assumed computational hardness of certain mathematical problems: integer factorization for RSA and the discrete logarithm problem for Elliptic Curve Cryptography (ECC) and Diffie–Hellman key exchange. These problems have withstood decades of cryptanalytic attempts, and their resistance to classical attacks has enabled trillions of dollars in digital commerce and the transmission of immeasurable amounts of sensitive data [11]. However, in 1994, a quiet revolution began in the corridors of AT&T Bell Laboratories. Peter Shor, a mathematician and computer scientist, demonstrated that a sufficiently powerful quantum computer could solve both the integer factorization problem and the discrete logarithm problem in polynomial time. This result fundamentally challenged the long-term viability of existing cryptographic infrastructure. The significance of Shor's discovery cannot be overstated. Where classical algorithms require time that grows exponentially with input size, Shor's algorithm achieves an exponential speedup by exploiting quantum mechanical phenomena. To factor a 2048-bit RSA modulus, the best classical algorithm (the General Number Field Sieve) would require billions of years on the most powerful classical supercomputers. Shor's algorithm, running on a fault-tolerant quantum computer of sufficient scale, could accomplish the same task in a matter of hours or even minutes [12].

The 1994 theoretical breakthrough has since evolved into a global technological race [13]. Three decades later, quantum computing has moved from abstract mathematical constructs to experimental devices with dozens to hundreds of qubits. Major technology companies—including Google, IBM, Microsoft, Amazon, and Intel—have established substantial quantum research divisions. Nation-states have recognized quantum computing as a strategic priority, with China, the United States, the European Union, and others investing billions of dollars in quantum research and development. In 2019, Google claimed to have achieved "quantum supremacy," demonstrating that its Sycamore processor could perform a specialized computation in 200 seconds that would take the world's most powerful classical supercomputer approximately 10,000 years. While this specific computation had no practical cryptographic relevance, the demonstration marked a milestone in quantum device engineering. Organizations face a daunting but manageable challenge [14]. Best practices are emerging: cryptographic agility—the ability to replace cryptographic primitives without architectural redesign—is becoming a critical requirement. Hybrid cryptographic approaches that combine classical and post-quantum algorithms offer a prudent path for transition. Inventorying cryptographic assets, prioritizing long-lived data for early protection, and engaging in standards development are concrete steps organizations can take today. This paper provides a rigorous yet accessible treatment of the intersection of quantum computing and cryptography. Researchers address three key questions that are central to understanding both the threat and the response [15]:

- How does Shor's algorithm achieve its computational advantage? Researchers examine the quantum principles of superposition, entanglement, and the quantum Fourier transform, and provide a detailed yet accessible explanation of the algorithm's mechanics and complexity.
- What cryptographic alternatives exist, and how should organizations transition? Researchers evaluate the leading post-quantum cryptography families, analyze performance trade-offs, and provide concrete recommendations for migration strategies.

## 2. Review of Literature

Diffie and Hellman [2] proposed public-key cryptography, enabling secure key exchange over unsecured channels without a shared secret and revolutionising modern cryptography. This idea led to the RSA cryptosystem proposed by Rivest et al. [1], which is now one of the most popular public-key algorithms for encryption, secure communication, electronic signatures, and authentication on the Internet. For over 40 years, RSA and Elliptic Curve Cryptography have been cornerstones of modern cybersecurity, protecting web communications, financial transactions, cloud computing platforms, government infrastructures, healthcare systems, and critical industrial networks. But quantum computing has emerged, challenging the long-term security assumptions underlying RSA and ECC. If sufficiently powerful, quantum computers can solve integer factorisation and discrete logarithm problems in polynomial time [3], making RSA and ECC vulnerable to practical attacks once fault-tolerant quantum computers are available. This finding turned quantum computing from a theoretical research subject into a serious cybersecurity threat. Recent progress in quantum hardware has raised new concerns about cryptographic resilience. Arute et al. [4] demonstrated quantum supremacy with a programmable superconducting processor, providing experimental evidence that quantum computers are moving toward larger, more capable architectures. Current quantum systems are not yet powerful enough to break modern cryptography. Still, rapid progress in qubit fidelity, coherence times, quantum error correction, and scalable processor design is expected to continue, eventually reaching cryptographically relevant quantum computers.

Nielsen and Chuang [6] provide a complete theoretical background on using superposition, interference and entanglement in quantum algorithms to achieve computational advantages over classical computing paradigms. These developments indicate that organisations relying solely on conventional public-key cryptography should start preparing for future quantum threats now, rather than waiting for practical quantum attacks. The cybersecurity implications go beyond future quantum capabilities, because adversaries can already use a harvest-now, decrypt-later strategy. Today's intercepted sensitive encrypted communications could remain secure only until sufficiently powerful quantum computers come online. Government secrets, military communications, financial records, health information, scientific research, intellectual property, diplomatic documents. These are often kept secret for decades. Thus, encrypted data stored today can be fully compromised in the future if organisations delay in moving towards quantum-safe cryptographic mechanisms. To reduce these risks, the National Institute of Standards and Technology (NIST) [5] launched the Post-Quantum Cryptography Standardisation Project, which evaluated dozens of candidate algorithms through multiple rounds of public cryptanalysis, and selected CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+ as the primary algorithms for future standardisation. Moving global digital infrastructure to post-quantum cryptography represents one of the biggest cybersecurity transitions ever undertaken. However, this change differs from prior cryptographic upgrades that used symmetric encryption or hash functions because it requires replacing core public-key algorithms embedded in almost every digital system.

RSA or elliptic curve cryptography underpins Transport Layer Security certificates, secure email systems, virtual private networks, blockchain technologies, electronic signatures, software update mechanisms, firmware authentication, Internet of Things devices, cloud infrastructures and critical industrial control systems. Researchers have studied the mathematical foundations of these cryptographic systems in depth for decades, including sophisticated methods for factorising large integers, such as the Number Field Sieve of Lenstra and Lenstra [7], currently one of the fastest classical algorithms for factorising large integers. But quantum algorithms are much faster than classical methods for factorisation, once we have sufficiently large quantum computers. Practical resource estimation studies have also been performed to investigate the scale of future quantum attacks. In principle, Gidney and Ekera [8] showed that the factoring of RSA-2048 can be done in about eight hours with approximately twenty million noisy qubits and large-scale quantum error correction, suggesting that quantum computing in the cryptographically relevant domain is an engineering problem rather than a theoretical impossibility. Although current quantum hardware is still far from meeting these resource requirements, technological advances make it likely that organisations will start applying cryptographic agility, hybrid cryptography protocols, and standardised post-quantum algorithms long before realistic quantum computers are in use. Early preparation will greatly reduce long-term security risks while keeping sensitive digital information confidential, complete and authentic in the emerging post-quantum era.

## 3. Methodology

### 3.1. The Qubit and Quantum Superposition

Whereas classical bits exist in mutually exclusive states—either 0 or 1—the quantum bit (qubit) can exist in a superposition of both basis states simultaneously. This seemingly simple extension unlocks computational possibilities that are fundamentally inaccessible to classical systems. Mathematically, a qubit state is represented as:

$$| \psi\rangle = \alpha | 0\rangle + \beta | 1\rangle \quad (1)$$

where $\alpha$ and $\beta$ are complex amplitudes satisfying $|\alpha|^2 + |\beta|^2 = 1$. The probability of measuring the qubit in state $|0\rangle$ is $|\alpha|^2$, and in state $|1\rangle$ is $|\beta|^2$ (Figure 1).

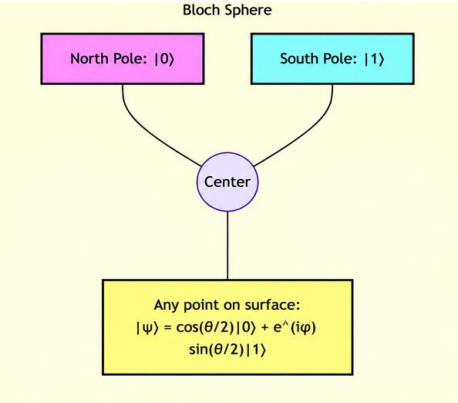



**Figure 1:** Bloch sphere representation of a qubit

Upon measurement, the superposition collapses to one basis state, destroying the quantum information. This probabilistic nature distinguishes quantum computation from classical deterministic computation. The power of superposition lies in quantum parallelism: a quantum computer operating on $n$ qubits can exist in a superposition of all $2^n$ classical states simultaneously, enabling the simultaneous evaluation of a function across an exponential number of inputs.

### 3.2. Quantum Entanglement

Entanglement represents a uniquely quantum correlation between two or more qubits such that the quantum state of each qubit cannot be described independently. For a two-qubit Bell state:

$$|\Phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}} \quad (2)$$

Measurement of one qubit instantaneously determines the state of the other, regardless of spatial separation. Albert Einstein famously described this phenomenon as "spooky action at a distance." However, subsequent research has confirmed entanglement as a fundamental feature of quantum mechanics, not a violation of locality (Figure 2).

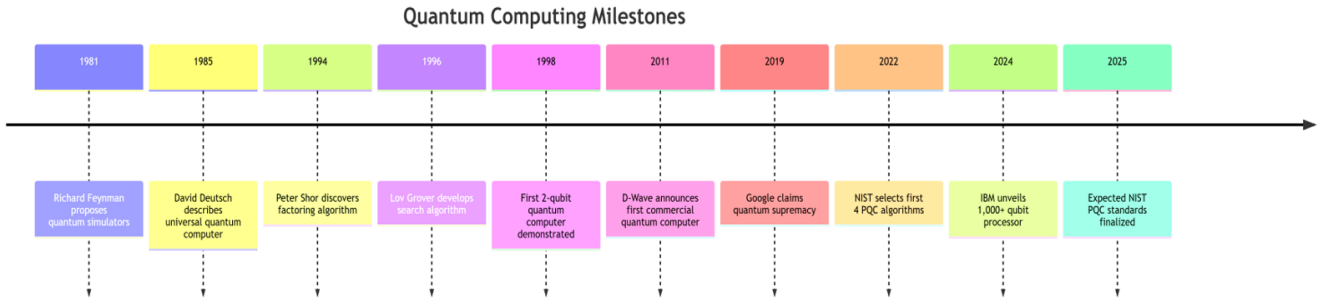



**Figure 2:** Timeline of quantum computing milestones from 1981 to 2024

Entanglement serves as a critical resource for quantum algorithms and quantum communication protocols. In Shor's algorithm, entanglement enables correlations between the input and output registers that are essential for quantum period finding. In quantum key distribution, entanglement underpins device-independent security proofs.

### 3.3. Quantum Gates and Circuits

Quantum computation proceeds through unitary transformations applied to qubits. Unlike classical logic gates, which are irreversible (except for theoretically reversible gates like the Toffoli gate), quantum gates are reversible unitary operations. This reversibility follows directly from the Schrödinger equation, which governs quantum mechanical evolution. Table 1 presents common quantum gates and their matrix representations.

**Table 1:** Common quantum gates

| Gate | Matrix Representation | Function |
|---|---|---|
| Hadamard (H) | $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1 \ 1 & -1\end{bmatrix}$ | Creates superposition |
| Pauli-X (NOT) | $\begin{bmatrix}0 & 1 \ 1 & 0\end{bmatrix}$ | Flips qubit state |
| Pauli-Y | $\begin{bmatrix}0 & -i \ i & 0\end{bmatrix}$ | Flips with phase |
| Pauli-Z | $\begin{bmatrix}1 & 0 \ 0 & -1\end{bmatrix}$ | Applies phase flip |
| CNOT | $\begin{bmatrix}1 & 0 & 0 & 0 \ 0 & 1 & 0 & 0 \ 0 & 0 & 0 & 1 \ 0 & 0 & 1 & 0\end{bmatrix}$ | Conditional flip (entangling) |
| Phase (S) | $\begin{bmatrix}1 & 0 \ 0 & i\end{bmatrix}$ | Applies $\pi/2$ phase shift |
| T (π/8) | $\begin{bmatrix}1 & 0 \ 0 & e^{i\pi/4}\end{bmatrix}$ | Applies $\pi/4$ phase shift |

A quantum circuit comprises a sequence of such gates, analogous to classical logic circuits but operating on quantum states. The quantum circuit model of computation is equivalent to other models, including the adiabatic and measurement-based models. The depth of a quantum circuit—the number of time steps required—directly affects feasibility, as qubits decohere over time and lose quantum information through environmental interaction.

## 4. Result

Shor's algorithm solves the integer factorization problem: given a composite integer $N = p \times q$ (where $p$ and $q$ are primes), find $p$ and $q$. This problem's classical difficulty underpins RSA security. While factoring small numbers is trivial, factoring numbers of cryptographic size—2048 bits, approximately 617 decimal digits—is computationally infeasible with classical algorithms. The significance of Shor's algorithm lies not merely in factoring, but in demonstrating that problems once thought to be intractable for all computers become tractable with quantum resources.

### 4.1. Reduction to Period Finding

The algorithm reduces factorization to period finding through number-theoretic reduction. The steps are as follows:

- Choose a random integer $a$ such that $1 < a < N$ and $\gcd(a, N) = 1$.
- Consider the modular exponential function: $f(x) = a^x \mod N$
- This function is periodic with period $r$, where $r$ is the smallest positive integer satisfying $a^r \equiv 1 \pmod{N}$.
- If $r$ is even and $a^{r/2} \not\equiv -1 \pmod{N}$, then: $\gcd(a^{r/2} \pm 1, N)$

Yield nontrivial factors of $N$. The number-theoretic reduction is efficient on classical computers. The quantum speedup comes from the period-finding step. The probability that a randomly chosen $a$ yields a usable period is at least $1/2$, so a small number of attempts suffice.

### 4.2. Quantum Period Finding

The quantum period-finding algorithm operates on two registers (Figure 3).

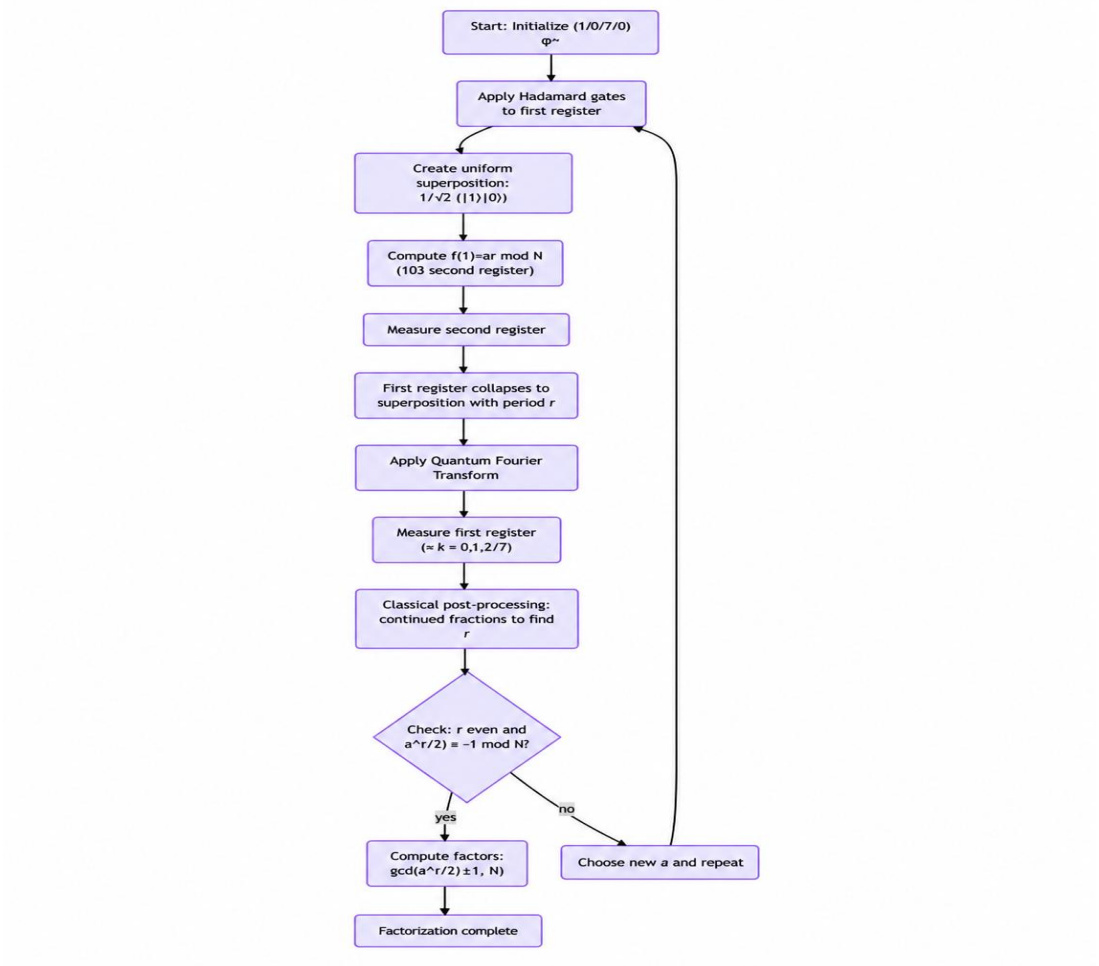



**Figure 3:** Flowchart of quantum period finding in shor's algorithm

The first register contains $n$ qubits, where $2^n > N^2$, allowing sufficient resolution to determine the period. The second register contains enough qubits to represent $N$. The algorithm proceeds as follows:

- Initialize both registers to $|0\rangle^{\otimes n}|0\rangle^{\otimes m}$
- Apply Hadamard gates to the first register, creating a uniform superposition: $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle$
- Compute $f(x) = a^x \mod N$ into the second register: $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|a^x \mod N\rangle$
- Measure the second register. The first register collapses to a superposition of values $x$ that produce the same $f(x)$ value: $\sqrt{\frac{r}{2^n}}\sum_{j=0}^{2^n/r - 1}|x_0 + jr\rangle$
- Apply the Quantum Fourier Transform to the first register, which converts the periodic superposition into a superposition of states peaked at multiples of $2^n/r$.
- Measure the first register, yielding a value $y \approx k \cdot 2^n/r$. Classical post-processing using continued fractions extracts $r$.

### 4.3. The Quantum Fourier Transform

The Quantum Fourier Transform (QFT) is the quantum analogue of the discrete Fourier transform, mapping a quantum state to its frequency domain representation:

$$QFT \mid j\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} \mid k\rangle \quad (3)$$

The QFT can be implemented efficiently with $O(n^2)$ gates, compared to the classical FFT's $O(n2^n)$ complexity for $n$ bits. This exponential speedup is the source of Shor's algorithm's power (Figure 4).

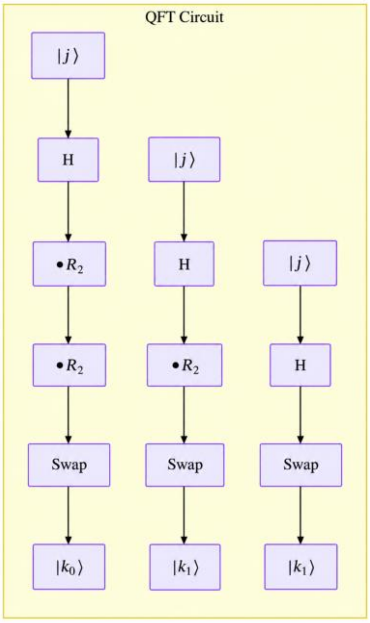



**Figure 4:** Quantum Fourier transform circuit for three qubits

The QFT exploits quantum parallelism to evaluate all frequencies simultaneously. Meanwhile, the classical FFT must compute each frequency component sequentially, or with parallel processors, but still has a fundamental $O(n2^n)$ complexity.

### 4.4. Complexity Analysis

The exponential gap in complexity turns problems that take billions of years on classical computers into hours or minutes on sufficiently powerful quantum computers. For RSA-2048, $\log_2 N = 2048$, so $(\log N)^2 \approx (2048)^2 = 4,194,304$ operations, ignoring logarithmic factors. In practice, constant factors and error-correction overhead increase this substantially, but the asymptotic advantage is decisive (Table 2).

**Table 2:** Complexity comparison for integer factorization

| Algorithm | Complexity | Notes |
|---|---|---|
| Classical (General Number Field Sieve) | $O\left(\exp\left(\left(\sqrt[3]{\frac{64}{9}} + o(1)\right)(\ln N)^{1/3}(\ln \ln N)^{2/3}\right)\right)$ | Sub exponential |
| Shor's Algorithm | $O((\log N)^2 (\log \log N)(\log \log \log N))$ | Polynomial |

### 4.5. RSA Vulnerability

RSA security relies on the difficulty of factoring $N = p \times q$. Shor's algorithm directly attacks this foundation. The number of qubits required to factor RSA-2048 is estimated at approximately 20 million physical qubits, or 4,000–10,000 logical qubits with error correction using the surface code. While 20 million physical qubits is far beyond current capabilities (state-of-the-art devices have 100–1,000 qubits), the trajectory of qubit scaling and error correction improvements suggests this threshold may be reached within 10–30 years.

#### 4.5.1. Elliptic Curve Cryptography Vulnerability

Shor's algorithm can also solve the discrete logarithm problem, which underpins ECC. While ECC offers stronger security per key bit—a 256-bit ECC key provides security roughly equivalent to a 3072-bit RSA key—a quantum computer capable of breaking RSA would also compromise ECC of comparable security levels. The discrete logarithm version of Shor's algorithm requires fewer qubits than the factoring version, potentially making ECC slightly more vulnerable.

#### 4.5.2. Symmetric Cryptography

Symmetric algorithms (AES) and hash functions (SHA-2, SHA-3) face less severe threats. Grover's algorithm provides a quadratic speedup for unstructured search, effectively halving the effective key length. Thus, AES-256 remains secure against quantum attack (effective 128-bit security), though AES-128 is potentially vulnerable (effective 64-bit security, which is on the boundary of feasibility for extremely powerful quantum computers) (Table 3).

**Table 3:** Quantum threats to cryptographic primitives

| Cryptographic Primitive | Classical Security | Quantum Threat | Mitigation |
|---|---|---|---|
| RSA-2048 | 112 bits | Broken by Shor | Migrate to PQC |
| ECC-256 | 128 bits | Broken by Shor | Migrate to PQC |
| AES-128 | 128 bits | ~64 bits (Grover) | Upgrade to AES-256 |
| AES-256 | 256 bits | ~128 bits (Grover) | Acceptable |
| SHA-256 | 128 bits | ~85 bits (Grover) | Acceptable for most uses |

### 4.6. Post-Quantum Cryptography

Post-quantum cryptography (PQC) refers to cryptographic algorithms designed to resist attacks from both classical and quantum computers while running on conventional computing hardware. Unlike quantum cryptography, which requires specialized quantum hardware, PQC algorithms run on classical computers—smartphones, servers, IoT devices, and embedded systems—making them suitable for widespread deployment.

#### 4.6.1. NIST Standardization Process

Since 2016, NIST has conducted a multi-round evaluation of PQC candidates, soliciting submissions from cryptographers worldwide and subjecting them to rigorous public scrutiny. The process has yielded four primary algorithms for standardization, as summarized in Table 4.

**Table 4:** NIST-selected post-quantum cryptography algorithms

| Algorithm | Type | Primary Application | Security Basis |
|---|---|---|---|
| CRYSTALS-Kyber | Lattice-based KEM | Key encapsulation | Module-LWE |
| CRYSTALS-Dilithium | Lattice-based | Digital signatures | Module-LWE, Module-SIS |
| FALCON | Lattice-based | Digital signatures | NTRU lattice |
| SPHINCS+ | Hash-based | Digital signatures | Hash functions |

#### 4.6.2. Lattice-Based Cryptography

- **Learning With Errors (LWE):** Given $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$, find $\mathbf{s}$, where $\mathbf{e}$ is small noise. This problem is believed to be hard even for quantum computers and has been reduced to worst-case lattice problems.
- **Shortest Vector Problem (SVP):** Find the shortest non-zero vector in a lattice. This problem is NP-hard and remains difficult for quantum algorithms.

Lattice-based cryptography offers favorable performance characteristics, with key sizes ranging from 1–10 KB and operation speeds comparable to classical RSA.

#### 4.6.3. Performance Comparison

Performance comparisons between classical and post-quantum algorithms show that PQC is practical for most applications, though it involves trade-offs. CRYSTALS-Kyber, for example, generates keys about 10× faster than RSA-2048, but its ciphertexts and public keys are larger (≈800 bytes vs. 256 bytes for RSA). SPHINCS+, being hash-based, produces large signatures (tens of kilobytes) but offers security based solely on hash function properties, which are exceptionally well understood.

### 4.7. Quantum Cryptography

Quantum cryptography represents an alternative paradigm, leveraging quantum mechanical principles to achieve security properties unattainable with classical cryptography. Rather than relying on computational hardness assumptions, quantum cryptography provides information-theoretic security—security that holds even against computationally unbounded adversaries.

#### 4.7.1. Quantum Key Distribution

Quantum Key Distribution (QKD) enables two parties to establish a shared secret key with information-theoretic security. The BB84 protocol, proposed by Bennett and Brassard in 1984, remains the most widely studied QKD protocol (Figure 5).

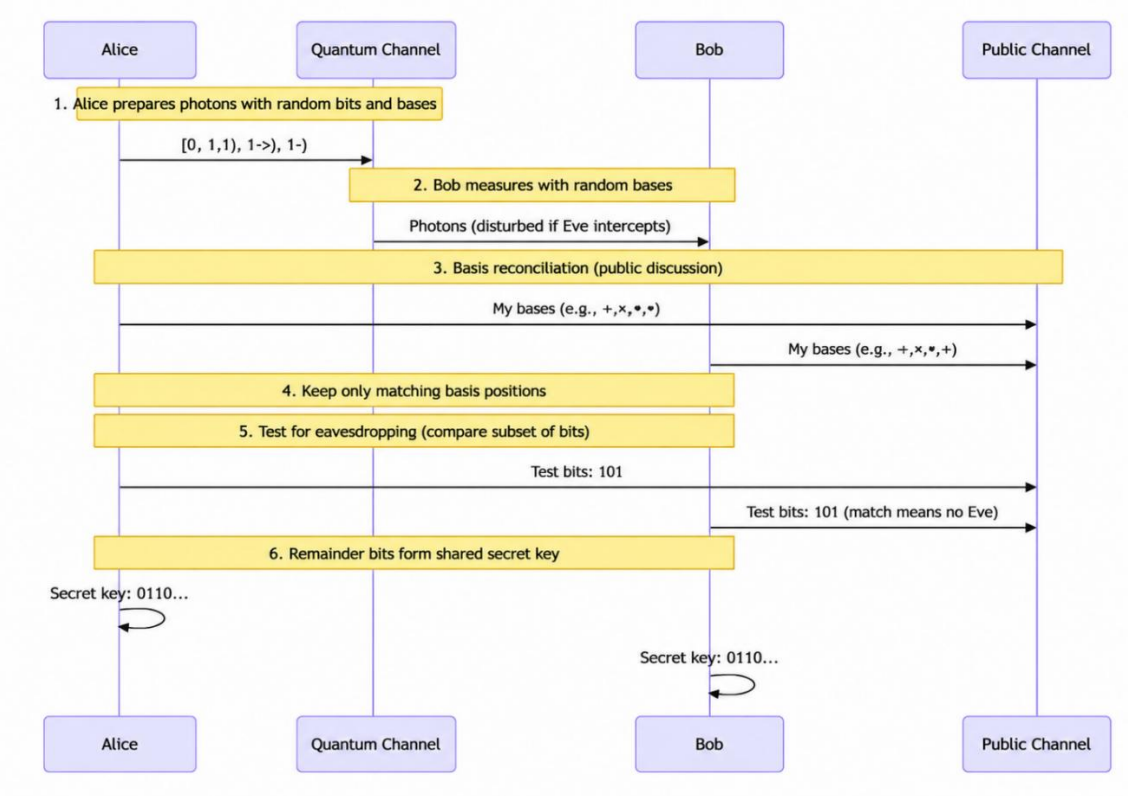



**Figure 5:** BB84 quantum key distribution protocol

The protocol uses single photons polarized in two conjugate bases (rectilinear and diagonal). The sender (Alice) randomly chooses a basis and a bit value for each photon. The receiver (Bob) randomly chooses a measurement basis. After transmission, Alice and Bob publicly compare bases and retain only those bits where bases matched. An eavesdropper (Eve) inevitably introduces quantum measurement disturbances that Alice and Bob can detect through statistical testing.

#### 4.7.2. No-Cloning Theorem and Security

The security of QKD derives from the no-cloning theorem, which prohibits perfect copying of unknown quantum states. Any attempt to intercept the quantum transmission inevitably introduces detectable disturbances, allowing legitimate parties to detect eavesdropping. The no-cloning theorem is a fundamental consequence of the linearity of quantum mechanics: if a unitary operator $U$ could clone arbitrary states, it would violate the superposition principle.

#### 4.7.3. Limitations of QKD

Despite theoretical strengths, QKD faces practical challenges (Figure 6):

- Requires specialized hardware (single-photon sources, ultra-low-noise detectors)
- Distance limitations (typically <100 km without trusted nodes or quantum repeaters)
- Vulnerable to side-channel attacks on implementation (detector blinding, wavelength attacks)
- Not a complete cryptosystem—requires integration with classical encryption for authenticated channels
- High cost and complexity compared to classical alternatives

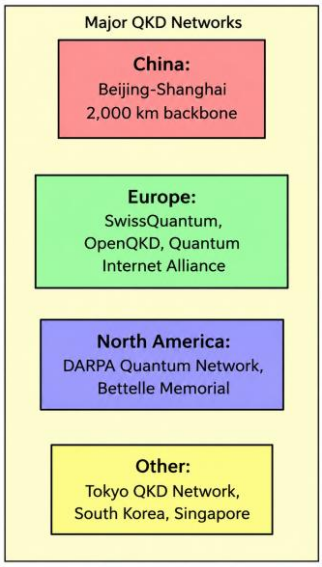



**Figure 6:** Global QKD network deployments

### 4.8. Current State of Quantum Hardware

#### 4.8.1. Leading Quantum Computing Platforms

Table 5 compares five quantum computing platforms, highlighting leading firms, essential features, and qubit counts, demonstrating differences in scalability and performance.

**Table 5:** Leading quantum computing platforms (Based on public disclosures as of 2024)

| Technology | Leading Organizations | Key Characteristics | Current Qubit Count |
|---|---|---|---|
| Superconducting Circuits | Google, IBM, Rigetti | Fast gates, scalable fabrication | 100–1,000+ |
| Trapped Ions | IonQ, Quantinuum | High fidelity, long coherence | 32–56 |
| Photonics | PsiQuantum, Xanadu | Room temperature, scalable optics | 100–200 |
| Neutral Atoms | Atom Computing, QuEra | Highly scalable, programmable arrays | 1,000+ |
| Silicon Spin Qubits | Intel, UNSW | CMOS compatible | 10–50 |

### 4.8.2. Error Correction and Logical Qubits

Current quantum devices are Noisy Intermediate-Scale Quantum (NISQ) devices and lack full error correction. The path to cryptographically relevant quantum computers requires (Figure 7):

- Fault-tolerant logical qubits from hundreds to thousands of physical qubits each
- Error rates below ~1% per gate operation (currently ~0.1–1% for leading platforms)
- Long coherence times exceeding algorithm duration (seconds to hours)

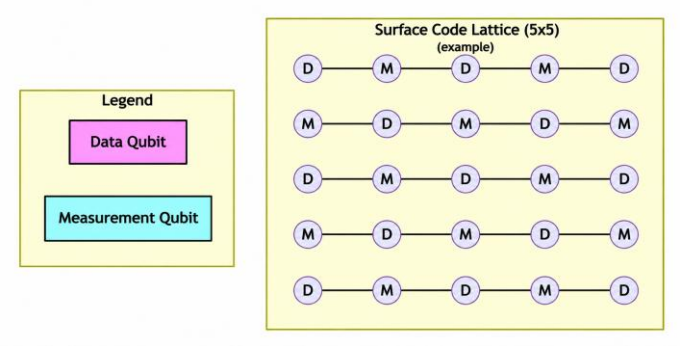



**Figure 7:** Surface code error correction lattice

Estimates for the number of logical qubits required to break RSA-2048 range from 4,000 to 20,000, corresponding to hundreds of thousands to millions of physical qubits with current error correction overheads (Table 6).

**Table 6:** Projected timelines for cryptographically relevant quantum computers

| Confidence | Estimated Timeline | Scenario |
|---|---|---|
| Low | 5–10 years | Optimistic |
| Moderate | 10–20 years | Moderate |
| Moderate | 20–30+ years | Conservative |
| Low | N/A | Never (skeptical view) |

### 4.8.3. Timeline Projections

The concept of "harvest now, decrypt later"—where adversaries collect encrypted data today for future decryption—creates urgency regardless of exact timelines (Figure 8).

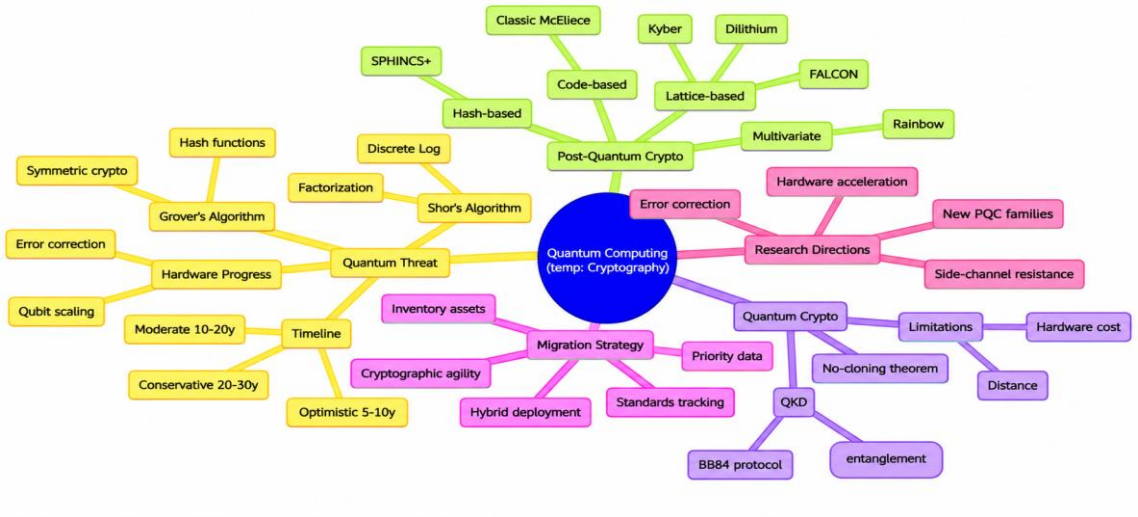



**Figure 8:** Comprehensive mind map of quantum threat and mitigation strategies

## 5. Discussions

In this study, an analysis is provided that confirms that quantum computing has become one of the most important long-term challenges to modern cryptography and cybersecurity. This threat, well understood theoretically through decades of mathematical and computational study, is now poised for exploitation. This is contrasted with traditional computational attacks, which rely on the increase in computational power or implementation weaknesses. Quantum computing breaks new ground in computation and can solve certain mathematical problems that were once thought to be computationally infeasible. One of the most important results is that Shor's quantum algorithm fundamentally changes the security assumptions of public-key cryptography by providing polynomial-time solutions to integer factorisation and discrete logarithm problems. Many widely deployed cryptographic algorithms, such as RSA and Elliptic Curve Cryptography, rely on the computational hardness of these problems. Sufficiently powerful fault-tolerant quantum computers would make such systems inherently insecure. Thus, as quantum computing capabilities advance, existing public-key infrastructures cannot maintain their long-term security guarantees indefinitely. The threat is theoretically established, but practical implementation challenges continue to delay the arrival of cryptography-relevant quantum computers. Today's quantum processors are still limited by relatively few logical qubits, high error rates, short coherence times, limited gate fidelities and the significant overhead of quantum error correction. This means current quantum hardware cannot run large-scale Shor's algorithm on real-world key sizes, such as RSA-2048. Still, quantum computing technology is advancing rapidly.

In recent years, advances in superconducting qubits, trapped-ion systems, photonic quantum processors, neutral-atom architectures, and quantum error-correction techniques have steadily increased computational capabilities. Industry observations suggest that real quantum hardware is still evolving, with more qubits, higher stability and better error management, narrowing the gap between what is theoretically feasible and what is practically achievable. While it remains unclear when cryptographically relevant quantum computers will be available, the current pace of technological development underscores the need for proactive migration rather than a reactive response. One of this study's main achievements is that post-quantum cryptography has matured through intensive international standardisation efforts. For several years, the National Institute of Standards and Technology has led a multi-year evaluation process to select cryptographic algorithms that can withstand attacks from quantum and conventional computers. These standardised algorithms provide workable substitutes for insecure public-key encryption and digital signature systems while having acceptable computational efficiency for a wide range of applications. Performance evaluations show that many post-quantum algorithms are now approaching the operational characteristics of classical cryptographic systems, making them increasingly suitable for deployment across enterprise networks, cloud infrastructures, government information systems, financial institutions, healthcare environments, and industrial communication platforms. This progress indicates that the cybersecurity community no longer lacks quantum-resistant cryptographic solutions, but must instead face the more complex task of incorporating them into globally interconnected digital infrastructures. The shift to quantum-resistant security is unlikely to be a matter of simple substitution of existing cryptographic mechanisms. Instead, one of the biggest industry-wide trends is the increasing adoption of hybrid cryptographic approaches.

Hybrid implementations combine traditional public-key crypto algorithms with standardised post-quantum crypto algorithms during the migration period. This will ensure compatibility with existing infrastructure while protecting against future quantum attacks. Such approaches offer several key benefits, including reduced deployment risk, incremental infrastructure modernisation, ongoing interoperability with legacy systems, and greater resilience to both classical and emerging quantum threats. Hybrid cryptographic mechanisms thus offer a practical middle ground for organisations to improve long-term security without disrupting existing operational environments. Among the security technologies under development for the quantum era, none can meet all security requirements today. The most practical migration path is probably post-quantum cryptography. This can be relatively easily incorporated into existing software infrastructure without requiring specialised communication hardware. Software updates can replace most existing public-key mechanisms with standardised algorithms without changing communication protocols, authentication frameworks, or certificate infrastructures. Moreover, post-quantum encryption scales across applications such as web security, cloud computing, financial services, Internet of Things devices, industrial automation, and secure communication. But these advantages notwithstanding, post-quantum encryption is based on relatively new mathematical hardness assumptions whose long-term security has not yet been subjected to the kind of extensive cryptanalytic scrutiny that RSA and elliptic curve cryptography have enjoyed over the past few decades. Therefore, ongoing mathematical analysis and public cryptanalysis are essential to sustain confidence in the new cryptographic standards. Quantum Key Distribution is an alternative approach that differs fundamentally from mathematical cryptography because its security derives directly from principles of quantum mechanics.

Unlike the computational security of cryptography, quantum key distribution provides information-theoretic security and can detect eavesdropping attempts because quantum measurements unavoidably disturb the system. In the ideal case, these physics-based guarantees offer very strong protection for key distribution. However, practical implementations of quantum key distribution (QKD) are still constrained by several factors, e.g., the need for specialised optical hardware, limited communication distance, high deployment cost, infrastructure complexity, and the lack of independent user authentication.

Quantum key distribution is therefore better suited to specific environments such as government communications, military applications and critical infrastructure than to general commercial deployment. These observations imply that hybrid security architectures combining post-quantum cryptography and quantum key distribution may ultimately offer the highest level of protection for particularly sensitive applications. Researchers combine mathematically secure post-quantum algorithms with physics-based quantum communication technologies to provide multiple independent layers of security, greatly increasing robustness against future cryptographic attacks and reducing reliance on any single security assumption. Much progress has been made, but many challenges remain that affect the global transition to quantum-resistant cybersecurity. One key requirement is developing cryptographic agility. Cryptographic algorithms are now often built directly into hardware, communication protocols, software libraries, authentication infrastructures and enterprise applications. This makes it very difficult to replace an algorithm quickly. Thus, future digital infrastructures must support flexible cryptographic architectures that can replace vulnerable algorithms without a complete system redesign. Developing cryptographic agility is a major long-term goal for both software developers and infrastructure architects.

Another important challenge is the ongoing development of international standardisation. While the primary post-quantum algorithms have been selected, implementation guidelines, interoperability standards, certification procedures, hardware acceleration mechanisms, validation testing and compliance frameworks are still being developed. In the future, processor architectures will likely include dedicated post-quantum cryptographic instructions and hardware accelerators to improve computational efficiency. But widespread hardware integration will require additional years of engineering development, manufacturing, testing and commercial adoption before it can be universally available. Performance considerations also matter throughout the migration process. Many post-quantum cryptographic schemes require substantially larger public keys, ciphertexts, and electronic signatures than traditional public-key cryptography algorithms. These larger data sizes can result in communication overhead in bandwidth-constrained environments such as embedded systems, wireless sensor networks, Internet of Things devices, satellite communication systems, mobile platforms and low-power industrial controllers. Additional computational requirements may also affect battery-powered devices and resource-constrained processors. Therefore, continued research in algorithm optimisation, efficient implementation techniques, hardware acceleration, and lightweight post-quantum cryptographic protocols will remain vital to guarantee practical deployment across various computing environments while maintaining acceptable performance, scalability, and long-term security.

## 6. Conclusion

One of the biggest technological challenges to today's cryptographic infrastructure is quantum computing. Large-scale, fault-tolerant quantum computers capable of breaking widely deployed cryptographic systems are not yet available. Still, Shor's algorithm provides mathematical certainty that current public-key algorithms such as RSA and Elliptic Curve Cryptography will become vulnerable once sufficiently powerful quantum hardware becomes available. This theoretical breakthrough has shifted the cybersecurity community from asking whether the threat exists to preparing for its inevitable arrival. Organisations, for their part, cannot afford to wait to plan their migration because the road to quantum-safe security includes extensive testing, infrastructure upgrades, software changes, and international coordination. Post-quantum cryptography is now mature enough for practical use. The NIST-standardised algorithms provide strong replacements for classical public-key cryptography that integrate well with existing digital infrastructure. Quantum cryptography offers theoretically unconditional security based on quantum mechanics principles, but it requires specialised communication hardware, is complex to deploy and has limited range. This has, so far, limited adoption. Therefore, quantum cryptography should be regarded as a complementary technology that bolsters highly sensitive communication environments rather than substituting post-quantum cryptography across all applications. The best long-term security strategy combines standardised post-quantum cryptography algorithms with cryptographic agility and, where appropriate, hybrid security architectures that add multiple layers of protection.

Organisations and enterprises should start now by taking a full inventory of all cryptographic assets in their infrastructure. This involves identifying all apps that use public-key cryptography, such as Transport Layer Security certificates, code-signing mechanisms, firmware authentication, secure e-mail systems, virtual private networks, cloud services, authentication infrastructures, Internet of Things devices, and blockchain applications. These inventories form the basis for systematic migration planning and risk assessment. Organisations should also implement cryptographic agility so systems can be designed to replace cryptographic algorithms without significant architectural redesign. This will help ensure long-term adaptability as cryptographic standards evolve. During the migration period, it should be feasible to deploy hybrid implementations that combine classical cryptographic algorithms with standardised post-quantum mechanisms to maintain interoperability while increasing resistance to future quantum attacks. Health care records, government intelligence, financial information, legal documents, defence communications and intellectual property all require long-term confidentiality. Sophisticated adversaries will target them with harvest-now-decrypt-later strategies. This information must be given special protection. Standards organisations, regulatory authorities and government agencies also play a critical role in enabling a successful global transition to quantum-resistant cybersecurity. Work should continue to accelerate development of post-quantum cryptographic standards, certification procedures, implementation guidance, validation frameworks and compliance programs that provide organisations

with consistent deployment recommendations. It is recommended that sector-specific migration guidance be developed for critical infrastructure sectors, e.g., healthcare, finance, energy, transport, telecommunications, and government services, so that each sector can adopt standardised quantum-resistant security based on its operational needs. Above all, international interoperability testing frameworks should be established to assess the compatibility of software platforms, communication protocols, hardware devices, cloud services, and enterprise security solutions, thus minimising deployment risks and ensuring uniform implementation across global digital infrastructures.

The research community should continue advancing both quantum computing and post-quantum cryptography to ensure long-term cybersecurity resilience. More progress in quantum error correction is needed to reduce the large physical-qubit overhead currently associated with fault-tolerant quantum computation and to improve the approach's reliability and scalability. At the same time, researchers should study other families of post-quantum cryptography algorithms alongside existing lattice-based standards to preserve cryptographic diversity and reduce dependence on a single mathematical security assumption. To detect possible weaknesses in standardised algorithms before they are widely used, ongoing cryptanalysis should be a major research focus. Special attention should be given to implementation-level vulnerabilities such as side-channel attacks, fault-injection attacks, timing attacks, power analysis, cache-based attacks and hardware security weaknesses that can compromise otherwise mathematically secure cryptographic systems. Continued collaboration among researchers, industry, governments, and international standards bodies can help the global cybersecurity community navigate the transition to a secure post-quantum digital ecosystem while ensuring the continued confidentiality, integrity, and authenticity of information in the quantum era.

**Acknowledgment:** N/A

**Data Availability Statement:** The datasets used in this study are available upon reasonable request to ensure transparency and facilitate research reproducibility.

**Funding Statement:** The authors confirm that this study and the preparation of the manuscript were completed without any external financial assistance or funding.

**Conflicts of Interest Statement:** The authors declare that they have no conflicts of interest that could have influenced or affected the results of this research.

**Ethics and Consent Statement:** The authors consent to making this work accessible to readers for educational, academic, and learning purposes.

**References**

1. R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
2. W. Diffie and M. E. Hellman, “New directions in cryptography,” *IEEE Trans. Inf. Theory,* vol. 22, no. 6, pp. 644–654, 1976.
3. P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM J. Comput.*, vol. 41, no. 2, pp. 303–332, 1997.
4. F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis., “Quantum supremacy using a programmable superconducting processor,” *Nature*, vol. 574, no. 10, pp. 505–510, 2019.
5. G. Alagic, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, and D. Apon, “Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process,” *NIST Interagency/Internal Report (NISTIR)*, 2022. [Accessed by 23/10/2024].
6. M. A. Nielsen and I. L. Chuang, “Quantum Computation and Quantum Information,” 10th ed., *Cambridge Univ. Press*, Cambridge, United Kingdom, 2010.

7. A. K. Lenstra and H. W. Lenstra, "The Development of the Number Field Sieve, Lecture Notes in Mathematics", *Springer*, Cham, Switzerland, 1993.
8. C. Gidney and M. Ekerå, "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits," quantum, vol. 5, no. 4, p. 433, 2021.
9. L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput. (STOC)*, Philadelphia, Pennsylvania, United States of America, 1996.
10. D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 9, pp. 188–194, 2017.
11. M. J. Kannwischer, R. Petri, J. Rijneveld, P. Schwabe, and K. Stoffelen, "Post-quantum crypto library for the ARM Cortex-M4," *GitHub repository*, 2023. [Accessed by 13/05/2025].
12. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys*., vol. 81, no. 9, p. 1301, 2009.
13. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science,* vol. 560, no. 12, pp. 7–11, 2014.
14. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 10, pp. 802–803, 1982.
15. M. Mosca, "Cybersecurity in an era with quantum computers: Will researchers be ready?" *IEEE Security Privacy,* vol. 16, no. 5, pp. 38–41, 2018.

***Publisher's Note:*** *The publisher remains impartial concerning jurisdictional claims in published maps and institutional affiliations. Responsibility for the content rests entirely with the authors and does not necessarily reflect the publisher's perspectives.*