www.ijonest.net

# Preparing Critical Infrastructure for Post-Quantum Cryptography: Strategies for Transitioning Ahead of Cryptanalytically Relevant Quantum Computing

**Amare Geremew**
Capitol Technology University, USA

**Atif Mohammad**
Capitol Technology University, USA

**To cite this article:**

Geremew, A. & Mohammad, A. (2024). Preparing critical infrastructure for post-quantum cryptography: Strategies for transitioning ahead of cryptanalytically relevant quantum computing. *International Journal on Engineering, Science, and Technology (IJonEST)*, *6*(4), 338-365. https://doi.org/10.46328/ijonest.240

International Journal on Engineering, Science, and Technology

2024, Vol. 6, No. 4, 338-365 https://doi.org/10.46328/ijonest.240

# Preparing Critical Infrastructure for Post-Quantum Cryptography: Strategies for Transitioning Ahead of Cryptanalytically Relevant Quantum Computing

**Amare Geremew, Atif Mohammad**

## Article Info

***Article History***

Received:
10 December 2023
Accepted:
13 June 2024

***Keywords***

Post-quantum cryptography
Cryptanalytically relevant
Quantum computing
Critical infrastructure
Cryptographic transition
Quantum-resistant
Algorithms
Artificial intelligent

## Abstract

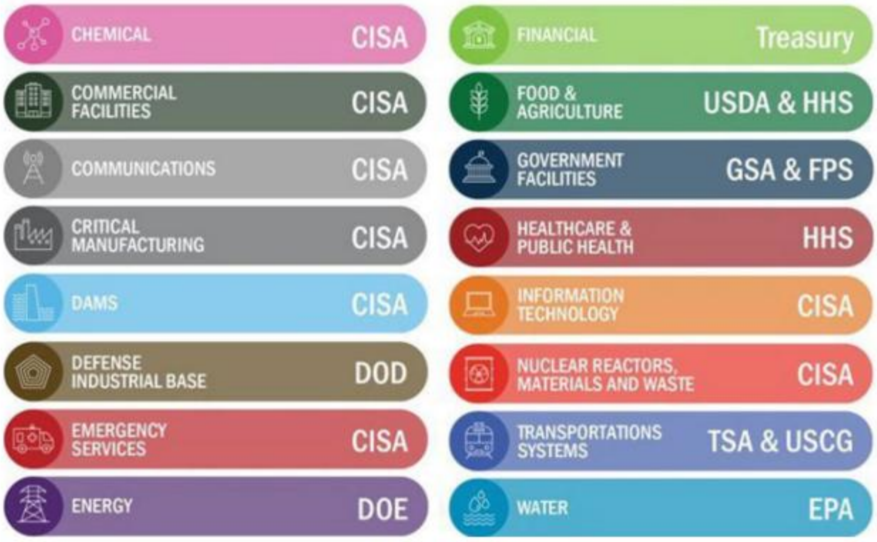
As Cryptanalytically Relevant Quantum Computing (CRQC) approaches, organizations managing critical infrastructure must prepare to transition to Post-Quantum Cryptography (PQC). This paper provides comprehensive guidance for this transition, addressing the challenges of quantum computing to current cryptographic systems. It presents a framework for the efficient and timely adoption of PQC within critical infrastructure. The study examines the current development of PQC, evaluates vulnerabilities in legacy cryptographic algorithms, and identifies key strategies for mitigating risks associated with quantum computing. The proposed framework includes a multi-faceted approach, encompassing the evaluation and selection of PQC algorithms, developing a phased transition plan, and establishing governance structures to ensure the long-term viability of quantum-resistant cryptographic infrastructure. Additionally, the paper underscores the importance of collaboration among business leaders, governmental bodies, and educational institutions to promote knowledge sharing and accelerate the adoption of PQC standards. By proactively addressing the challenges of transitioning to PQC, organizations can enhance the resilience of critical infrastructure, ensuring the confidentiality, integrity, and availability of sensitive data in the face of advancing quantum computing capabilities.

## Introduction

The rapid advancement of quantum computing technology has brought forth a new era of computational capabilities that promise to revolutionize various fields. However, this progress also poses a significant threat to the security of modern cryptographic systems that underpin the protection of sensitive data within critical infrastructure. As the realization of Cryptanalytically Relevant Quantum Computing (CRQC) – the stage at which quantum computers are powerful enough to break the current public-key cryptographic algorithms draws closer, it is important for organizations responsible for safeguarding critical infrastructure to proactively adapt their cryptographic frameworks to withstand the impending quantum-enabled attacks.

The looming quantum threat arises from quantum computers' potential to solve specific mathematical problems, such as integer factorization and discrete logarithms, which form the foundation of widely used public-key cryptography schemes like RSA and elliptic curve cryptography (ECC). The emergence of CRQC would render these cryptographic algorithms vulnerable, jeopardizing the confidentiality and integrity of sensitive information exchanged within critical infrastructure sectors, including communication, energy, transportation, healthcare, and financial services. The United States has identified 16 critical infrastructure sectors, depicted in Figure 1 which are defined as "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." (CISA, 2003).

The 16 critical infrastructure sectors identified by the U.S. Department of Homeland Security are deeply interconnected, forming a complex web of dependencies that underpin national security, economic stability, and public safety. From energy and water systems to healthcare and financial services, these sectors rely heavily on secure communications and data protection, with cryptography serving as a cornerstone of their cybersecurity strategies. The pervasive use of cryptographic protocols across these sectors ensures the confidentiality, integrity, and authenticity of sensitive information and critical operations. However, this widespread reliance also creates a significant vulnerability in the face of quantum computing advancements. As quantum computers threaten to break current encryption methods, the transition to Post-Quantum Cryptography (PQC) becomes not just important, but critical for all sectors. A coordinated shift to PQC is essential because a breach in one sector could have cascading effects across others, potentially compromising national security, disrupting essential services, and causing economic turmoil. Therefore, a unified approach to implementing quantum-resistant cryptography across all critical infrastructure sectors is paramount to maintaining the resilience and security of the nation's most vital systems in the post-quantum era (DSH, 2021).



| | |
|---|---|
| CHEMICAL | CISA |
| COMMERCIAL FACILITIES | CISA |
| COMMUNICATIONS | CISA |
| CRITICAL MANUFACTURING | CISA |
| DAMS | CISA |
| DEFENSE INDUSTRIAL BASE | DOD |
| EMERGENCY SERVICES | CISA |
| ENERGY | DOE |
| FINANCIAL | Treasury |
| FOOD & AGRICULTURE | USDA & HHS |
| GOVERNMENT FACILITIES | GSA & FPS |
| HEALTHCARE & PUBLIC HEALTH | HHS |
| INFORMATION TECHNOLOGY | CISA |
| NUCLEAR REACTORS, MATERIALS AND WASTE | CISA |
| TRANSPORTATIONS SYSTEMS | TSA & USCG |
| WATER | EPA |

Source: CISA

Figure 1. 16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

According to the Department of Homeland Security (DHS), approximately 85% of the 16 U.S. critical infrastructure sectors, including key areas like electricity, water, telecommunications, and financial services, are owned and operated by private enterprises. The remaining 15% is managed by federal, state, and local governments (DHS, 2003). To effectively protect these essential systems, collaboration between private sector companies and federal agencies is vital. This partnership should involve sharing knowledge, best practices, and resources to address the unique challenges of implementing Post-Quantum Cryptography (PQC) in critical infrastructure environments.

As the cryptography community actively engages in research and development of PQC algorithms, the focus is on creating quantum-resistant cryptographic schemes designed to withstand future quantum computers' capabilities. Transitioning from legacy cryptographic systems to PQC is a complex and time-consuming process that demands meticulous planning, coordination, and execution to ensure a smooth transition. This paper explores strategies and best practices for proactively preparing critical infrastructure for the PQC transition before the arrival of CRQC. This paper assesses the current state of post-quantum cryptography, evaluates quantum computing threats to critical infrastructure, and presents a framework for implementing quantum-resistant solutions. The work advances the security and resilience of essential systems as quantum computing capabilities continue to evolve.

## Literature Review

Significant strides have been made in understanding the potential threats posed by quantum computing to current cryptographic systems. Researchers like Mosca and Roetteler have provided mathematical frameworks and timelines predicting the advent of cryptanalytically relevant quantum computers (Mosca & Piani, 2022). Concurrently, efforts by bodies such as the National Institute of Standards and Technology (NIST) have been pivotal in driving forward the standardization of quantum-resistant algorithms (NIST, 2017). Key studies, such as those by Chen et al., have detailed the progress and evaluation criteria of candidate algorithms for PQC, offering vital insights into their security parameters and computational requirements (Chen et al., 2016). In addition to the technical dimensions of PQC, a growing body of literature has focused on the organizational and policy implications of quantum-resistant security. Studies have explored the challenges of integrating PQC into existing security frameworks and governance structures, as well as the role of government agencies and industry stakeholders in driving PQC adoption (World Economic Forum, 2021).

On the other hand, this paper addresses several notable gaps identified in the existing literature, particularly in the practical aspects of PQC implementation across different sectors of critical infrastructure. By focusing on tailored transition strategies, this paper offers a unique contribution to the field by delineating sector-specific guidelines and protocols that consider both the operational peculiarities and the security requirements of varied infrastructures. Moreover, it emphasizes the need for longitudinal performance evaluations and regulatory adaptation, providing a framework that not only anticipates but actively guides the development of compliance.

### Background

Cryptography is a fundamental pillar in the security framework of critical infrastructure, playing a crucial role in protecting sensitive information, facilitating secure communication channels, and preserving the integrity and confidentiality of digital transactions (Stallings, 2017). The current cryptographic landscape comprises both symmetric and asymmetric algorithms, which find widespread application across various critical infrastructure sectors, such as communication, energy, transportation, healthcare, and financial services, underscoring their vital importance in safeguarding these essential domains.

Symmetric cryptography, such as the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES), uses a single shared key for both encryption and decryption. These algorithms are generally faster and more efficient than asymmetric algorithms, making them suitable for encrypting large volumes of data (Daemen & Rijmen, 2002). On the other hand, asymmetric cryptography, also known as public-key cryptography, utilizes a pair of keys – a public key for encryption and a private key for decryption. Widely used asymmetric algorithms include RSA, Elliptic Curve Cryptography (ECC), and Diffie-Hellman key exchange (Diffie & Hellman, 1976). However, the emergence of Cryptanalytically Relevant Quantum Computing (CRQC) presents a grave threat to the security of these cryptographic algorithms (Paine, 2023). Quantum computers, with their ability to perform certain computations exponentially faster than classical computers, have the potential to break the mathematical problems that underpin modern cryptography (Ruane, McAfee, & Oliver, 2022). Shor's and Grover's algorithms are two of the most significant and well-known quantum algorithms that have sparked concerns within the cryptography community due to their potential impact on existing cryptographic systems.

Shor's algorithm, developed by Peter Shor in 1994, is a quantum algorithm that efficiently solves integer factorization and discrete logarithm problems. The security of widely used public-key cryptosystems, such as the RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), heavily relies on the difficulty of solving these problems using classical computers (Shor, 1994, 1999). When Peter Shor published his seminal paper, quantum computers were purely theoretical devices, and no practical implementations were available to run the algorithm. Today, while quantum computing technology has advanced considerably and functioning quantum computers exist, the current models lack the necessary power and scale to run Shor's algorithm efficiently. However, researchers continue to push the boundaries, and future advancements in quantum computing could potentially render these asymmetric cryptography schemes vulnerable. On the other hand, Grover's algorithm, developed by Lov Grover in 1996, is a quantum search algorithm that provides a quadratic speedup for searching unstructured databases (Grover, 1996). Although it's not as disruptive as Shor's algorithm, Grover's algorithm can still affect symmetric cryptography by halving the effective key size, thereby diminishing the security of these algorithms (Bernstein, 2010).

Table 1 summarizes the impact of Shor's and Grover's algorithms on various cryptographic algorithms, hashes, and digital signatures. This context sets the stage for understanding the imperative need for post-quantum cryptography (PQC), which aims to develop secure cryptographic systems against both quantum and classical computational threats. The transition to PQC is not merely a technical upgrade rather, a comprehensive strategy that involves assessing the potential impact of quantum attacks, selecting and implementing quantum-resistant cryptographic algorithms, and developing a comprehensive transition plan to ensure a smooth and secure migration to PQC while equipping all stakeholders with the necessary knowledge and tools to navigate this new era of cryptography effectively.

Table 1. Summary of Shor's and Grover's Algorithms and Their Cryptographic Impact

| Algorithm | Description | Impact on Cryptography | Affected Algorithms | Implications |
|---|---|---|---|---|
| **Shor's** | Employs quantum superposition, entanglement, and Fourier transform for factoring and logarithms. Requires large-scale quantum computer. | Compromises public-key schemes by breaking encryption and digital signature integrity. | RSA, Diffie-Hellman, ECDSA, DSA, ECC | Requires transition to quantum-resistant cryptography, significant impact on secure communication and data integrity. |
| **Grover's** | Utilizes quantum superposition and amplitude amplification for quadratic speedup in searching unstructured data; needs large-scale quantum setup. | Reduces key strength in symmetric schemes by halving effective key size. | AES, SHA-2, SHA-3 | Requires longer key sizes in symmetric cryptography, moderate adjustment compared to Shor's impact, emphasizes need for enhanced security measures. |

## Navigating the Quantum Threat Landscape

This paper first addresses the pressing need for Post-Quantum Cryptography (PQC) adoption, then presents a structured transition framework. Among these critical drivers are the economic impacts, national security concerns, cryptographic breakthroughs, historically prolonged transition periods, and government compliance mandates, as discussed in the sections that follows.

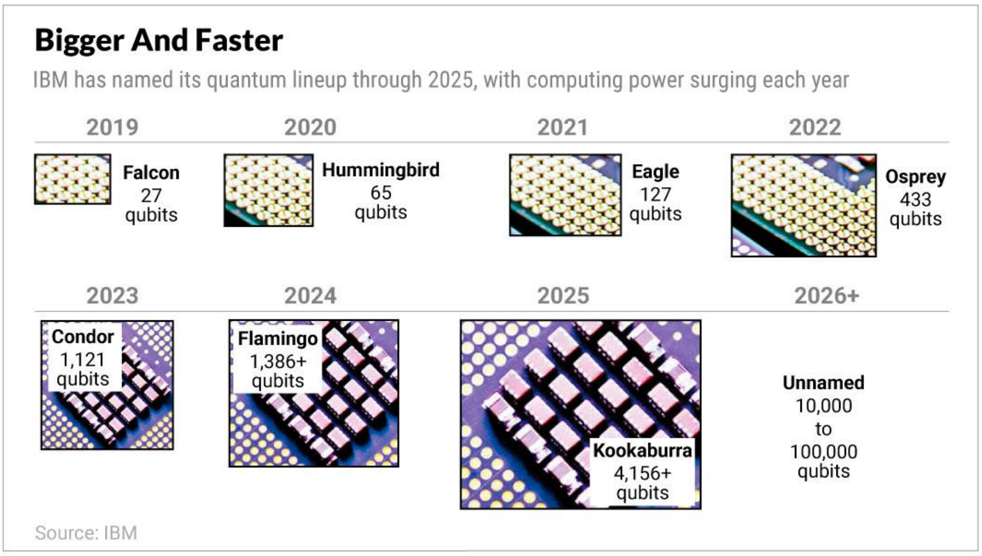
### *A. Business and National Security Implications*

The emergence of Cryptanalytically Relevant Quantum Computing (CRQC) presents a profound threat to the security of our digital infrastructure, with serious implications for both the business world and national security (Paine, 2023). The advancement of quantum computing threatens to compromise current cryptographic standards, creating vulnerabilities in data protection, intellectual property security, and critical infrastructure systems. Given the interdependence of modern digital services, organizations that delay implementing post-quantum cryptography (PQC) risk financial exposure, loss of stakeholder confidence, and potential service interruptions.

Moreover, the quantum threat poses grave challenges to national security, as the ability to decrypt classified communications and sensitive intelligence could grant hostile nation-states an immense strategic advantage (Lydersen et al., 2010). The compromise of military secrets, diplomatic communications, and critical infrastructure could undermine the very foundations of national defense and sovereignty (Wallden & Kashefi, 2019). Thus, adopting PQC is essential for maintaining national security and economic resilience.

### B. *Accelerated Quantum Computing Development*

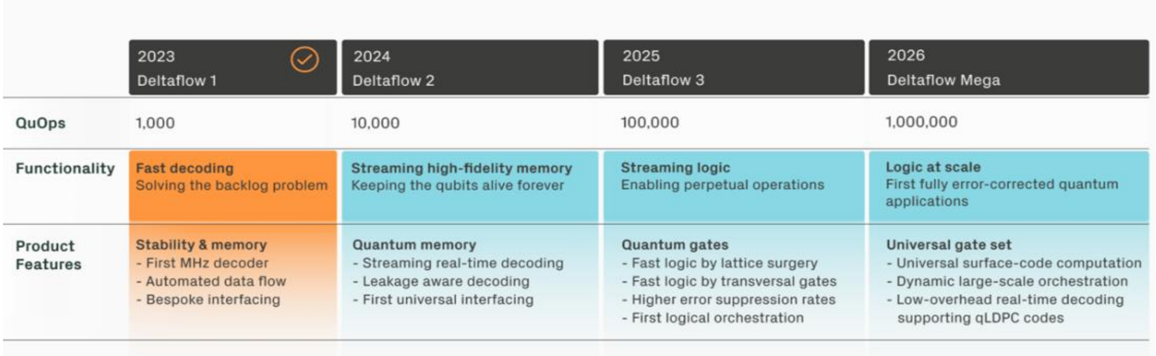
Quantum computing development continues to accelerate, with major technology companies achieving significant milestones that suggest Cryptanalytically Relevant Quantum Computing (CRQC) may arrive sooner than initial estimates indicated. For example, IBM demonstrated significant progress in quantum computing with its 433-qubit processor in November 2022, representing a threefold increase from its previous year's capability (Krause, 2023). The company has outlined development targets that include reaching 4,000 qubits by 2025, as illustrated in Figure 2. Google has also announced substantial development goals, including plans to develop a million-qubit system with error correction by 2029 (Krause, 2023). These industry developments indicate the continuing advancement of quantum computing capabilities.



Source: IBM

Figure 2. IBM's Quantum Computing Evolution

Furthermore, Quantum error correction (QEC) addresses a fundamental challenge in quantum computing: the susceptibility of quantum systems to noise and decoherence. As quantum processors scale up, maintaining qubit stability becomes increasingly critical for reliable computation. For instance, Riverlane's quantum error correction roadmap through 2026, shown in Figure 3, illustrates key milestones toward fault-tolerant quantum computing (GQI, 2024). This development highlights that advancing quantum computing requires both increasing qubit count and improving error correction capabilities.

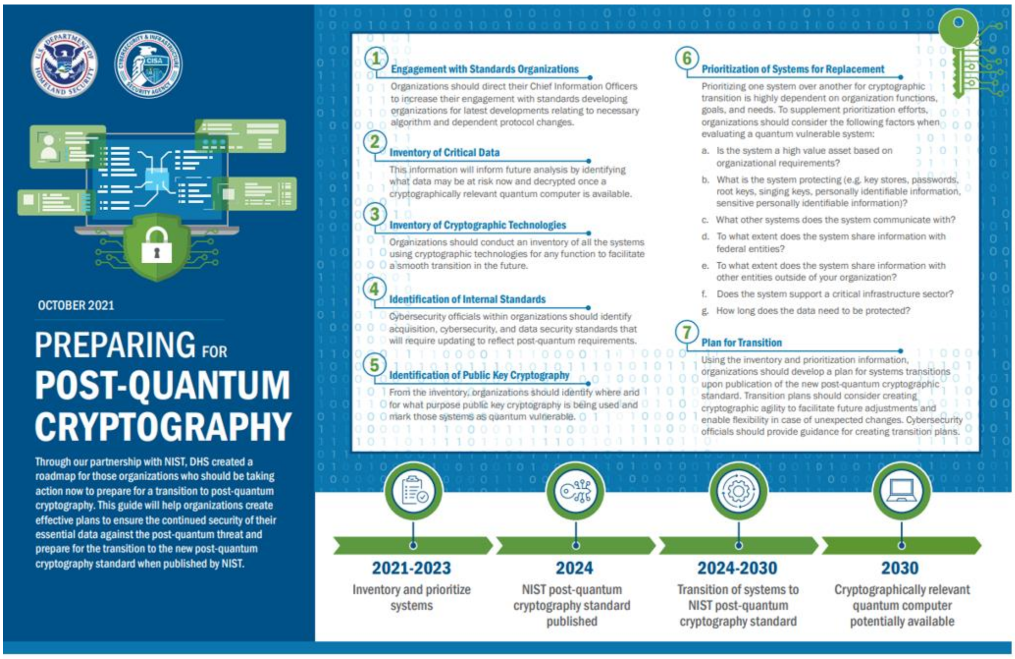


| | 2023<br>Deltaflow 1 ✓ | 2024<br>Deltaflow 2 | 2025<br>Deltaflow 3 | 2026<br>Deltaflow Mega |
|---|---|---|---|---|
| QuOps | 1,000 | 10,000 | 100,000 | 1,000,000 |
| Functionality | **Fast decoding**<br>Solving the backlog problem | **Streaming high-fidelity memory**<br>Keeping the qubits alive forever | **Streaming logic**<br>Enabling perpetual operations | **Logic at scale**<br>First fully error-corrected quantum applications |
| Product Features | **Stability & memory**<br>- First MHz decoder<br>- Automated data flow<br>- Bespoke interfacing | **Quantum memory**<br>- Streaming real-time decoding<br>- Leakage aware decoding<br>- First universal interfacing | **Quantum gates**<br>- Fast logic by lattice surgery<br>- Fast logic by transversal gates<br>- Higher error suppression rates<br>- First logical orchestration | **Universal gate set**<br>- Universal surface-code computation<br>- Dynamic large-scale orchestration<br>- Low-overhead real-time decoding supporting qLDPC codes |

Source: Riverlane

Figure 3. Riverlane's Quantum Error Correction Roadmap

To prepare organizations for quantum computing advances, the Cybersecurity and Infrastructure Security Agency (CISA), in collaboration with the National Security Agency (NSA) and Department of Homeland Security (DHS), has developed a transition roadmap for post-quantum cryptography (PQC), shown in Figure 4. CISA's assessment indicates potential Cryptanalytically Relevant Quantum Computing (CRQC) capabilities by 2030 (DHS, 2021), while some industry and academic researchers suggest an earlier timeline (Vezic, 2023). This assessment considers ongoing quantum research investments, hardware developments, and the role of artificial intelligence in quantum algorithm optimization (Biamonte et al., 2017).



OCTOBER 2021

PREPARING FOR POST-QUANTUM CRYPTOGRAPHY

Through our partnership with NIST, DHS created a roadmap for those organizations who should be taking action now to prepare for a transition to post-quantum cryptography. This guide will help organizations create effective plans to ensure the continued security of their essential data against the post-quantum threat and prepare for the transition to the new post-quantum cryptography standard when published by NIST.

1 Engagement with Standards Organizations

Organizations should direct their Chief Information Officers to increase their engagement with standards developing organizations for latest developments relating to necessary algorithm and dependent protocol changes.

2 Inventory of Critical Data

This information will inform future analysis by identifying what data may be at risk now and decrypted once a cryptographically relevant quantum computer is available.

3 Inventory of Cryptographic Technologies

Organizations should conduct an inventory of all the systems using cryptographic technologies for any function to facilitate a smooth transition in the future.

4 Identification of Internal Standards

Cybersecurity officials within organizations should identify acquisition, cybersecurity, and data security standards that will require updating to reflect post-quantum requirements.

5 Identification of Public Key Cryptography

From the inventory, organizations should identify where and for what purpose public key cryptography is being used and mark those systems as quantum vulnerable.

6 Prioritization of Systems for Replacement

Prioritizing one system over another for cryptographic transition is highly dependent on organization functions, goals, and needs. To supplement prioritization efforts, organizations should consider the following factors when evaluating a quantum vulnerable system:

a. Is the system a high value asset based on organizational requirements?
b. What is the system protecting (e.g. key stores, passwords, root keys, singing keys, personally identifiable information, sensitive personally identifiable information)?
c. What other systems does the system communicate with?
d. To what extent does the system share information with federal entities?
e. To what extent does the system share information with other entities outside of your organization?
f. Does the system support a critical infrastructure sector?
g. How long does the data need to be protected?

7 Plan for Transition

Using the inventory and prioritization information, organizations should develop a plan for systems transitions upon publication of the new post-quantum cryptographic standard. Transition plans should consider creating cryptographic agility to facilitate future adjustments and enable flexibility in case of unexpected changes. Cybersecurity officials should provide guidance for creating transition plans.

2021-2023
Inventory and prioritize systems

2024
NIST post-quantum cryptography standard published

2024-2030
Transition of systems to NIST post-quantum cryptography standard

2030
Cryptographically relevant quantum computer potentially available

Source: DHS

Figure 4. CISA's PQC Transition Roadmap

## C. Quantum AI Fusion

The integration of artificial intelligence with quantum computing is accelerating quantum technology development (Dunjko & Briegel, 2018). Machine learning and deep learning techniques are being applied to address key challenges in quantum system scaling, including noise reduction and error correction (Preskill, 2018). AI methods are enhancing the design of quantum circuits and algorithms, potentially advancing progress toward Cryptanalytically Relevant Quantum Computing (CRQC) capabilities (Dunjko & Briegel, 2018).This technical convergence has implications for multiple fields, including cryptography, materials science, and complex systems simulation. Beyond hardware and algorithm optimization, AI applications are improving quantum simulation precision, enabling more accurate modeling of quantum system behavior. Given these developments in AI-enhanced quantum computing and evolving CRQC timelines (Vezic, 2023), organizations should evaluate their quantum readiness and develop appropriate preparation strategies.

## D. Harvest Now, Decrypt Later: The Silent Compromise

One of the most insidious aspects of the quantum threat is the "harvest now, decrypt later" attack vector. In this scenario, adversaries capture, and store encrypted data transmitted today, which they decrypt once CRQC becomes available (Mosca & Piani, 2019). This silent compromise of encrypted data poses a long-term risk to the confidentiality of sensitive information, as data considered secure today may be vulnerable to quantum attacks in the future. Organizations handling sensitive data with enduring value face specific challenges from the 'harvest now, decrypt later' strategy. Current encrypted data—including intellectual property, trade secrets, and classified information—requires protection against future quantum decryption capabilities. This security consideration underscores the importance of transitioning to post-quantum cryptography (PQC) as part of a comprehensive data protection strategy.

As organizations anticipate the standardization of post-quantum cryptography (PQC) and strategize their transition plans, they can adopt various mitigation strategies to lessen the impact of the 'harvest now, decrypt later' threat in the meantime. These strategies include integrating quantum random number generators (QRNGs) to enhance key unpredictability in existing cryptographic systems (Herrero-Collantes & Garcia-Escartin, 2017), adopting a Zero Trust Architecture (ZTA) (Rose, Borchert, Mitchell, & Connelly, 2020), exploring hybrid encryption schemes that merge classical and quantum-resistant algorithms, and implementing techniques like ephemeral key exchanges and forward secrecy to protect past communications even if future keys are compromised. While not inherently quantum-proof, these mechanisms contribute to a framework that can mitigate some risks associated with quantum attacks, particularly those targeting the decryption of previously intercepted communications.

### *E. The Geopolitical Race for Quantum Supremacy*

History has demonstrated that breakthroughs in cryptography can arise unexpectedly, often propelled by the genius of individuals or the concerted efforts of well-resourced nation-states. For instance, during World War II, Alan Turing and his team at Bletchley Park managed to decipher the German Enigma code, once deemed impregnable (Copeland, 2012). This significant achievement gave the Allied forces a vital intelligence edge, crucially influencing the war's outcome (Copeland, 2012). Similarly, the invention of public-key cryptography by British mathematician Clifford Cocks in 1973, though initially kept secret until 1997, revolutionized cryptographic practices and established the groundwork for secure digital communications (ETHW, n.d.). This instance illustrates how nation-states can achieve substantial cryptographic advances in secrecy. The possibility that a nation-state could covertly achieve a significant milestone in quantum computing, explicitly achieving Cryptographically Relevant Quantum Computing (CRQC) before the global community is ready, must be seriously considered (Singh, 1999). This underscores the urgent need for global readiness and collaboration in the face of such potential advancements, to ensure that no single entity gains an unfair advantage (Biercuk & Fontaine, 2017).

### *F. The Time Challenge: Prolonged Shifts in Cryptographic Standards*

The history of cryptography demonstrates that transitioning from one cryptographic standard to another is a complex and challenging process, often fraught with difficulties and delays. For example, the transition from DES to AES encryption spanned over a decade, a period marked by numerous obstacles. Although the AES standard was officially adopted in 2001, DES continued to be used widely until it was officially deprecated by NIST in 2005 (Chown, 2002). Similarly, the transition from SHA-1 to SHA-2 hash functions began in earnest in 2011 and remains ongoing in some applications despite SHA-1 being officially deprecated by NIST in 2015 (Barker & Roginsky, 2019). Another prolonged transition is from RSA to ECC for public-key cryptography, which has been ongoing for over two decades, a testament to the enduring complexity of the process. Despite ECC's advantages in security and efficiency, its adoption has been gradual, with various applications slowly integrating ECC over time (Fischlin & Schnorr, 2000; Gueron & Krasnov, 2015). These examples underscore the significant time and effort required to move from one cryptographic system to another, often spanning several years or decades, and validate the complexity of the transition process.

The protracted transition periods between cryptographic standards can be attributed to several factors, including the need for backward compatibility, the cost and complexity of upgrading infrastructure, and the absence of immediate incentives for organizations to prioritize security upgrades (NIST, 2016). Furthermore, developing and standardizing novel cryptographic algorithms is a time-intensive process that necessitates extensive testing, validation, and consensus-building among stakeholders (Smid & Branstad, 1988). These challenges are expected to be exacerbated during the transition to Post-Quantum Cryptography (PQC), given the inherent complexity of quantum-resistant algorithms and the requirement to ensure their interoperability with existing systems.

### *G. Regulatory Landscape and Compliance*

As post-quantum cryptography (PQC) development progresses, governments and regulatory bodies worldwide are beginning to establish frameworks and guidelines for its adoption in critical infrastructure and sensitive sectors (Alagic et al., 2022). The National Institute of Standards and Technology (NIST) has been at the forefront of efforts to standardize quantum-resistant cryptographic algorithms in the United States. This initiative, launched in 2016, aims to finalize a set of recommended quantum-resistant algorithms by 2024, providing a clear roadmap for organizations to transition to PQC (Alagic et al., 2022; Moody et al., 2022). Once these standards are established, they are likely to precipitate a wave of regulatory requirements compelling businesses and government entities to adopt these algorithms within a specified timeframe. Failure to comply could lead to penalties, including fines, loss of contracts, and reputational damage (Fernandez-Vazquez et al., (2022). Furthermore, compliance with PQC standards will become critical for adhering to data protection regulations, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), which may be updated to reflect the new security challenges posed by quantum computing (Buchmann et al., (2022).Effective preparation for quantum computing advances requires organizations to monitor both technical developments and evolving cryptographic standards. Implementation of post-quantum cryptography (PQC) aligned with industry standards helps ensure regulatory compliance while preserving data security. This strategic approach enables organizations to address quantum computing challenges through systematic preparation and risk management.

The success of transitioning to post-quantum cryptography hinges on organizations' ability to navigate these complex challenges, adapt to the rapidly changing quantum landscape, and leverage the transformative potential of quantum technologies while ensuring the security and trust that are fundamental to our digital world. The Figure

5 below illustrates the PQC Transition Ladder, a structured framework designed to guide organizations in upgrading their cryptographic systems to be secure against quantum computing threats. The process begins with the PQC Transition Plan, where the scope is defined, business risks are assessed, and executive commitment is secured. This is followed by Cryptography Discovery, where existing cryptographic implementations are evaluated for readiness and locations of key cryptographic elements are identified. The third step involves assessing Secure Communication Protocols to pinpoint vulnerabilities in current cryptographic algorithms. The fourth step, Vendor PQC Readiness, focuses on evaluating vendor capabilities and establishing collaborations for PQC support. In the fifth step, Data Criticality & Secret Shelf-Life, data types and their security lifespans are analyzed to prioritize migration efforts. The final step involves the PQC Key Selection and Deployment, where standardized quantum-resistant keys are chosen, tested and implemented based on standardized criteria, followed by ongoing monitoring to assess performance and new security threats. This comprehensive approach ensures a systematic transition to quantum-resistant cryptography, addressing critical security, operational, and strategic factors and will be discussed in detail in the subsequent section.

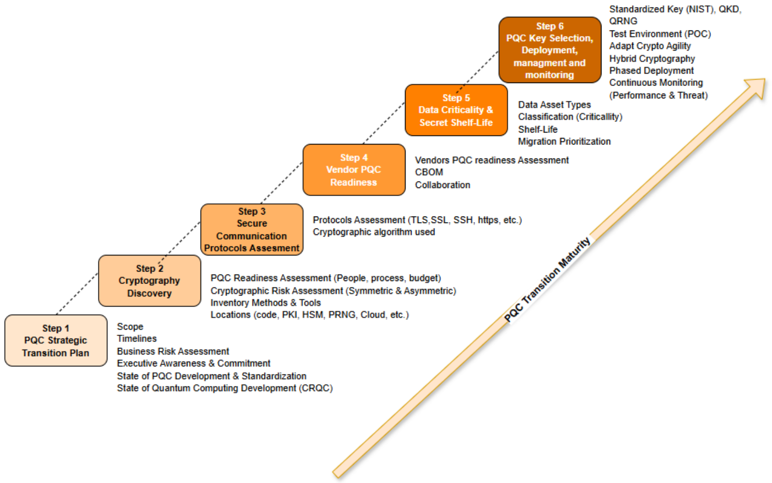

Step 6
PQC Key Selection, Deployment, managment and monitoring
Standardized Key (NIST), QKD, QRNG
Test Environment (POC)
Adapt Crypto Agility
Hybrid Cryptography
Phased Deployment
Continuous Monitoring (Performance & Threat)
Step 5
Data Criticality & Secret Shelf-Life
Data Asset Types
Classification (Criticallity)
Shelf-Life
Migration Prioritization
Step 4
Vendor PQC Readiness
Vendors PQC readiness Assessment
CBOM
Collaboration
Step 3
Secure Communication Protocols Assesment
Protocols Assessment (TLS,SSL, SSH, https, etc.)
Cryptographic algorithm used
Step 2
Cryptography Discovery
PQC Readiness Assessment (People, process, budget)
Cryptographic Risk Assessment (Symmetric & Asymmetric)
Inventory Methods & Tools
Locations (code, PKI, HSM, PRNG, Cloud, etc.)
Step 1
PQC Strategic Transition Plan
Scope
Timelines
Business Risk Assessment
Executive Awareness & Commitment
State of PQC Development & Standardization
State of Quantum Computing Development (CRQC)
PQC Transition Maturity

Figure 5. PQC Transition Framework

## I. Critical Executive Support for PQC Transition

Executive support is fundamental to successful post-quantum cryptography (PQC) implementation, as it requires strategic resource allocation and organizational alignment. Leadership must understand both the technical implications and business risks, including potential impacts on data security, operational continuity, and regulatory compliance. This understanding enables informed decisions about investment timing and resource allocation.Executive endorsement of PQC transition ensures proper prioritization, resource availability, and organizational focus. It facilitates necessary changes in security infrastructure and practices while maintaining business operations. Leadership commitment also helps align PQC implementation with broader organizational strategy and risk management objectives.Effective executive support encompasses allocating appropriate resources and budget, establishing clear implementation priorities, and ensuring cross-departmental coordination.

It includes supporting necessary technical and operational changes while maintaining focus on long-term security objectives. Without active leadership engagement, PQC implementation may face resource constraints and coordination challenges, potentially leading to delayed adoption and increased organizational risk

### A. CRQC Business Risk Calculations

Effective risk assessment for Cryptanalytically Relevant Quantum Computing (CRQC) requires systematic quantification of potential business impacts to justify post-quantum cryptography investment. This analysis should evaluate data asset value, potential breach costs, and projected quantum computing timelines.Financial impact assessment includes measuring potential losses from intellectual property compromise, operational disruptions, and regulatory compliance issues. Risk modeling techniques, such as Monte Carlo simulations and scenario analysis, help organizations estimate the financial implications of quantum threats. The 'harvest now, decrypt later' threat model adds urgency to these calculations by highlighting current vulnerability to future quantum capabilities.A comprehensive risk framework incorporating financial metrics, operational factors, and compliance requirements provides executives with concrete data for investment decisions. This analysis compares post-quantum cryptography implementation costs against potential losses from delayed action, enabling informed strategic planning and resource allocation.

## II. Cryptography Discovery and Risk Assessment

The initial phase of Post-Quantum Cryptography (PQC) migration requires thorough analysis of existing cryptographic deployments. This process includes documenting current algorithms, assessing quantum computing vulnerabilities, and creating detailed implementation maps across organizational networks. Tables 2-5 outline the systematic assessment methodology and provide a comprehensive inventory of cryptographic protocol locations.

Table 2. Classic Cryptography and CRQC Impact

| Classical Cryptography | Algorithm/Scheme | Impacted by Shor's Algorithm | Impacted by Grover's Algorithm | Impact Level |
|---|---|---|---|---|
| **Symmetric Encryption** | AES | No | Yes (reduces key size) | Medium |
| | DES | No | Yes (reduces key size) | High |
| | 3DES | No | Yes (reduces key size) | Medium |
| **Asymmetric Encryption** | RSA | Yes | No | Critical |
| | ECC | Yes | No | Critical |
| | Diffie-Hellman | Yes | No | Critical |
| **Hash Functions** | SHA-2 | No | Yes (reduces collision resistance) | Low |
| | SHA-3 | No | Yes (reduces collision resistance) | Low |
| **Digital Signatures** | RSA | Yes | No | Critical |
| | ECDSA | Yes | No | Critical |
| | DSA | Yes | No | Critical |

Table 2 presents a systematic analysis of classical cryptography algorithms' vulnerability to Cryptanalytically Relevant Quantum Computing (CRQC). The analysis categorizes cryptographic schemes based on their susceptibility to quantum algorithms, specifically examining the implications of Shor's and Grover's algorithms on current cryptographic security.

### Symmetric Encryption Methods

The table examines popular symmetric encryption algorithms such as AES, DES, and 3DES. It illustrates how Grover's algorithm could potentially reduce the effective key strength of these ciphers, necessitating larger key sizes to maintain equivalent security levels in a post-quantum world.

### Asymmetric Encryption Methods

For asymmetric or public-key cryptography, the table highlights the severe vulnerabilities of widely used algorithms like RSA, DSA, and elliptic curve cryptography (ECC) to Shor's algorithm. These systems, which form the backbone of secure internet communications, could be completely broken by sufficiently powerful quantum computers.

### Hash Functions

The impact on cryptographic hash functions like SHA-2 and SHA-3 is also addressed. While these are generally considered more resistant to quantum attacks, the table shows how Grover's algorithm could potentially weaken their collision resistance, affecting their use in digital signatures and other security protocols.

### Digital Signatures

The table examines various digital signature schemes, including those based on RSA and elliptic curves, showing their high vulnerability to quantum attacks. This is particularly concerning given the critical role of digital signatures in ensuring the authenticity and integrity of digital communications and transactions.

This differentiation is essential as it underscores the varying degrees of security risks associated with different cryptographic schemes with emerging quantum technologies. The details provided can serve as a baseline for prioritizing the transition to quantum-resistant cryptography. Organizations can use this information to strategically plan their upgrades, focusing first on the most critically impacted areas to maintain data security against potential quantum threats.

Table 3 presents a systematic framework for cryptographic asset inventory, essential for organizations planning Post-Quantum Cryptography (PQC) implementation. This framework incorporates network traffic analysis, deep packet inspection, and vulnerability scanning to map existing cryptographic deployments.

Table 3. Cryptography Inventory Tools & Methods

| Method | Description |
|---|---|
| **Network Traffic Analysis** | Monitor and analyze network traffic for encryption patterns and encrypted data transfers. |
| **Protocol Analysis** | Identify and review the cryptographic protocols used across the network, such as SSL/TLS. |
| **Endpoint Security Solutions** | Utilize endpoint security systems that can detect and report on cryptographic processes. |
| **Firewall Logs** | Review firewall logs for indications of encrypted traffic and rule triggers related to cryptography. |
| **Intrusion Detection Systems** | Deploy IDS tools to flag anomalies in network traffic that could indicate cryptographic activities. |
| **Network Scanners** | Use network scanning tools to identify devices and services that employ encryption techniques. |
| **Configuration Audits** | Conduct audits of network device configurations to find enabled encryption settings. |
| **Penetration Testing** | Perform penetration tests to discover cryptographic vulnerabilities and misconfigurations. |
| **Software Inventory Tools** | Implement software inventory management tools to detect cryptographic libraries and tools. |
| **Deep Packet Inspection** | Inspect and manage network data packets to identify encrypted traffic and encryption types. |
| **Digital Forensic Tools** | Use forensic tools to analyze data remnants that indicate cryptographic operations. |
| **Compliance Scanning** | Conduct scans to ensure cryptographic standards compliance as per industry regulations. |
| **Third-Party Security Services** | Engage cybersecurity firms for specialized scanning and monitoring of cryptographic activities. |
| **Machine Learning Models** | Use AI to detect patterns and anomalies in cryptographic use beyond traditional methods. |
| **Vulnerability Scanning** | Scan for vulnerabilities in the network that might expose or compromise cryptographic functions. |
| **SIEM Analysis** | Utilize Security Information and Event Management systems to analyze and manage security events related to cryptography. |

The inventory process combines automated and manual discovery methods. Automated tools efficiently identify cryptographic patterns across network systems and applications, while manual code reviews and audits uncover cryptographic implementations that may elude automated detection. Cryptographic asset inventory requires continuous monitoring and regular reassessment as systems evolve. This ongoing evaluation helps maintain current documentation of organizational cryptographic implementations and supports effective PQC transition planning. The comprehensive discovery process enables organizations to assess risk exposure, determine implementation priorities, and develop targeted migration strategies.

Table 4 provides a structured mapping of cryptographic implementation locations across organizational systems, essential for Post-Quantum Cryptography (PQC) transition planning.

Table 4. Cryptography Inventory Locations

| Category | Locations to Inventory Cryptographic Usage |
|---|---|
| **Code-Based Assets** | Application Source Code: Cryptographic libraries, custom encryption implementations<br>Database Encryption: Encryption at rest, key management<br>APIs: Cryptographic functions in source code and documentation |
| **Network Assets** | TLS Implementations: Across web, mail servers, etc.<br>Network Appliances: Firewalls, load balancers, intrusion systems<br>VPN Configurations: Encryption, authentication methods<br>Wireless Networks: Encryption methods in Wi-Fi protocols |
| **Hardware** | HSMs: Management and storage of cryptographic keys<br>Embedded Systems/IoT Devices: Cryptographic implementations<br>Data Storage Devices: Self-encrypting drives and encryption methods |
| **Third-Party and Cloud Services** | Cloud Service Providers: Data encryption in transit and at rest<br>SaaS Applications: Encryption methods for data protection<br>Third-Party Vendors: Cryptographic standards and compliance |
| **Public Key Infrastructure (PKI)** | Certificate Authorities: Inventory of digital certificates<br>SSL/TLS Certificates: Encryption and hashing algorithms<br>Key Management Systems: Management of cryptographic keys |
| **Administrative and Management Interfaces** | Configuration Management Tools: Cryptographic settings<br>Access Control Systems: Encryption and hashing for authentication |
| **Development and Testing Environments** | Development Tools: Use of cryptography in software development<br>Testing Scripts and Tools: Use of cryptography in testing environments |
| **Backup Systems** | Backup Solutions: Encryption in backup software and hardware<br>Disaster Recovery Plans: Cryptographic measures and updates |
| **Mobile and Remote Environments** | Mobile Apps: Encryption within apps accessing corporate data<br>Remote Desktop Protocols: Cryptographic protocols for remote access |
| **Legacy Systems** | Older Hardware and Software: Review of cryptographic standards<br>Historic Data: Security of encrypted archived data |
| **Documentation and Configuration Management** | Security Policies: Reflection of current cryptographic standards<br>Configuration Files: Management of cryptographic settings in files and templates |
| **Supply Chain Interdependencies** | Embedded Cryptography: Third-party products with integrated cryptography<br>Service Providers: Cryptographic practices of infrastructure and managed services providers |
| **Specialized Use Cases** | Blockchain Technologies: Cryptographic algorithms in use<br>Industry-Specific Devices: Cryptography in sector-specific tools and devices<br>Research and Development: Projects exploring new cryptographic technologies |
| **Audit and Compliance Tools** | Audit Logs and Monitoring Tools: Cryptography used in security monitoring tools |

The mapping encompasses application source code, APIs, network configurations, hardware components, and cloud services. This framework includes mobile platforms, remote access systems, and legacy infrastructure to capture the full scope of cryptographic deployments. This systematic inventory supports comprehensive assessment of current cryptographic implementations and guides quantum-resistant upgrade planning. While the mapping addresses common deployment scenarios from backend systems to user interfaces, organizations may identify additional locations based on specific operational requirements or industry needs. This detailed documentation enables thorough evaluation of quantum computing vulnerabilities throughout the infrastructure.

## III. Secure Communication Protocols

Analysis of secure communication protocols is fundamental to quantum computing vulnerability assessment. Core protocols such as SSL/TLS, SSH, IPsec, and WireGuard implement cryptographic algorithms for network security. Understanding their cryptographic foundations guides the development of quantum-resistant protocol adaptations to maintain secure data transmission.

Table 5. Secure Communication Protocols

| Sector | Protocol | Cryptographic Algorithms Used | Usage |
|---|---|---|---|
| General IT | HTTPS, SSL/TLS, DNSSEC | RSA, ECC, AES, 3DES, SHA-256, SHA-1 | Secure web transactions and information exchange |
| | SSH, SFTP | RSA, ECC, AES, 3DES, ED25519 | Secure shell and file transfer |
| Network Security | SNMPv3 | HMAC-MD5, HMAC-SHA, AES, 3DES | Secure network management |
| | RPKI | RSA, ECC | Secure BGP routing information |
| Financial Services | ISO 20022, FIX, SWIFT | SSL/TLS for transport security, Varies by implementation | Secure financial data transmissions |
| Healthcare | DICOM, HL7 | AES, RSA (DICOM); SSL/TLS (HL7) | Secure health information and medical imaging data |
| Energy Sector | IEC 62351, DNP3 SA, SCADA | RSA, AES (IEC 62351); AES-CBC, SHA-256 (DNP3 SA) | Secure energy management and data acquisition |
| Defense | HAIPE | AES, Suite B Cryptographic algorithms | Secure government and military communications |
| Communication & IT | Kerberos | DES, RC4, AES | Secure network authentication |
| | RADIUS, TACACS+, PGP | MD5, SHA-1, TLS enhancements (RADIUS); MD5, TLS (TACACS+) | Authentication, Authorization, and Accounting (AAA) |
| Cable | DOCSIS | AES, BPI+ | Secure cable communications |
| Wireless Networks | WPA2/WPA3 | AES, HMAC-SHA256, ECC (WPA3 key exchange) | Secure Wi-Fi communication |
| VPN Technologies | IPsec, OpenVPN, WireGuard | AES, HMAC-SHA256, ECC, ChaCha20, Poly1305 | Secure virtual private networks |
| Other Protocols | CoAP over DTLS, MQTT over SSL/TLS | DTLS (RSA, ECC, AES); SSL/TLS as above | Secure device-to-device and IoT communications |

| | | | |
|---|---|---|---|
| Remote Access | L2TP/IPsec | RSA, ECC, AES, 3DES | Secure remote network access |
| Emerging Technologies | ZTNA, ZeroMQ | SSL/TLS, ECC, AES; Curve25519, Salsa20, Poly1305 | Secure messaging and data flows |
| 4G/5G/6G | LTE, NR, Next G | AES, Snow 3G, ZUC (4G); AES, 5G AKA, PKI enhancements (5G); Potential post-quantum algorithms (6G) | Secure mobile communications |
| SIM/eSIM | ISIM, eSIM | AES, RSA, ECC | Secure storage and communication of subscriber identities |
| Internet Key Exchange | IKEv1, IKEv2 | RSA, ECC, AES, SHA-256 | Secure IPsec VPN connections |

Table 5 presents key secure communication protocols deployed across critical infrastructure sectors, including their core cryptographic implementations. While this framework provides baseline guidance, organizations should conduct detailed protocol assessments specific to their operational requirements.

The transition to Post-Quantum Cryptography (PQC) in critical infrastructure requires systematic planning that balances security needs with operational continuity. This includes risk-based prioritization of systems and data, followed by phased implementation to ensure effective migration while maintaining essential operations.

## IV. Data Criticality and Secret Shelf-Life

The shift to Post-Quantum Cryptography (PQC) in critical infrastructure demands a meticulous strategy centered around data. This includes conducting a comprehensive evaluation of data based on their significance and identifying their ‘secret lifespan’ – the duration for which the data's confidentiality is paramount. Such classification enables organizations to prioritize data sets that need immediate security enhancements and synchronize their cryptographic updates to safeguard sensitive information from potential quantum threats. This systematic approach ensures a strategic and efficient transition to PQC.

### *A. Catalogue Data Types*

Develop a comprehensive data inventory by collaborating with department leaders and IT teams to identify all organizational data types. This includes business-critical information such as employee records, customer data, financial information, health records, intellectual property, and operational data. This systematic cataloging enables effective assessment of data security requirements and risk levels.

### *B. Establish Data Classfication Framework*

Implement structured data classification policies as a foundation for Post-Quantum Cryptography (PQC) transition. Define classification tiers according to data sensitivity and business risk: Public (unrestricted information), Internal Use Only (organization-specific), Confidential (protected business data), and Restricted (highest sensitivity). Coordinate with data owners to ensure precise classification alignment with organizational security requirements (Ticong, 2024).

### *C. Evaluate Data Criticality*

Evaluate data assets based on business value, regulatory obligations, and quantum computing vulnerability. This assessment guides protection priorities and Post-Quantum Cryptography (PQC) implementation sequence. Understanding the criticality and risk exposure of different data types enables strategic security planning and efficient resource allocation for quantum-resistant upgrades.

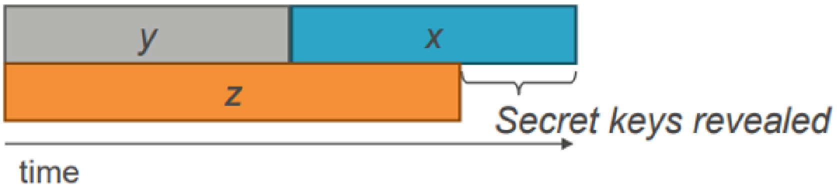
### *D. Determine Data Secret Shelf-Life*

Data prioritization for Post-Quantum Cryptography (PQC) transition requires analysis of confidentiality requirements and data longevity. Evaluate each data type's business significance, regulatory obligations, and required protection duration to determine quantum vulnerability risk. Prioritize data with extended confidentiality requirements and high business impact, such as regulated financial records and personal identifiable information (PII) under GDPR or HIPAA, for early PQC implementation.

### *E. Prioritize Based on Quantum Risk and Business Impact*

Post-Quantum Cryptography (PQC) migration sequencing requires systematic evaluation of data criticality and vulnerability. Assessment factors include confidentiality requirements, data integrity needs, and operational impact, along with potential breach consequences. This analysis enables resource allocation based on data value and protection requirements.Strategic prioritization ensures high-risk data receives early protection while enabling controlled migration that maintains operational continuity. Integration of Mosca's theorem provides additional risk assessment framework, considering quantum computing development timelines against data protection requirements and value duration (Mosca, 2015)

**Theorem 1: If x + y > z, then worry**



Source: IQC

Figure 6. Mosca’s Inequality Theorem

Where:

**X**=Security shelf life

**Y**=Migration time

**Z**=CRQC arrival time

Per Michele Mosca's Theorem (X+Y)>Z depicted in Figure 6, if the duration for which data needs to stay secure (X) combined with the time required to upgrade cryptographic systems (Y) exceeds the point when powerful quantum computers capable of breaking cryptography (CRQC) become available (Z), organization is already behind schedule to migrate to PQC (Mosca, 2015).

## V. Vendor PQC Readiness Assessment

Creating a Cryptographic Bill of Materials (CBOM) and evaluating vendor Post-Quantum Cryptography (PQC) readiness enables systematic security transition planning. This documentation and assessment process ensures aligned implementation of quantum-resistant measures throughout the supply chain ecosystem.

### *A. Identifying Key Vendors and Evaluate their PQC Readiness*

Post-Quantum Cryptography (PQC) preparation requires structured evaluation of vendor ecosystems. Develop prioritized vendor assessment based on operational criticality, data sensitivity, system integration levels, and security implications. Engage key vendors to evaluate their PQC implementation readiness, including transition planning, standards compliance, and solution delivery capabilities.Assessment should address vendors' quantum threat awareness, implementation timelines, research initiatives, and interoperability considerations. This systematic evaluation identifies supply chain vulnerabilities, aligns internal PQC strategies, and guides partnership decisions. Understanding vendor capabilities and limitations enables organizations to develop comprehensive quantum-resistant security frameworks.

### *B. Developing a Cryptographic Bill of Materials (CBOM)*

A comprehensive Cryptographic Bill of Materials (CBOM) documents all cryptographic implementations, including algorithms, libraries, and tools across organizational systems. This inventory, developed through technical assessment and vendor engagement, catalogs cryptographic components with detailed implementation specifications and security parameters.Analysis of the CBOM identifies quantum vulnerability levels and critical upgrade requirements. The assessment supports migration planning by evaluating replacement options, implementation timelines, and risk mitigation strategies. This systematic approach ensures alignment with post-quantum standards while maintaining operational continuity through testing and monitoring protocols.

### *C. Collaborating with Vendors on PQC Migration*

Work closely with vendors to develop a well-coordinated plan for transitioning to Post-Quantum Cryptography (PQC). Establish transparent and efficient communication channels to assess progress regularly, ensuring that issues are promptly addressed, and the migration stays on track. This ongoing dialogue will enable both parties to allocate resources effectively and provide the support needed to navigate the complexities of adopting quantum-resistant security solutions. Consider both performance benchmarks and timelines in these discussions to facilitate a seamless and timely transition, minimizing disruptions to operational workflows while enhancing security measures against quantum threats.

## VI. PQC Selection and Deployment

The National Institute of Standards and Technology (NIST) has led the development of Post-Quantum Cryptography (PQC) standards since 2016. This program evaluates cryptographic algorithms for quantum computing resistance and practical implementation requirements (NIST, 2016).NIST's selection process engages the global cryptographic community to identify algorithms resistant to both classical and quantum attacks. The evaluation examines security strength, performance metrics, and implementation efficiency across different applications. Through multiple review phases, NIST continues to refine candidate algorithms based on technical analysis and industry feedback (Moody, 2024).In July 2022, NIST selected four algorithms for Post-Quantum Cryptography (PQC) standardization, as detailed in Table 6. The selection includes CRYSTALS-KYBER for key encapsulation mechanism (KEM) and three digital signature algorithms: CRYSTALS-Dilithium, FALCON, and SPHINCS+ (Moody et al., 2022). Three of these algorithms—CRYSTALS-KYBER, CRYSTALS-Dilithium, and FALCON—are based on structured lattice problems, while SPHINCS+ uses hash-based cryptography.The structured lattice algorithms offer efficient performance and smaller key sizes, making them suitable for widespread deployment (Alagic et al., 2023). SPHINCS+, while having larger signatures and slower performance, provides an important alternative based on well-understood hash functions (Bernstein et al., 2022).

Table 6: NIST Selected PQC

| Algorithm Name | Primary Function | Cryptographic Basis | Key Benefits |
|---|---|---|---|
| **CRYSTALS-KYBER** | Key Encapsulation Mechanism | Lattice-based | Small key size, fast operational speed, and strong security against quantum attacks |
| **CRYSTALS-Dilithium** | Digital Signature | Lattice-based | High efficiency and speed, NIST-recommended and versatile for various applications |
| **FALCON** | Digital Signature | Lattice-based | Compact signatures, efficient verification and strong quantum and classical security |
| **SPHINCS+** | Digital Signature | Hash-based | Stateless, flexible security levels and long-term security from hash-based approach |

Finally, on August 14, 2024, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) achieved a historic milestone by finalizing three Federal Information Processing Standards (FIPS) for post-quantum cryptography from the third round (NIST, 2024). These standards are designed to fortify modern public-key cryptography infrastructure against quantum computing threats:

FIPS 203 establishes ML-KEM (derived from CRYSTALS-Kyber) as the standard key encapsulation mechanism for general encryption purposes, such as securing website access. FIPS 204 introduces ML-DSA (derived from CRYSTALS-Dilithium) as the primary lattice-based algorithm for general-purpose digital signature protocols. FIPS 205 implements SLH-DSA (derived from SPHINCS+) as the standard stateless hash-based digital signature scheme (IBM, 2024). The publication of these standards represents a pivotal moment in cryptographic security, providing organizations with a clear framework to implement Post-Quantum Cryptography (PQC) technologies. While NIST had previously advocated for proactive preparation through infrastructure assessment and migration planning, these finalized standards now offer concrete implementation guidance. Looking ahead, NIST maintains its commitment to evolving these guidelines in parallel with quantum computing advancements, ensuring robust cryptographic security and compliance across all sectors.

Recognizing the importance of cryptographic diversity, NIST also continues to evaluate additional algorithms based on different mathematical approaches. This fourth round of evaluation focuses particularly on alternative key encapsulation mechanisms not based on lattice problems, including BIKE and HQC, which are structured code-based cryptography (CSRC, 2022). This effort to standardize algorithms with different mathematical foundations provides crucial backup options should vulnerabilities be discovered in lattice-based approaches.

### *A. PQC Key Selection*

Post-Quantum Cryptography (PQC) key selection requires evaluation of several technical parameters (Chen et al., 2023). Security level requirements should align with organizational risk assessment and data protection needs (Alagic et al., 2024). Implementation considerations include computational efficiency, key size requirements, and system resource utilization (NIST, 2024).Successful deployment depends on backward compatibility with existing infrastructure and established cryptographic protocols (Mosca & Perlner, 2023). Organizations should prioritize validated algorithms that meet standardization requirements while supporting operational needs (Alagic et al., 2024).

### *B. PQC Key Testing*

Once potential PQC algorithms are selected, comprehensive testing is necessary to evaluate their effectiveness in real-world scenarios. This includes assessing their resistance to various attack vectors, both classical and quantum. Performance benchmarks are crucial to understand the impact on system resources and operational latency. Additionally, key management and secure storage practices must be scrutinized to ensure the protection of cryptographic keys throughout their lifecycle. This phase may involve simulations and pilot projects to observe the algorithms' behavior under different network conditions and load scenarios. These steps are critical in verifying the practical viability and security robustness of the selected PQC algorithms.

### *C. PQC Key Deployment*

Implementing Post-Quantum Cryptography (PQC) requires a careful and staged approach, starting with less critical systems to minimize the risk of disruptions. Organizations may adopt hybrid key deployment strategies, using quantum-resistant keys alongside traditional cryptographic keys to maintain compatibility with legacy systems. This approach ensures that organizations can benefit from the enhanced security of PQC while keeping all network components operational and accessible during the transition. It is essential to integrate these keys seamlessly into the current security framework and align them with existing IT and security procedures.

### D. *Ongoing PQC Monitoring and Update*

Post-deployment, continuous monitoring is essential to evaluate the effectiveness of PQC solutions and detect emerging security vulnerabilities. This involves regular audits, updates, and potential recalibrations of cryptographic measures as new quantum computing breakthroughs occur. Crypto-agility becomes a significant asset, enabling organizations to swiftly adapt to new algorithms or updated versions of current ones without extensive overhauls. Regularly updating the cryptographic landscape in response to evolving quantum computing technologies and maintaining compliance with regulatory standards are vital for sustaining long-term security and trust.

### E. *The Role of Artificial Intelligence (AI) in Transitioning to PQC*

Artificial intelligence significantly advances Post-Quantum Cryptography (PQC) development through powerful analytical capabilities (Dunjko & Briegel, 2018). Machine learning algorithms enhance cryptographic analysis by optimizing algorithm performance and detecting potential vulnerabilities. This systematic approach helps create more efficient quantum-resistant implementations while maintaining rigorous security standards.In practical deployments, AI automates critical aspects of PQC integration, including key management and system compatibility analysis. For organizations with diverse technology infrastructures, AI tools streamline the migration to quantum-resistant protocols by automating key distribution, monitoring system performance, and identifying potential implementation challenges.

### F. *Collaboration and Partnership*

Cross-sector collaboration accelerates effective Post-Quantum Cryptography (PQC) adoption through coordinated implementation strategies (NIST, 2024). Industry partnerships, including participation in technical working groups and research initiatives, provide valuable insights for addressing common migration challenges.

Strategic engagement with technology providers ensures PQC solutions meet both current requirements and emerging standards. Vendor relationships support implementation planning by addressing compatibility needs and integration requirements. These partnerships help organizations develop comprehensive approaches to PQC deployment

## VII. Challenges

Transitioning to Post-Quantum Cryptography (PQC) is a complex endeavor encompassing technical, logistical, and human challenges. As the quantum computing horizon draws closer, organizations are urged to adopt cryptographic methods resistant to quantum attacks. This shift introduces various difficulties, from choosing suitable algorithms to integrating them into existing systems and training the workforce. Successfully navigating this transition is essential for securing sensitive data against future quantum threats, but doing so requires overcoming significant hurdles that can impact every aspect of an organization's operations.

### A. Algorithm Selection and Standardization

The selection and standardization of PQC algorithms present significant challenges for organizations transitioning to quantum-resistant security. With numerous candidate algorithms proposed by researchers and industry experts, each with its strengths and weaknesses, determining the best algorithms for specific use cases can be difficult. A universally accepted standard for PQC algorithms is necessary for informed decision-making. With a common framework for implementing and integrating PQC solutions, organizations may be able to ensure interoperability and compatibility across different systems and platforms. The lack of standardization can lead to market fragmentation, with different vendors and service providers offering proprietary PQC solutions that may not be easily integrated with one another.

Industry stakeholders must work together to develop and promote open standards for PQC algorithms and protocols. This includes collaboration with national and international standards bodies, such as NIST and ISO, to establish guidelines and best practices for PQC implementation. Adopting PQC standards will facilitate the development of interoperable and scalable security solutions, enabling organizations to transition to quantum-resistant security while minimizing the risk of vendor lock-in and incompatibility issues.

### B. Scalability and Performance Overhead

Implementing PQC algorithms introduces increased computational complexity and larger key sizes compared to traditional cryptographic methods, leading to significant performance overhead, especially for resource-constrained devices (McKay, Bassham, Turan, & Mouha, 2017). The heightened processing power and memory requirements of PQC algorithms may surpass the capabilities of many devices, impairing their ability to perform essential security functions. Additionally, managing and distributing larger cryptographic keys can strain network bandwidth and storage capacity.

To address these challenges, organizations must optimize PQC implementations through hardware acceleration and other performance-enhancing techniques. Although developing PQC algorithms tailored to specific devices is challenging, adopting standardized PQC solutions provided by NIST can help ensure broad compatibility and effectiveness. These standardized solutions aim to balance robust security with practical performance considerations, even if some performance compromises are necessary.

### C. Key Management Challenges

The transition to Post-Quantum Cryptography (PQC) brings new challenges in managing and distributing cryptographic keys. Due to the larger key sizes, many PQC algorithms require traditional key management systems, and protocols may become cumbersome and inefficient. Organizations are thus compelled to explore new key generation, storage, and exchange methods to handle the increased complexity and size of PQC keys. This could include adopting specialized hardware modules, such as hardware security modules (HSMs), which securely generate and store PQC keys. While the development of quantum-resistant key exchange protocols like Quantum Key Distribution (QKD) could enhance the security of distributing PQC keys across networks, it is essential to note that the National Security Agency (NSA) and National Institute of Standards and Technology (NIST) are not currently advocating the use of QKD (NSA, n.d.). Implementing such solutions demands significant investments in hardware, software, and personnel (Harishankar et al., 2024). Therefore, organizations must thoroughly assess their key management needs and devise strategies that effectively balance security, efficiency, and cost in their specific PQC deployment scenarios.

### *D. Crypto-Agility*

Achieving crypto-agility—the ability for systems to quickly adapt to new cryptographic standards is another challenge. Adopting crypto-agility is challenging because it requires companies to design their systems to be inherently flexible, capable of integrating new cryptographic standards quickly as they emerge. This flexibility must allow for updates without the need for extensive system overhauls, responding efficiently to new threats or improved cryptographic methods as they develop. Such a capability demands forward-thinking in design, significant investment in technology, and continuous staff training, all of which pose considerable operational and financial challenges (Harishankar et al., 2024).

### *E. Legacy System Integration (Interoperability and Compatibility)*

Transitioning to new cryptographic algorithms must be done in a way that maintains compatibility with existing systems and protocols. Many organizations rely on legacy systems and infrastructure that were not designed with PQC in mind. Integrating PQC algorithms and protocols into these systems can be a complex and time-consuming process, requiring significant modifications to existing hardware and software components. In some cases, legacy systems may not even be capable of supporting PQC at all, necessitating costly upgrades or replacements. This is particularly relevant for devices that rely on embedded systems or specialized hardware for cryptographic operations, like hardware security modules (HSMs) or network encryption devices. These devices might need hardware upgrades or replacements to handle the increased computational requirements of PQC algorithms, which can be more complex and demanding than current cryptographic standards. Even when integration is possible, the process of testing and validating PQC implementations can be resource-intensive, requiring extensive efforts to ensure the security and stability of the overall system. Organizations must carefully assess the feasibility and cost-effectiveness of integrating PQC into their legacy systems, weighing the benefits of enhanced security against the potential disruption to business operations. In some cases, a phased approach to PQC integration may be necessary, allowing organizations to gradually migrate their systems to quantum-resistant security while minimizing the risk of downtime and compatibility issues.

### *F. Workforce Training and Awareness*

The successful adoption of PQC requires a knowledgeable and skilled workforce to implement and manage quantum-resistant security solutions. However, many organizations may lack the necessary expertise and awareness to effectively transition to PQC. This can result in implementation challenges and potential security issues that undermine the effectiveness of PQC deployments. To address this challenge, organizations must invest in comprehensive training and awareness programs that educate employees on the basics of quantum computing, the potential impacts of quantum attacks, and the proper use and management of PQC solutions. This may involve developing specialized training curricula, hiring PQC experts to provide guidance and support, and establishing centers of excellence to foster knowledge sharing and collaboration. Prioritizing workforce education and awareness helps organizations ensure their employees possess the necessary skills and knowledge to effectively implement and maintain PQC solutions, thereby reducing the risk of security breaches and other negative outcomes.

### *G. Organizational Challenges*

Organizational challenges pose significant hurdles in the transition to post-quantum cryptography. One of the primary obstacles is the lack of awareness and understanding among decision-makers regarding the gravity of quantum threats and the urgent need for quantum-resistant security measures. This knowledge gap often leads to a scarcity of resources and funding allocated towards quantum security initiatives, as organizations prioritize other pressing matters. Moreover, the inherent resistance to change within organizations can hinder the adoption of new technologies, such as post-quantum cryptography, as employees may be hesitant to embrace unfamiliar systems and processes. Overcoming these organizational challenges requires a concerted effort to educate stakeholders, secure adequate funding, and foster a culture of adaptability and innovation.

### *H. Cost of Migration*

The transition to PQC can be a costly endeavor, requiring significant investment in hardware, software, and personnel. Organizations must carefully evaluate the financial implications of PQC adoption, considering factors such as the cost of upgrading or replacing legacy systems, the development and testing of PQC implementations, and the ongoing maintenance and support of quantum-resistant security solutions. In addition to direct costs, organizations must also consider the potential indirect costs of PQC migration, such as lost productivity due to system downtime, reduced efficiency due to increased computational overhead, and the opportunity cost of diverting resources away from other business priorities. To mitigate these costs, organizations must develop comprehensive migration strategies that prioritize the most critical systems and data, leverage existing investments where possible, and phase the implementation of PQC over time. The use of open-source PQC solutions and collaborative development models can also help to reduce costs and promote interoperability, enabling organizations to share the burden of PQC migration and benefit from the collective expertise of the broader security community. Ultimately, the cost of PQC migration must be weighed against the potential costs of a quantum attack, which could be devastating in terms of financial losses, reputational damage, and legal liabilities.

## VIII. Conclusion

The imminent arrival of quantum computing underscores the urgent need to safeguard critical infrastructure with Post-Quantum Cryptography (PQC). This qualitative research paper has delivered an in-depth examination of the strategies and methodologies essential for successfully transitioning to quantum-resistant cryptographic systems. By outlining the multidimensional challenges—from algorithm selection and standardization to integration and workforce training—this provides a solid framework for organizations navigating this complex terrain. The valuable insights presented here address immediate concerns and set the stage for future advancements in fortifying critical infrastructures against quantum threats.

By embracing a proactive and collaborative approach to the PQC transition, organizations can establish themselves as pioneers in the quantum-resistant security landscape. The insights and best practices showcased in this paper serve not only as theoretical guidance but also as a practical foundation for developing customized PQC migration strategies. These strategies can be tailored to meet specific critical infrastructure sectors' unique requirements and constraints, spanning energy, transportation, healthcare, and financial services. The knowledge gained from this research can be applied across various industries, ensuring that the most critical systems and assets remain secure amidst the evolving quantum threats.

The transition to PQC is not a one-time event but a continuous journey. It requires steadfast commitment and investment from organizations, policymakers, and the broader security community. As quantum computing capabilities advance, maintaining a vigilant and adaptable approach to PQC adoption is paramount. This involves constantly evaluating the effectiveness of quantum-resistant security measures and adjusting strategies as necessary. By fostering a culture of innovation and collaboration, organizations can spearhead the fight against quantum-enabled adversaries, developing new tools, techniques, and best practices that ensure the long-term security and resilience of critical infrastructure.

## References

CISA, (2003). Homeland Security Presidential Directive 7. Retrieved from http://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7

DSH, (2021). Preparing for Post-Quantum Computing Cryptography. Retrieved from http://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf

DHS, (2003).The Physical Protection of Critical Infrastructures and Key Assets. Retrieved from http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

Mosca, M., & Piani, M. (2022). 2021 Quantum Threat Timeline Report. Retrieved from http://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report-global-risk-institute-global-risk-institute/

NIST, (2017). Post-Quantum Cryptography Standardization. Retrieved from http://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

Chen et al. (2016). Report on post-quantum cryptography. National Institute of Standards and Technology.

World Economic Forum, (2021). Quantum computing governance principles. https://www.weforum.org/whitepapers/quantum-computing-governance-principles

Stallings, W. (2017). Cryptography and network security: principles and practice (7th ed.). Pearson.

Daemen, J., & Rijmen, V. (2002). The design of Rijndael: AES-the advanced encryption standard. Springer.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644-654.

Kirsty Paine, K.P. (2023). Cryptographically Relevant Quantum Computers (CRQCs) & The Quantum Threat. Retrieved from http://www.splunk.com/en_us/blog/learn/crqcs-cryptographically-relevant-quantum-computers.html

Ruane, J., McAfee, A., & Oliver, W. D. (2022). Quantum computing for business leaders. Harvard Business Review. Retrieved from https://hbr.org/2022/01/quantum-computing-for-business-leaders

Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE.

Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review, 41(2), 303-332

Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).

Bernstein, D. J. (2010). Grover vs. McEliece. In Post-Quantum Cryptography (pp. 73-80). Springer, Berlin, Heidelberg.

Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., & Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. Nature photonics, 4(10), 686-689.

Wallden, P., & Kashefi, E. (2019). Cyber security in the quantum era. Communications of the ACM, 62(4), 120-129.

Krause, R. (2023). After Artificial Intelligence, Quantum Computing Could Be The Next Big Thing. Retrieved from https://www.investors.com/news/technology/quantum-computing-after-artificial-intelligence-it-could-be-the-next-big-thing/

GQI, (2024). Riverlane Discloses Its Quantum Error Correction Roadmap Through 2026. Retrieved from http://quantumcomputingreport.com/riverlane-discloses-its-quantum-error-correction-roadmap-through-2026

DHS, (2021). Preparing for Post-Quantum Computing Cryptography. Retrieved from http://www.dhs.gov/sites/default/files/publications/post-quantum_cryptography_infographic_october_2021_508.pdf

Vezic, M. (2023). Q-Day Predictions: Anticipating the Arrival of Cryptanalytically Relevant Quantum Computers (CRQC). Retrieved from http://postquantum.com/post-quantum/q-day-crqc-predictions/

Biamonte et al. (2017). Quantum machine learning. Nature, 549(7671), 195-202

Dunjko, V., & Briegel, H. J. (2018). Machine learning & artificial intelligence in the quantum domain: a review of recent progress. Reports on Progress in Physics, 81(7), 074001.

Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79

Mosca, M., & Piani, M. (2019). Quantum Threat Timeline Report 2019. Global Risk Institute

Herrero-Collantes, M., & Garcia-Escartin, J. C. (2017). Quantum random number generators. Reviews of Modern Physics, 89(1), 015004

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. National Institute of Standards and Technology (NIST) Special Publication 800-207.

Copeland, B. J. (2012). Turing: Pioneer of the Information Age. Oxford University Press.

ETHW, (n.d.). Milestones:Invention of Public-key Cryptography, 1969 - 1975. Retrieved from http://ethw.org/Milestones:Invention_of_Public-key_Cryptography,_1969_-_1975

Singh, S. (1999). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books.

Biercuk, M. J., & Fontaine, R. (2017). The leap into quantum technology: A primer for national security professionals. War on the Rocks, 17.

Chown, P. (2002). Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS). RFC 3268, DOI 10.17487/RFC3268.

Barker, E., & Roginsky, A. (2019). Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST Special Publication 800-131A, Revision 2, DOI 10.6028/NIST.SP.800-131Ar2.

Fischlin, R., & Schnorr, C. P. (2000). Stronger security proofs for RSA and Rabin bits. Journal of Cryptology, 13(2), 221-244, DOI 10.1007/s001459910011.

Gueron, S., & Krasnov, V. (2015). Fast prime field elliptic-curve cryptography with 256-bit primes. Journal of Cryptographic Engineering, 5(2), 141-151, DOI 10.1007/s13389-014-0090-x.

National Institute of Standards and Technology. (2016). Report on Post-Quantum Cryptography. NIST IR 8105, DOI 10.6028/NIST.IR.8105.

Smid, M. E., & Branstad, D. K. (1988). The Data Encryption Standard: past and future. Proceedings of the IEEE, 76(5), 550-559, DOI 10.1109/5.4441.

Alagic et al. (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8413.

Moody et al. (2022). Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8413. https://doi.org/10.6028/NIST.IR.8413

Fernandez-Vazquez et al. (2022). Security Standards and Post-Quantum Cryptography: Current Situation and Future Trends. IEEE Access, 10, 38831-38849. https://doi.org/10.1109/ACCESS.2022.3166092

Buchmann et al. (2022). Post-quantum cryptography: An introduction for data protection officers. Datenschutz und Datensicherheit-DuD, 46(2), 83-88. https://doi.org/10.1007/s11623-022-1587-7

Ticong, L. (2024). 7 Types of Data Classification. Retrieved from http://www.datamation.com/big-data/types-of-data-classification/

Mosca, M. (2015). Cybersecurity in a Quantum World: will we be ready?. Retrieved from http://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

NIST, (2016). Public-Key Post-Quantum Cryptographic Algorithms. Retrieved from http://csrc.nist.gov/News/2016/Public-Key-Post-Quantum-Cryptographic-Algorithms

Moody, D. (2024). Are We there Yet? Retrieved from http://csrc.nist.gov/csrc/media/Presentations/2024/update-on-the-nist-pqc-standardization-project/images-media/moody-are-we-there-yet-pqc-pqc2024.pdf

CSRC, (2022, July). Announcing PQC Candidates to be Standardized, Plus Fourth Round Candidates. Retrieved from http://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4

NIST, (2022). Announcing PQC Candidates to be Standardized, Plus Fourth Round Candidates. Retrieved from http://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

NIST, (2024, August). Quantum Cryptography FIPS Approved. Retrieved from http://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

IBM, (2024, August). NIST’s post-quantum cryptography standards are here. Retrieved from http://research.ibm.com/blog/nist-pqc-standards

McKay, K., Bassham, L. E., Turan, M. S., & Mouha, N. (2017). Report on lightweight cryptography. National Institute of Standards and Technology. Retrieved from https://www.nist.gov/publications/report-lightweight-cryptography

NSA, (n.d.). Quantum Key Distribution (QKD) and Quantum Cryptography QC. Retrieved from http://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

Harishankar, R., Osborne, M., Arun, J. S., Buselli, J., & Janechek, J. (2024). Crypto agility and quantum-safe cryptography. IBM Quantum. Retrieved August 8, 2024, from https://www.ibm.com/quantum/blog/crypto-agility

## Author Information

**Amare Geremew**
https://orcid.org/0009-0007-3599-7049
Capitol Technology University
11301 Springfield Rd, Laurel, MD 20708
USA
Contact e-mail: ageremew*@gmail.com*

**Atif Mohammad (PhD)**
https://orcid.org/0009-0007-6187-0105
Capitol Technology University
11301 Springfield Rd, Laurel, MD 20708
USA