**Post-Quantum Cryptography Transition: Assessing Business Risks and Developing Migration Roadmaps for the Electronics and Software Industries**

**Executive Summary**

The advent of cryptographically relevant quantum computers (CRQCs) presents an existential threat to current cybersecurity infrastructures, which are predominantly reliant on classical public-key cryptography (PKC). This report provides an in-depth analysis of the profound business risks this paradigm shift poses, specifically for the electronics and software industries. It further outlines actionable migration roadmaps towards Post-Quantum Cryptography (PQC), the next generation of cryptographic algorithms designed to withstand quantum attacks.

The core risks stem from the vulnerability of widely deployed asymmetric encryption algorithms such as RSA and Elliptic Curve Cryptography (ECC) to Shor's algorithm, a quantum algorithm capable of breaking their underlying mathematical foundations with unprecedented speed.1 While symmetric algorithms like AES are also impacted by quantum attacks (via Grover's algorithm), the threat is less severe and can generally be mitigated by increasing key lengths.4

A particularly insidious and immediate threat is the "Harvest Now, Decrypt Later" (HNDL) attack strategy. Adversaries are actively collecting and storing vast amounts of encrypted data today, with the intent of decrypting it once sufficiently powerful CRQCs become available.4 This means that any sensitive data with a long confidentiality lifespan, if encrypted with classical algorithms, is already at risk of future exposure.

The electronics industry faces unique challenges due to the proliferation of resource-constrained embedded systems and Internet of Things (IoT) devices, where the typically larger computational and memory footprints of PQC algorithms can be problematic.15 Securing the hardware lifecycle, including secure boot and firmware updates with PQC, is paramount. For the software industry, the transition involves complex integration into the Software Development Lifecycle (SDLC), updating network protocols and APIs, and managing backward compatibility with legacy systems.12

To navigate this transition, organizations are strongly advised to:

* Initiate a comprehensive cryptographic inventory to identify all instances of vulnerable cryptography.
* Conduct a thorough quantum risk assessment, prioritizing assets based on data sensitivity and business criticality.
* Develop and implement a phased PQC migration strategy that embraces crypto-agility—the ability to adapt and update cryptographic algorithms efficiently—and considers hybrid approaches that combine classical and PQC algorithms during the transition.
* Align migration efforts with the standards and timelines set forth by the U.S. National Institute of Standards and Technology (NIST), which has been leading a global effort to standardize PQC algorithms.2
* Invest proactively in research, development, rigorous testing, and collaborative efforts within the industry.

The PQC transition is not merely a technical upgrade; it represents a fundamental strategic shift that will impact business continuity, data governance, regulatory compliance, and the long-term security posture of organizations. Historical cryptographic migrations have often taken a decade or more.10 Given the complexity and scale of the PQC transition, coupled with the immediacy of the HNDL threat, the cost of inaction or delayed response significantly outweighs the investment required for a proactive and well-planned migration. This endeavor demands executive-level attention and strategic resource allocation to safeguard digital assets against the quantum future.

**1. The Quantum Imperative: Understanding the Paradigm Shift**

The digital world is on the cusp of a cryptographic revolution, driven by the rapid advancement of quantum computing. While offering transformative potential in various fields, quantum computers also pose an unprecedented threat to the cryptographic foundations that secure modern communications, data, and digital infrastructure. Understanding this paradigm shift is the first critical step for businesses in the electronics and software industries to prepare for a post-quantum future.

* **1.1. The Looming Quantum Threat to Current Cryptography**

Quantum computers operate on principles fundamentally different from classical computers. Instead of bits representing 0s or 1s, quantum computers use "qubits." Qubits can exist in a state of superposition, representing 0, 1, or a combination of both simultaneously. Furthermore, qubits can be linked through a phenomenon called entanglement, where the state of one qubit is directly correlated with the state of another, regardless of the distance separating them.3 These properties allow quantum computers to perform certain types of calculations exponentially faster than any known classical computer.

This computational prowess has profound implications for cryptography. Two quantum algorithms, in particular, threaten the security of widely used cryptographic systems:

Shor's Algorithm and its Impact on Public-Key Cryptography:

Public-Key Cryptography (PKC), also known as asymmetric cryptography, is the bedrock of secure internet communication, digital signatures, and data protection. Systems like RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography), and Diffie-Hellman (DH) key exchange rely on the computational difficulty of mathematical problems such as factoring very large integers (for RSA) or solving the discrete logarithm problem over finite fields or elliptic curves (for ECC and DH).5 Classical computers find these problems intractable for sufficiently large key sizes.

However, Peter Shor's quantum algorithm, developed in 1994, can solve these underlying mathematical problems efficiently.2 Once a sufficiently large and stable quantum computer capable of running Shor's algorithm becomes available, it will be able to break RSA, ECC, and DH encryption, rendering them effectively useless for securing information.1 This means that secure web connections (HTTPS/TLS), encrypted emails, digital signatures verifying software authenticity, and many other critical security functions will become vulnerable.

The resources required are substantial. Estimates suggest that breaking a common RSA-2048 key might require approximately 4,100 error-corrected, or "logical," qubits, while breaking ECC-256 might need around 500 to 1,600 logical qubits.6 It is important to note that a single logical qubit requires many physical qubits to implement quantum error correction, potentially scaling to millions of physical qubits depending on their error rates.7 This distinction underscores the significant engineering challenges in building a CRQC, but the theoretical vulnerability remains.

Grover's Algorithm and its Impact on Symmetric Cryptography and Hash Functions:

Symmetric cryptography, such as the Advanced Encryption Standard (AES), uses the same key for both encryption and decryption. Hash functions, like SHA-2 (Secure Hash Algorithm 2) and SHA-3, create fixed-size "fingerprints" of data, essential for data integrity checks and various other cryptographic protocols. These systems are not directly vulnerable to Shor's algorithm.

However, Lov Grover's quantum algorithm, developed in 1996, provides a quadratic speedup for searching unsorted databases.4 This can be applied to brute-force attacks against symmetric keys or to finding pre-images or collisions in hash functions, effectively halving the bit security of these primitives.8 For example, Grover's algorithm reduces the effective strength of AES-128 to that of a 64-bit key, and AES-256 to that of a 128-bit key.

Fortunately, the impact of Grover's algorithm is less catastrophic than Shor's. The standard mitigation is to double the key lengths of symmetric ciphers or use hash functions with larger output sizes.4 For instance, migrating from AES-128 to AES-256 is generally considered sufficient to maintain security against known quantum attacks.4 Even with Grover's algorithm, breaking AES-128 is estimated to take an astronomically long time (e.g., 2.61×1012 years with an ideal quantum computer) and require thousands of logical qubits (around 2,953 for AES-128).9

The differential impact is a crucial factor in strategic planning: asymmetric cryptography faces an existential threat requiring complete replacement, whereas symmetric cryptography faces a manageable weakening that can be addressed by increasing key sizes. This distinction directly informs the prioritization and resource allocation in PQC migration strategies.

**Table 1: Impact of Quantum Algorithms on Current Cryptographic Standards**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Classical Algorithm** | **Threatening Quantum Algorithm** | **Nature of Threat** | **Estimated Logical Qubits to Break/Weaken** | **Recommended PQC Action** |
| RSA-2048 | Shor's Algorithm | Broken | ~4,096 7 (or ~4,100 6) | Replace with PQC KEM/Signature |
| ECC-256 | Shor's Algorithm | Broken | ~512 7 (or ~1,600 6) | Replace with PQC KEM/Signature |
| AES-128 | Grover's Algorithm | Weakened | ~2,953 (for theoretical break) 9 | Migrate to AES-256 |
| AES-256 | Grover's Algorithm | Weakened | ~6,681 (for theoretical break) 9 | Considered quantum-resistant |
| SHA-256 | Grover's Algorithm | Weakened | (Effective security reduced to 128-bit) | Use SHA-384 or PQC hashes |
| SHA-384 | Grover's Algorithm | Weakened | (Effective security reduced to 192-bit) | Considered quantum-resistant |

This table provides a concise summary of the core threats, directly informing risk assessment. It highlights which parts of current cryptographic infrastructure are most vulnerable and the general type of remedial action required, synthesizing data from multiple sources.1

* **1.2. "Harvest Now, Decrypt Later" (HNDL): The Silent Risk**

The timeline for the arrival of a fully capable CRQC is still subject to debate, but the "Harvest Now, Decrypt Later" (HNDL) attack scenario makes the quantum threat an immediate concern.4 In an HNDL attack, adversaries intercept and exfiltrate encrypted data today, even if they cannot decrypt it with current classical computing capabilities. They then store this data, sometimes for years or decades, anticipating that future quantum computers will possess the power to break the classical encryption used to protect it.4

This strategy is particularly dangerous for information that retains its value over long periods. Examples include:

* National security secrets and classified government intelligence.13
* Corporate intellectual property, trade secrets, and long-term strategic plans.12
* Personal identifiable information (PII), personal health records (PHR), and financial data that may be exploited for identity theft, fraud, or blackmail years later.13
* Long-term sensitive communications between individuals or organizations.

Data with shorter lifespans, such as credit card numbers that can be quickly cancelled and reissued, are less attractive targets for HNDL attacks because their value diminishes rapidly.13

The HNDL threat fundamentally alters the risk calculation timeline. It is no longer solely about when quantum computers can break *future* encrypted communications, but when they can compromise *past and currently encrypted* sensitive data that has already been stolen. This implies that organizations cannot afford to wait for the definitive arrival of a CRQC to begin protecting data that requires long-term confidentiality. The migration to PQC must start well before a CRQC is known to be operational to counter this silent and ongoing data harvesting.11 The recognition of HNDL as an active threat underscores the urgency for organizations to identify their most sensitive long-lived data and prioritize its protection with quantum-resistant measures.

* **1.3. Projected Timelines and the Urgency for Action**

Estimating the arrival of a CRQC capable of breaking current PKC standards is challenging, with predictions varying among expert groups:

* The Global Risk Institute, in 2024, estimated a 17% to 34% chance of a CRQC capable of breaking RSA-2048 within 24 hours by 2034, with this probability rising to 79% by 2044.37
* Gartner suggests that quantum computers could begin compromising current encryption methods as early as 2029, with widespread vulnerability by 2034.10
* The Boston Consulting Group forecasts a period of broad quantum advantage emerging between 2030 and 2040.10
* Some industry projections, like one from Samsung LSI, suggest that a 1 million-qubit quantum computer—potentially capable of breaking RSA-2048 in approximately 160 hours—could be achievable by 2028, assuming a continued rapid pace of qubit development.16

Currently, quantum computing capabilities are still in their nascent stages relative to what is needed to break strong classical encryption. Small-scale quantum computers have been built, successfully demonstrating the underlying physical principles.3 However, the largest RSA number definitively factored by a quantum computer using Shor's algorithm is still only 21, a feat achieved in 2012.38 Analog quantum computers have factored slightly larger, but still very small, numbers (e.g., a 23-bit integer 39). In contrast, classical supercomputers have factored numbers like RSA-250 (an 829-bit number), though this required immense computational effort.39

Physical qubit counts in experimental quantum processors are now in the hundreds to over a thousand (e.g., IBM's 1121-qubit Condor QPU 38). However, these are physical qubits, which are prone to errors ("noise"). Running complex quantum algorithms like Shor's against strong encryption requires a large number of high-fidelity *logical* qubits, each of which is constructed from many physical qubits using quantum error correction codes.7 The development of robust logical qubits is a critical ongoing research area. Milestones are being achieved, such as Google's 2023 demonstration of a logical qubit (using 49 physical qubits) that exhibited a lower error rate than its constituent physical qubits 35, and Microsoft's work on topological qubits aiming for a fault-tolerant prototype within years.40 Despite this progress, the gap between current capabilities and the thousands of stable logical qubits needed to threaten RSA-2048 remains significant.

Compounding the uncertainty of CRQC arrival is the timeline for cryptographic migration. Past transitions, such as the move from DES to AES or the deprecation of SHA-1, often took over a decade to complete across the global digital ecosystem.10 The PQC transition is anticipated to be at least as complex and lengthy, if not more so, due to the pervasive nature of public-key cryptography and the more substantial changes some PQC algorithms introduce in terms of key sizes and performance characteristics.12

Recognizing these factors, NIST has provided transition guidance. According to NIST Interagency Report (IR) 8547, classical algorithms providing 112-bit security strength (such as some deployments of RSA and ECC) are proposed to be deprecated after 2030 and disallowed for use in new systems after 2035. Classical algorithms offering 128-bit security strength or higher are proposed to be disallowed after 2035.32 These timelines effectively create a "quantum decade" (roughly 2025-2035) during which organizations must make substantial progress in their PQC migrations. Given the HNDL threat and the lengthy migration process, waiting until the end of this period to act is not a viable strategy. The convergence of CRQC development estimates, regulatory timelines, and the inherent complexity of crypto migration creates a window of high urgency for organizations to commence their PQC transition planning and execution immediately.

**2. Navigating the Post-Quantum Cryptography Landscape**

As the quantum threat materializes, the global cryptographic community, spearheaded by NIST, has been diligently working to develop and standardize a new suite of cryptographic algorithms collectively known as Post-Quantum Cryptography (PQC). These algorithms are designed to be secure against attacks from both powerful classical computers and the anticipated capabilities of future quantum computers.

* **2.1. Overview of PQC: Principles and Goals**

Post-Quantum Cryptography refers to cryptographic algorithms, particularly public-key algorithms, that are resistant to cryptanalysis by quantum computers.11 Unlike classical PKC (RSA, ECC, DH) which relies on the difficulty of number-theoretic problems like integer factorization or discrete logarithms, PQC algorithms derive their security from a different set of mathematical problems believed to be hard for quantum computers to solve. These include problems based on:

* **Lattices:** Finding the shortest or closest vector in a high-dimensional geometric grid (lattice).5
* **Codes:** Decoding information from a noisy signal using error-correcting codes.5
* **Multivariate Polynomials:** Solving systems of many polynomial equations with many variables over a finite field.5
* **Hash Functions:** Relying on the one-way, collision-resistant properties of cryptographic hash functions.5
* **Isogenies:** Finding a specific type of map (an isogeny) between elliptic curves.5

The primary goal of the PQC initiative is to develop, rigorously evaluate, and standardize new public-key cryptographic algorithms for key establishment (or key encapsulation mechanisms - KEMs) and digital signatures. These new standards are intended to replace or augment currently vulnerable classical algorithms, ensuring the continued confidentiality, integrity, and authenticity of digital information in the quantum era.11

* **2.2. The NIST Standardization Process: Milestones and Key Outcomes**

NIST initiated its PQC standardization process in December 2016, issuing a public call for proposals for quantum-resistant algorithms.29 This multi-year, transparent, and collaborative international effort involved several rounds of submission, public scrutiny, cryptanalysis, and evaluation by NIST and the global cryptographic community.28 The process started with 69 candidate algorithms in the first round, which were narrowed down through rigorous analysis in subsequent rounds.31

Key Outcomes and Finalized Standards (Published August 2024):

**Works cited**

1. www.ej-compute.org, accessed May 17, 2025, <https://www.ej-compute.org/index.php/compute/article/view/146/116#:~:text=While%20quantum%20attacks%20against%20RSA,cryptography%20on%20a%20large%20scale.>
2. What Is Quantum Computing's Threat to Cybersecurity? - Palo Alto Networks, accessed May 17, 2025, <https://www.paloaltonetworks.com/cyberpedia/what-is-quantum-computings-threat-to-cybersecurity>
3. The Impact of Quantum Computing on Cryptography - Cryptomathic, accessed May 17, 2025, <https://www.cryptomathic.com/blog/quantum-computing-and-its-impact-on-cryptography>
4. The Impact of Quantum Computing on Cryptography (2025). - Aliyesha, accessed May 17, 2025, <https://aliyesha.com/sub/articles/technology/display/al_impact_quantum_computing_cryptography>
5. Types of Post Quantum Cryptography Public Key Schemes - Utimaco, accessed May 17, 2025, <https://utimaco.com/news/blog-posts/types-post-quantum-cryptography-public-key-schemes>
6. What is post-quantum cryptography, accessed May 17, 2025, <https://quantumstrategyinstitute.com/2023/02/15/what-is-post-quantum-cryptography/>
7. NIST PQC Algorithms - Cogito Group, accessed May 17, 2025, <https://cogitogroup.net/wp-content/uploads/2024/09/NIST-Post-Quantum-Cryptography-Alogorithms.pdf>
8. Quantum Cryptanalysis - PQSecure Technologies, accessed May 17, 2025, <https://pqsecurity.com/quantum-cryptanalysis/>
9. 128 or 256 bit Encryption: Which Should I Use? - Ubiq Security, accessed May 17, 2025, <https://www.ubiqsecurity.com/128bit-or-256bit-encryption-which-to-use/>
10. 10 seconds to break: Preparing for quantum security threats | Unisys, accessed May 17, 2025, <https://www.unisys.com/blog-post/cis/10-seconds-to-break-preparing-for-quantum-security-threats/>
11. From the Frontlines of Post-Quantum Cryptography - Booz Allen, accessed May 17, 2025, <https://www.boozallen.com/insights/velocity/from-the-frontlines-of-post-quantum-cryptography.html>
12. Cloud CISO Perspectives: Why PQC is the next Y2K, and what you ..., accessed May 17, 2025, <https://cloud.google.com/blog/products/identity-security/cloud-ciso-perspectives-prepare-early-for-PQC-resilient-cryptographic-threats>
13. Harvest Now, Decrypt Later(HNDL): Preparing for the Quantum Threat, accessed May 17, 2025, <https://www.encryptionconsulting.com/harvest-now-decrypt-later-preparing-for-the-quantum-threat/>
14. Data protection in a quantum enabled future | Gowling WLG, accessed May 17, 2025, <https://gowlingwlg.com/en/insights-resources/articles/2025/data-protection-in-a-quantum-enabled-future>
	1. Hybrid PQC Rollout Guide for Enterprises - OnlineHashCrack, accessed May 17, 2025, <https://www.onlinehashcrack.com/guides/post-quantum-crypto/hybrid-pqc-rollout-guide-for-enterprises.php>
	2. RWPQC 2025 Brings Together Industry Leaders to Advance Cybersecurity and Quantum Innovation | MITRE, accessed May 17, 2025, <https://www.mitre.org/news-insights/news-release/rwpqc-2025-brings-together-industry-leaders-advance-cybersecurity-and>