Post-Quantum Cryptography: Preparing for the Quantum Threat to Global Security

Author: Driti Virani

Affiliation: EVHS High School, Senior

Date: October 2024 - Present

Abstract

The public-key infrastructure that underpins global digital security is predicated on the computational intractability of certain mathematical problems for classical computers. This paradigm is facing an existential threat from the development of cryptographically-relevant quantum computers (CRQCs), which will render these problems solvable in practical timeframes. This report provides a comprehensive analysis of this impending cryptographic transition. By synthesizing foundational academic papers, standards from the National Institute of Standards and Technology (NIST), and extensive industry analysis, this research examines the mathematical certainty of classical cryptography's collapse due to Shor's algorithm.[1] It establishes the immediate and severe risk posed by "Harvest Now, Decrypt Later" (HNDL) attacks, wherein adversaries are currently archiving encrypted data for future decryption. The report evaluates the leading quantum-resistant alternative—lattice-based cryptography—and details the technical specifications of the NIST-selected standards, CRYSTALS-Kyber and CRYSTALS-Dilithium.[1] The primary thesis of this report is that the migration to post-quantum cryptography (PQC) is not merely a technical upgrade but a complex, decade-long socio-technical challenge. A successful transition requires immediate action to preempt the retroactive compromise of data encrypted today, with the ultimate strategic goal being the establishment of a cryptographically agile infrastructure resilient to future computational breakthroughs.

1. Introduction: The Impending Cryptographic Singularity

The advent of quantum computing represents a fundamental discontinuity in the history of information security. It is not an incremental threat to be managed with conventional patches or larger key sizes, but a deterministic outcome of progress in physics and computer science that necessitates a complete re-architecting of our digital trust infrastructure. The transition to post-quantum cryptography (PQC) is therefore one of the most critical and urgent infrastructure projects of the 21st century.[1]

1.1 The Mathematical Bedrock of Modern Digital Trust

Modern digital civilization operates on a foundational assumption: that certain mathematical problems are so computationally intensive that they are, for all practical purposes, unsolvable by classical computers. This assumption of intractability forms an "exponential wall" that protects the vast majority of digital interactions.[1] This security model underpins:

- **Secure Communications:** The Transport Layer Security (TLS) protocol, signified by the padlock in a web browser, uses public-key cryptography to secure trillions of dollars in e-commerce and protect the privacy of billions of users.[1]
- **Financial Transactions:** Banking systems, credit card networks, and cryptocurrencies rely on digital signatures to authenticate transactions and prevent fraud.[1]
- **Data Integrity:** Digital signatures are used to verify the authenticity of software updates, legal documents, and critical system files.[1]
- **National Security:** Governments use public-key cryptography to protect classified communications, diplomatic cables, and military operations.[1]

The security of these systems rests on the difficulty of solving problems such as:

1. **Integer Factorization:** Given a large number n that is the product of two prime numbers p and q, finding p and q. This is the basis for the RSA algorithm.[1]
2. **The Discrete Logarithm Problem (DLP):** Given a generator g and a value g^x, finding the exponent x. This underlies the Diffie-Hellman key exchange protocol.[1]
3. **The Elliptic Curve Discrete Logarithm Problem (ECDLP):** A variant of the DLP performed on the points of an elliptic curve, which forms the basis for Elliptic Curve Cryptography (ECC).[1]

For a standard 2048-bit RSA key, the most efficient classical algorithm, the General Number Field Sieve (GNFS), would require billions of years of computation on the world's most powerful supercomputers to succeed.[1] This computational infeasibility is the bedrock of digital trust.

1.2 Shor's Algorithm: A Discontinuous Leap in Computational Capability

In 1994, mathematician Peter Shor published a theoretical algorithm that shattered this bedrock assumption.[1] He proved that a sufficiently powerful quantum computer could solve both the integer factorization and discrete logarithm problems in polynomial time. This represents a paradigm shift—not an incremental improvement, but a fundamental change in the nature of computational complexity that invalidates the core security assumptions of the last half-century.[1]

The scale of this leap is difficult to overstate. As illustrated in Table 1, problems that are effectively impossible for classical machines become trivial for a CRQC.

Table 1: Classical vs. Quantum Computational Complexity [1]

Problem	Best Classical Algorithm Complexity	Quantum Algorithm (Shor's) Complexity	Practical Impact
Factoring a 2048-bit RSA integer	$O(\exp(n^{1/3}(\log n)^{2/3}))$	$O(n^3)$	Billions of years → Hours
ECDLP on a 256-bit curve	$O(\sqrt{n})$	$O(n^3)$	Trillions of years → Minutes

Increasing key sizes, the traditional defense against growing computational power, offers no protection. RSA-4096 and RSA-8192 are just as vulnerable to Shor's algorithm as RSA-2048, requiring only a polynomial increase in quantum resources to break.[1] This is not a vulnerability that can be patched; it is an architectural collapse of the entire public-key cryptographic paradigm.

1.3 The Harvest Now, Decrypt Later Imperative: A Threat to Past, Present, and Future Data

The most insidious and urgent aspect of the quantum threat is that it does not require a CRQC to exist today to compromise data encrypted today. The "Harvest Now, Decrypt Later" (HNDL) attack model, also known as "store now, decrypt later," is actively being pursued by sophisticated adversaries, particularly nation-state intelligence agencies.[1]

The attack proceeds in two phases:

1. **Phase 1: Harvest (Present Day):** Adversaries intercept and store vast quantities of encrypted data traversing the internet—HTTPS traffic, VPN tunnels, secure emails, and messaging archives. With the cost of data storage plummeting (a petabyte of storage costs a few thousand dollars), this large-scale collection is economically feasible.[1] The data remains secure for now, protected by classical cryptographic algorithms.
2. **Phase 2: Decrypt (Future):** When a CRQC becomes available (with timelines estimated between 2035 and 2045), adversaries will apply Shor's algorithm to the harvested data, compute the private keys, and retroactively decrypt decades of historical communications.[1]

This attack model creates a temporal paradox that breaks traditional cybersecurity paradigms. Standard incident response is reactive: a vulnerability is discovered, exploited, and then patched, with the damage contained to the period of exposure. In the HNDL model, the *attack* (data harvesting) is decoupled from the *breach* (decryption) by 10 to 20 years. This means that from a risk management perspective, any data with a long confidentiality requirement is *already compromised* the moment it is transmitted using quantum-vulnerable cryptography, even though its contents remain secret today. This temporal dislocation invalidates conventional security metrics and response models, forcing a shift from reactive defense to a proactive, predictive posture based on data lifecycle management and future threat forecasting.

The risk is not uniform across all data types. The critical factor is the required confidentiality lifespan of the information versus the projected timeline for the arrival of a CRQC.

Table 2: Data at Risk from Harvest-Now-Decrypt-Later Attacks [1]

Data Type	Required Confidentiality Period	Threat Level
Credit Card Numbers	3-5 years	Low
Corporate Intellectual Property	10-20 years	High
Military Operational Plans	30-50 years	Critical
Government Secrets / Diplomatic Cables	20-75 years	Critical
Medical Records / Genetic Data	Lifetime (70+ years)	Critical

As Table 2 demonstrates, any information that must remain confidential beyond the next 15 to 30 years is already at severe risk. This includes national security intelligence, genomic data, corporate trade secrets, and critical infrastructure plans. The HNDL threat transforms the future quantum risk into an immediate data security crisis.[1]

2. Classical Public-Key Cryptography: A Paradigm on the Brink of Obsolescence

To fully appreciate the scale of the quantum threat, it is essential to understand the mathematical elegance of the systems it will break. For decades, RSA and ECC have provided robust security, but their shared reliance on problems within the same mathematical class creates a systemic single point of failure.

2.1 The RSA Cryptosystem: Security Through the Assumed Intractability of Integer Factorization

The RSA algorithm, named for its inventors Rivest, Shamir, and Adleman, has been the workhorse of public-key cryptography since 1977. Its operation is straightforward [1]:

1. **Key Generation:** Two very large prime numbers, p and q, are chosen and multiplied to produce a public modulus $n = p \times q$. A public exponent e is chosen, and a private exponent d is computed such that $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$. The public key is (n, e), and the private key is (n, d).
2. **Encryption:** A message m is encrypted to a ciphertext c using the public key: $c = m^e \pmod{n}$.
3. **Decryption:** The ciphertext c is decrypted back to the message m using the private key: $m = c^d \pmod{n}$.

The security of the entire system rests on a single assumption: given n and e, it is computationally infeasible to find d without first factoring n into p and q. Against classical computers, this assumption holds true due to the exponential growth in the difficulty of factoring as the size of n increases.

Table 3: RSA Key Size vs. Classical Factoring Time [1]

RSA Key Size	Decimal Digits in n	Estimated Classical Factoring Time
512 bits	155	Broken in 1999
1024 bits	309	Months with a supercomputer
2048 bits	617	**Billions of years**
4096 bits	1,234	**Trillions of years**

This exponential scaling provided a reliable security margin for decades. However, as established, this scaling provides zero protection against a quantum computer, making the entire architecture obsolete.[1]

2.2 Elliptic Curve Cryptography: The Irony of Classical Efficiency versus Quantum Fragility

In the 2000s and 2010s, much of the internet migrated from RSA to Elliptic Curve Cryptography (ECC). The motivation was not a security concern, but a drive for efficiency. ECC provides the same level of security as RSA but with dramatically smaller keys, which translates to faster computations, lower bandwidth usage, and reduced power consumption—critical advantages for mobile and embedded devices.[1]

ECC's security is based on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP). Instead of integers, operations are performed on the points of an elliptic curve defined by the equation $y^2 = x^3 + ax + b$ over a finite field. A private key is a scalar k, and the public key is a point Q on the curve, computed as $Q = k \cdot G$, where G is a public base point. The operation $k \cdot G$ involves adding the point G to itself k times. While computing Q from k and G is fast, finding k given Q and G is classically intractable.[1]

Table 4: RSA vs. ECC Key Size Comparison for Equivalent Security [1]

Security Level (Symmetric Equivalent)	**RSA Key Size**	**ECC Key Size**	**Efficiency Gain**
128-bit	3072 bits	256 bits	**12x smaller**
192-bit	7680 bits	384 bits	**20x smaller**
256-bit	15360 bits	521 bits	**29x smaller**

This efficiency led to ECC's widespread adoption in modern protocols like TLS 1.3, cryptocurrencies like Bitcoin, and secure messaging apps like Signal.[1] However, this massive, multi-billion dollar global migration effort now serves as a powerful cautionary tale in threat modeling. The underlying hard problem for ECC, the ECDLP, belongs to the same general class of mathematical problems (the Hidden Subgroup Problem) as integer factorization. Shor's algorithm solves both with similar polynomial-time efficiency.[1] Consequently, the vast investment in migrating from RSA to ECC, while beneficial against classical adversaries, yielded zero improvement in security against the emerging quantum threat. This history demonstrates the profound danger of optimizing for a known threat landscape while failing to account for paradigm-shifting changes in adversary capability. It underscores the critical need for mathematical diversity in any future cryptographic portfolio, a principle that has heavily influenced NIST's PQC standardization process.[9]

3. The Quantum Attack Vector: A Mathematical Autopsy of Shor's Algorithm

Shor's algorithm is not a brute-force attack; it is an elegant mathematical procedure that exploits the unique properties of quantum mechanics—superposition and interference—to find structure in large numerical problems. Understanding its mechanism is key to understanding why the threat is so fundamental.

3.1 The Core Insight: Reducing Factoring and Discrete Logarithms to Period-Finding

The first part of Shor's algorithm is entirely classical. It uses number theory to transform the problem of factoring an integer n into the problem of finding the period of a modular exponential function.[1]

1. Choose a random integer $a < n$.
2. Consider the function $f(x) = a^x \pmod{n}$. This function is periodic, meaning it repeats its values in a cycle. The length of this cycle is called the period, r.
3. If one can find this period r, and if r is even, then the factors of n can likely be found by computing the greatest common divisor: $\gcd(a^{r/2} - 1, n)$ and $\gcd(a^{r/2} + 1, n)$.[1]

Classically, finding r is just as hard as factoring n in the first place, because it requires computing $f(x)$ for a potentially exponential number of inputs until the pattern repeats. The quantum breakthrough was in finding r efficiently.[1]

3.2 The Quantum Fourier Transform and Phase Estimation: The Engine of Exponential Speedup

The quantum part of the algorithm is a specialized subroutine known as Quantum Phase Estimation, which uses the Quantum Fourier Transform (QFT) to find the period r. While the underlying physics is complex, the process can be understood conceptually [1]:

1. **Superposition:** Two quantum registers are prepared. The first register is put into a uniform superposition of all possible integer values up to a certain size. This is akin to preparing the computer to test all possible inputs simultaneously.
2. **Quantum Parallelism:** A quantum operation corresponding to the function $f(x) = a^x \pmod{n}$ is applied. Due to superposition, this single operation effectively computes the function's output for all possible inputs at once, encoding the results in the second register.
3. **Quantum Fourier Transform (QFT):** The QFT is applied to the first register. The QFT is the quantum analogue of the classical Fourier transform, which is used to find periodicities in signals. In this context, the QFT causes constructive interference at frequencies related to the period r and destructive interference at all other frequencies.
4. **Measurement:** The first register is measured. The laws of quantum mechanics dictate that the measurement will collapse the superposition into a single classical value. Due to the interference pattern created by the QFT, this measured value will, with high probability, be an integer multiple of $1/r$.
5. **Classical Post-Processing:** From the measured value, the period r can be efficiently deduced using a classical algorithm called the Continued Fractions Algorithm. Once r is known, the factors of n are computed as described above.[1]

This combination of quantum parallelism and the QFT allows a quantum computer to find the hidden period in a number of steps that grows only polynomially with the size of the number being factored, achieving an exponential speedup over any known classical method.[1]

3.3 Resource Estimates for Cryptographically-Relevant Quantum Computers (CRQCs)

Breaking modern encryption requires a large, fault-tolerant quantum computer. While current devices are small and noisy, progress is rapid. The timeline for the arrival of a CRQC is being compressed by a "pincer movement" of two simultaneous trends. From the bottom up, hardware is improving, with steady increases in the number and quality of physical qubits (the basic building blocks of quantum computers).[1] From the top down, algorithmic and error-correction improvements are continuously *reducing* the number of qubits required to execute attacks. For example, leading academic estimates for the number of noisy qubits needed to break RSA-2048 have fallen from approximately 20 million in a 2021 analysis to under 1 million in a 2025 projection.[1] This pincer movement means that forecasting CRQC arrival by simply extrapolating current qubit counts is likely to be overly optimistic; the target is moving closer as the technology advances toward it.

Table 5: Timeline Projections and Resource Requirements for a CRQC [1]

Scenario	Estimated Timeline	Required Logical (Error-Corrected) Qubits	Required Noisy Physical Qubits	Key Assumptions
Optimistic	10-15 years (2035-2040)	~4,000	~1,000,000	Rapid progress in quantum error correction and qubit coherence.
Realistic	20-25 years (2045-2050)	~10,000	~5,000,000	Steady, incremental progress in overcoming engineering challenges.
Pessimistic	30+ years (2055+)	~20,000	~20,000,000	Fundamental physical limits are encountered; investment slows.

Even under the most pessimistic scenarios, a CRQC is expected to arrive within the confidentiality lifetime of critical data being generated today. This reinforces the urgency of the HNDL threat and the need to begin the migration to PQC immediately.[1]

4. Post-Quantum Cryptography: The Search for Quantum-Resistant Hard Problems

With the mathematical foundations of RSA and ECC set to collapse, the cryptographic community has spent the last decade searching for and analyzing new classes of mathematical problems that are believed to be hard for both classical and quantum computers. The most promising and mature of these are based on the geometry of high-dimensional lattices.[1]

4.1 The Promise of Lattices: Hardness in High-Dimensional Geometry

In mathematics, a lattice is a regular, infinite grid of points in an n-dimensional space.[1] Lattice-based cryptography derives its security from the apparent difficulty of solving certain geometric problems on these high-dimensional grids. The two most famous such problems are [10]:

- **Shortest Vector Problem (SVP):** Given a description of a lattice, find the shortest non-zero vector from the origin to another lattice point.
- **Closest Vector Problem (CVP):** Given a description of a lattice and a target point in space that is not on the lattice, find the lattice point closest to the target.

While these problems are easy to visualize and solve in two or three dimensions, their difficulty grows exponentially with the number of dimensions. Crucially, no efficient quantum algorithm analogous to Shor's has been discovered that provides a significant speedup for solving SVP or CVP in high dimensions.[1] This apparent quantum resistance has made lattices the leading foundation for PQC standards.

4.2 Learning With Errors (LWE): The Foundational Problem for Modern PQC

The most versatile and widely used hard problem for constructing PQC systems is Learning With Errors (LWE). The LWE problem, introduced by Oded Regev in 2005, can be understood as solving a system of linear equations that has been perturbed by a small amount of random noise.[1]

The problem is defined as follows: given a matrix A and a vector b such that $b \approx A \cdot s$, the goal is to find the secret vector s. More formally, $b = A \cdot s + e$, where e is a small, random "error" vector. Without the error term e, finding s is a standard problem in linear algebra that is easy to solve. The addition of the small, random noise makes the problem computationally intractable for both classical and quantum computers.[1]

LWE-based cryptosystems possess a powerful security property that most classical schemes lack: a formal mathematical proof that reduces the difficulty of breaking an average instance of the cryptosystem to the difficulty of solving an underlying lattice problem (like SVP) in the *worst case*.[1] This means that if an adversary can break an average LWE-based encryption, they must have discovered a method to solve the hardest possible instances of these foundational lattice problems, which have resisted decades of intense scrutiny.

However, this powerful theoretical guarantee comes with a practical subtlety. The mathematical reduction is not "tight," meaning it loses some security parameters in the conversion from the worst-case lattice problem to the average-case LWE problem. This "tightness gap" means that to achieve a desired security level (e.g., 128-bit security), the parameters used in the LWE cryptosystem must correspond to an underlying lattice problem that is significantly harder (e.g., 200+ bits of security).[1] This necessity to compensate for the looseness in the security proof is a primary reason why PQC keys and signatures are substantially larger than their ECC counterparts. This trade-off between theoretical security guarantees and real-world performance remains a key focus of ongoing cryptanalysis and explains why NIST has adopted conservative parameter sets for its standards.[1]

4.3 The NIST Standards: A Technical Analysis of CRYSTALS-Kyber and CRYSTALS-Dilithium

After a multi-year competition involving cryptographers from around the world, NIST announced its first set of standardized PQC algorithms in 2022, with the final standards published in August 2024. The primary selections are both based on structured variants of the LWE problem over module lattices.[1]

- **CRYSTALS-Kyber (Standardized as ML-KEM in FIPS 203):** This is the selected standard for Key Encapsulation Mechanisms (KEMs), which are used to establish a shared secret key between two parties (a replacement for Diffie-Hellman and ECDH).[1] Kyber is known for its excellent performance, with key generation, encapsulation, and decapsulation operations taking well under a millisecond on modern processors.[1]

However, its public keys are significantly larger than those of ECC. For example, the recommended security level, Kyber-768, has a public key of 1,184 bytes, compared to just 32 bytes for an equivalent ECC key.[1]

- **CRYSTALS-Dilithium (Standardized as ML-DSA in FIPS 204):** This is the primary standard for digital signatures, replacing RSA signatures and ECDSA.[1] Dilithium is also highly performant but introduces an even larger size overhead. A Dilithium3 signature is 3,293 bytes, and its corresponding public key is 1,952 bytes. In contrast, an ECDSA signature and public key are each only 64 bytes.[1] This size increase has significant implications for applications with bandwidth or storage constraints, such as certificate chains and blockchain technologies.
- **SPHINCS+ (Standardized as SLH-DSA in FIPS 205):** NIST also standardized SPHINCS+, a hash-based signature scheme, as a conservative backup.[1] Its security relies only on the hardness of the underlying hash function (like SHA-256), a much older and more battle-tested security assumption. This provides valuable mathematical diversity. The trade-off is poor performance: SPHINCS+ signatures are enormous (nearly 30 KB for high security) and the signing process is orders of magnitude slower than Dilithium.[1] It is intended for niche applications where performance is not a primary concern, such as signing firmware updates.

5. The Migration Imperative: A Roadmap for Global Transition

The development of quantum-resistant algorithms is only the first step. The far greater challenge is migrating the entire global digital ecosystem to these new standards—a process that is fraught with technical, economic, and organizational hurdles.[1]

5.1 A Triumvirate of Challenges: Technical, Economic, and Organizational Hurdles

The PQC migration is a complex undertaking with multifaceted challenges:

- **Technical Challenges:** The most immediate issue is the significant increase in key and signature sizes associated with the new standards. This "size explosion" impacts network bandwidth, slows down protocols like TLS that require key exchange in their handshake, and can exceed the memory and storage capacity of resource-constrained embedded systems and IoT devices.[1] Furthermore, these new algorithms introduce novel implementation risks, particularly from side-channel attacks (e.g., timing or power analysis) that can leak secret key information if not coded with extreme care.[1]

- **Economic Challenges:** The cost of this global transition is immense. The U.S. Office of Management and Budget (OMB) delivered a preliminary estimate of $7.1 billion to migrate just the U.S. federal government's non-national security systems.[30] Extrapolating this globally to the private sector suggests a total cost well over $100 billion, comparable in scale to the Y2K remediation effort.[33] These costs include not only direct software and hardware upgrades but also extensive testing, validation, training, and the replacement of legacy systems that cannot be updated.[1]
- **Organizational Challenges:** Perhaps the most significant barrier is organizational inertia. Surveys indicate that a large majority of organizations are unaware of the quantum threat or do not consider it an immediate priority.[35] Securing executive buy-in for a multi-million dollar, decade-long project to mitigate a future threat is extremely difficult, especially when security teams are already overstretched dealing with immediate risks like ransomware.[1] The first and most critical step for any organization is to conduct a comprehensive cryptographic inventory to understand where vulnerable algorithms are being used—a task that is itself a major undertaking.[7]

The PQC migration is not fundamentally a technology problem; the core algorithms are standardized and functional. It is a socio-technical problem rooted in misaligned incentives. The costs of migration are immediate, concrete, and high, while the benefits—averting a future threat—are delayed, abstract, and probabilistic. This creates a powerful disincentive to act. Overcoming this inertia is the central challenge of the transition and requires strong external "forcing functions," such as government mandates (e.g., the NSA's CNSA 2.0), regulatory pressure (e.g., from financial or healthcare sectors), and clear vendor-driven timelines (e.g., Microsoft's public commitment to a 2033 migration deadline).[1]

5.2 The Hybrid Approach: A Pragmatic Bridge to a Quantum-Safe Future

Given the novelty of PQC algorithms and the risks associated with a "flash cut" transition, a broad consensus has emerged around a hybrid approach as the best practice for the initial migration phase.[1]

In a hybrid key exchange, both a classical algorithm (e.g., ECDH) and a post-quantum algorithm (e.g., Kyber) are used in parallel. The public keys for both are exchanged, and the two resulting shared secrets are combined (typically by hashing them together) to produce the final session key.[1]

This approach offers a powerful security property: the connection remains secure as long as *at least one* of the constituent algorithms is secure.

- If a catastrophic flaw is discovered in the new PQC standard, the classical ECDH algorithm still protects the connection from classical adversaries.
- If a CRQC arrives sooner than expected, the PQC Kyber algorithm protects the connection from quantum adversaries.

This "belt and suspenders" strategy provides a low-risk, robust bridge to a quantum-safe future, allowing organizations to deploy and test PQC in production environments without abandoning the proven security of classical cryptography prematurely.[1]

5.3 A Phased Migration Timeline: From Cryptographic Inventory to Full Sunset of Classical Algorithms

The global PQC migration will not be a single event but a gradual, multi-year process. Synthesizing roadmaps from various national and international bodies, a coherent four-phase timeline emerges.[38]

1. **Phase 1: Preparation & Discovery (Now - 2026):** This initial phase focuses on planning and assessment. Organizations must establish a PQC migration team, begin the critical task of creating a comprehensive cryptographic inventory, identify the data and systems most at risk from HNDL attacks, and develop a strategic migration plan.[39]
2. **Phase 2: Planning & Hybrid Execution (2026 - 2031):** During this phase, organizations will begin executing their plans. This involves engaging with technology vendors to understand their PQC roadmaps, conducting pilot deployments of hybrid cryptographic solutions on high-priority systems, and performing extensive interoperability testing.[39]
3. **Phase 3: PQC-Primary Transition (2031 - 2035):** In this phase, the ecosystem will shift to a "PQC-first" posture. PQC-only algorithms will become the default for new deployments, and support for classical public-key algorithms will be deprecated. The migration of most critical systems should be completed by the end of this period.[40]
4. **Phase 4: Monitoring & Evaluation (Ongoing):** This final phase involves the full sunset and decommissioning of legacy classical algorithms. However, the work is not finished. Organizations must continuously monitor the cryptographic landscape for new threats, maintain their systems, and be prepared for future cryptographic transitions.[39]

The ultimate lesson of the quantum threat is that any security based on a single class of computational assumptions is inherently temporary. The transition from RSA/ECC to PQC is merely the current iteration of a cycle that will likely repeat. Therefore, the strategic goal of this migration should not be simply to replace one set of static algorithms with another, but to re-architect systems to achieve *cryptographic agility*—the ability to swap out cryptographic primitives quickly and with minimal disruption.[1] The PQC migration is a painful but necessary forcing function to build this crucial, long-term resilience into our global digital infrastructure.

6. Conclusion: Navigating the Post-Quantum Transition

The advent of quantum computing marks a pivotal moment in the history of cryptography. The transition to a quantum-resistant cryptographic infrastructure is not a matter of if, but when and how. The analysis presented in this report, synthesizing foundational research and current policy, distills this complex challenge into a set of core conclusions and an urgent call to action.

6.1 Seven Foundational Insights on the Nature of the Quantum Threat

The research and analysis converge on seven foundational truths that must guide the global response to the quantum threat:

1. **Mathematics is Destiny:** The vulnerability of RSA and ECC is not a software bug to be patched but a consequence of mathematical fact. Shor's algorithm proves they are insecure against a quantum adversary; no amount of engineering can change this.[1]
2. **Efficiency Against One Adversary Can Be Vulnerability Against Another:** The migration to ECC, driven by classical performance benefits, offered no advantage against the quantum threat. Optimizing for today's threat model can create a catastrophic liability against tomorrow's.[1]
3. **The Attack is Happening Now:** Through "Harvest Now, Decrypt Later" attacks, adversaries are currently collecting data that will be decrypted in the future. The compromise begins today, even if the breach materializes in a decade.[1]
4. **Migration Takes Longer Than the Threat Timeline:** A full global migration to PQC will take 10-15 years. Waiting for a CRQC to appear before starting the transition guarantees failure, as the vulnerable data will have already been harvested.[1]
5. **Lattices Offer Hope, Not Certainty:** Lattice-based cryptography is our best defense, backed by strong theoretical arguments. However, it is a newer field than number-theoretic cryptography, and history teaches that no cryptographic assumption

should be considered permanent.[1]

6. **The Harvest-Decrypt Window Threatens Data Already Encrypted:** Any data requiring confidentiality beyond the projected 15- to 30-year arrival of a CRQC is already at risk. This creates an immediate need to protect long-lived secrets.[1]
7. **This is an Infrastructure Challenge, Not Just a Technical Problem:** The mathematics of PQC are largely solved. The true bottleneck is the immense technical, economic, and organizational challenge of deploying it at a global scale.[1]

6.2 The Path Forward: A Call for Immediate Action and Long-Term Vigilance

The path forward requires a dual focus on immediate, pragmatic action and long-term strategic vision.

- **For Organizations:** The first steps are non-negotiable and must begin now:
    1. **Cryptographic Inventory:** You cannot protect what you do not know you have. A comprehensive inventory of all systems using public-key cryptography is the mandatory starting point.[1]
    2. **Data Classification and Risk Assessment:** Identify data with long-term confidentiality requirements and prioritize systems for migration based on the HNDL threat.[1]
    3. **Begin Hybrid Deployments:** Engage with vendors and start pilot projects to test and deploy hybrid cryptographic solutions, building expertise and uncovering integration challenges early.[1]
- **For Policymakers and the Broader Ecosystem:**
    1. **Establish Clear Mandates:** Government and regulatory bodies must set clear and firm migration deadlines to overcome organizational inertia.[1]
    2. **Promote Cryptographic Agility:** The focus must be on building systems that can adapt to the next cryptographic threat, not just the current one.[1]
    3. **Invest in Continuous Research:** The security of our new PQC standards must be constantly scrutinized through public cryptanalysis to build confidence and uncover potential weaknesses before they can be exploited.

The question is not whether quantum computers will break our encryption—they mathematically will. The critical question is whether we will complete the global migration to quantum-resistant cryptography before adversaries decrypt the data they are harvesting today. The clock is ticking.[1]

References

[List of references from the source document would be formatted here.]

Appendices

Appendix A: Glossary of Terms and Mathematical Notation

Table 6: Glossary of Key Terms [1]

Term	Definition
CRQC	Cryptographically-Relevant Quantum Computer: A quantum computer with sufficient scale and fault tolerance to break current public-key algorithms like RSA-2048.
ECC	Elliptic Curve Cryptography: A type of public-key cryptography based on the algebraic structure of elliptic curves over finite fields.
HNDL	Harvest Now, Decrypt Later: An attack model where adversaries collect encrypted data today for decryption in the future with a CRQC.
KEM	Key Encapsulation Mechanism: A cryptographic technique used to securely

	establish a shared secret key over an insecure channel.
Lattice	A regular, periodic arrangement of points in n-dimensional space. The basis for the leading PQC candidates.
LWE	Learning With Errors: A hard mathematical problem, based on solving noisy systems of linear equations, that forms the security basis for Kyber and Dilithium.
NIST	National Institute of Standards and Technology: The U.S. agency responsible for developing and standardizing cryptographic algorithms.
PQC	Post-Quantum Cryptography: Cryptographic algorithms believed to be secure against attack by both classical and quantum computers.
QFT	Quantum Fourier Transform: The core quantum subroutine in Shor's algorithm used for efficient period-finding.
RSA	Rivest-Shamir-Adleman: A public-key cryptosystem based on the presumed difficulty of factoring large integers.
SVP	Shortest Vector Problem: A computationally hard problem on lattices that involves finding the shortest non-zero vector.

Appendix B: Comparative Analysis of Cryptographic Algorithms

Table 7: Master Algorithm Comparison [1]

Algorithm	**Type**	**Public Key Size (bytes)**	**Output / Signature Size (bytes)**	**Relative Speed**	**Quantum-Safe**	**Conservatism**
RSA-2048	Signature	256	256	Fast	❌ No	N/A
ECDSA-256	Signature	64	64	Very Fast	❌ No	N/A
Dilithium 3	Signature	1,952	3,293	Fast	✅ Yes	Medium
SPHINCS+-128	Signature	32	7,856	Slow	✅ Yes	High
FALCON-512	Signature	897	666	Fast	✅ Yes	Medium
ECDH (P-256)	KEM	32	32 (shared secret)	Very Fast	❌ No	N/A
Kyber-768	KEM	1,184	1,088 (ciphertext)	Fast	✅ Yes	Medium
Classic McEliece	KEM	1,357,824	256 (ciphertext)	Fast	✅ Yes	Very High

Works cited

1. Module-Lattice-Based Key-Encapsulation Mechanism Standard, accessed October 19, 2025, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.203.pdf
2. FIPS 204, Module-Lattice-Based Digital Signature Standard | CSRC, accessed October 19, 2025, https://csrc.nist.gov/pubs/fips/204/final
3. Migration to Post-Quantum Cryptography - NIST NCCoE, accessed October 19, 2025, https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
4. How Will Lattice-Based Cryptography Protect Us from Quantum Computers? - BTQ, accessed October 19, 2025, https://www.btq.com/blog/how-will-lattice-based-cryptography-protect-us-from-quantum-computers
5. Challenges for NIST PQC Adoption - Quantum Xchange, accessed October 19, 2025, https://quantumxc.com/featured/nist-pqc-adoption-challenges/
6. 4-Sight: How to Prepare Your Organization for Post-Quantum ..., accessed October 19, 2025, https://www.keyfactor.com/blog/4-sight-how-to-prepare-your-organization-for-post-quantum-cryptography/
7. Quantum-Readiness: Migration to Post-quantum Cryptography | AHA, accessed October 19, 2025, https://www.aha.org/fbi-tlp-alert/2023-08-23-quantum-readiness-migration-post-quantum-cryptography
8. NSAs Cybersecurity Perspective on Post Quantum Cryptography Algorithms, accessed October 19, 2025, https://www.nsa.gov/Cybersecurity/NSAs-Cybersecurity-Perspective-on-Post-Quantum-Cryptography-Algorithms/
9. Lattice-based cryptography - Wikipedia, accessed October 19, 2025, https://en.wikipedia.org/wiki/Lattice-based_cryptography
10. Lattice-Based Post-Quantum Public Key Encryption Scheme Using ElGamal's Principles, accessed October 19, 2025, https://www.mdpi.com/2410-387X/8/3/31
11. What is Lattice-Based Cryptography? A Beginner's Guide to Post ..., accessed October 19, 2025, https://www.ssh.com/academy/what-is-lattice-based-cryptography-beginners-guide-to-post-quantum-security
12. Post-quantum cryptography: Lattice-based cryptography - Red Hat, accessed October 19, 2025, https://www.redhat.com/en/blog/post-quantum-cryptography-lattice-based-cryptography
13. Why is lattice-based cryptography believed to be hard against quantum

computer?, accessed October 19, 2025, https://crypto.stackexchange.com/questions/50856/why-is-lattice-based-cryptography-believed-to-be-hard-against-quantum-computer

14. Evaluation and Comparison of Lattice-Based Cryptosystems for a Secure Quantum Computing Era - MDPI, accessed October 19, 2025, https://www.mdpi.com/2079-9292/12/12/2643
15. Learning with errors - Wikipedia, accessed October 19, 2025, https://en.wikipedia.org/wiki/Learning_with_errors
16. Learning with Errors (LWE): The Foundation of Post-Quantum Cryptography - Medium, accessed October 19, 2025, https://medium.com/@kootie73/learning-with-errors-lwe-the-foundation-of-post-quantum-cryptography-f85ec40c5840
17. The Learning with Errors Problem, accessed October 19, 2025, https://cims.nyu.edu/~regev/papers/lwesurvey.pdf
18. Learning with Errors: A Lattice-Based Keystone of Post-Quantum Cryptography - MDPI, accessed October 19, 2025, https://www.mdpi.com/2624-6120/5/2/12
19. Learning with errors: Encrypting with unsolvable equations - YouTube, accessed October 19, 2025, https://www.youtube.com/watch?v=K026C5YaB3A
20. Kyber - Wikipedia, accessed October 19, 2025, https://en.wikipedia.org/wiki/Kyber
21. Kyber - CRYSTALS, accessed October 19, 2025, https://pq-crystals.org/kyber/
22. www.ibm.com, accessed October 19, 2025, https://www.ibm.com/docs/en/zos/2.5.0?topic=cryptography-crystals-dilithium-digital-signature-algorithm#:~:text=CRYSTALS%2DDilithium%20is%20a%20lattice,Algebraic%20Lattices)%20suite%20of%20algorithms.
23. ML-DSA, CRYSTALS-Dilithium Digital Signature Algorithm - IBM, accessed October 19, 2025, https://www.ibm.com/docs/en/zos/3.1.0?topic=cryptography-ml-dsa-crystals-dilithium-digital-signature-algorithm
24. Dilithium - CRYSTALS, accessed October 19, 2025, https://pq-crystals.org/dilithium/
25. CRYSTALS-Dilithium: The Digital Signature Scheme for the Post-Quantum Era | by Denys Popov | Aug, 2025 | Medium, accessed October 19, 2025, https://denispopovengineer.medium.com/crystals-dilithium-the-digital-signature-scheme-for-the-post-quantum-era-d8ba8f0213b9
26. Microsoft outlines ambitious post-quantum plans, but challenges remain | The Strategist, accessed October 19, 2025, https://www.aspistrategist.org.au/microsoft-outlines-ambitious-post-quantum-plans-but-challenges-remain/
27. Post-Quantum Cryptography: Migration Challenges for Embedded Devices - NXP Semiconductors, accessed October 19, 2025, https://www.nxp.com/docs/en/white-paper/POSTQUANCOMPWPA4.pdf
28. Untold Challenge of Post-Quantum Cryptography Migration | Fortanix, accessed October 19, 2025, https://www.fortanix.com/blog/untold-challenge-of-post-quantum-cryptography-migration

29. 2024-2025 CRA Quad Paper: The Post-Quantum Cryptography Transition: Making Progress, But Still a Long Road Ahead - Computing Research Association, accessed October 19, 2025, https://cra.org/wp-content/uploads/2025/01/2024-2025-CRA-Quad-Paper_-The-Post-Quantum-Cryptography-Transition_-Making-Progress-But-Still-a-Long-Road-Ahead.pdf
30. White House: Agencies Need $7.1B to Transition to PQC – MeriTalk, accessed October 19, 2025, https://www.meritalk.com/articles/white-house-agencies-need-7-1b-to-transition-to-pqc/
31. White House Report: U.S. Federal Agencies Brace for $7.1 Billion Post-Quantum Cryptography Migration, accessed October 19, 2025, https://thequantuminsider.com/2024/08/12/white-house-report-u-s-federal-agencies-brace-for-7-1-billion-post-quantum-cryptography-migration/
32. Moody's sounds alarm on quantum computing risk, as transition to PQC 'will be long and costly' - Industrial Cyber, accessed October 19, 2025, https://industrialcyber.co/reports/moodys-sounds-alarm-on-quantum-computing-risk-as-transition-to-pqc-will-be-long-and-costly/
33. REPORT ON POST-QUANTUM CRYPTOGRAPHY - Biden White House, accessed October 19, 2025, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf
34. Organizational Quantum Readiness Remains Low: Poll Finds Only 5% of Organizations Have A Quantum Computing Roadmap, accessed October 19, 2025, https://thequantuminsider.com/2025/04/28/organizational-quantum-readiness-remains-low-poll-finds-only-5-of-organizations-have-a-quantum-computing-roadmap/
35. A CISO's guide to post-quantum readiness: How to build crypto ..., accessed October 19, 2025, https://www.cyberark.com/resources/blog/a-cisos-guide-to-post-quantum-readiness-how-to-build-crypto-agility-now
36. What is hybrid post-quantum encryption? - QCVE.org, accessed October 19, 2025, https://qcve.org/blog/what-is-hybrid-post-quantum-encryption
37. PQC Migration Roadmap - Post-Quantum Cryptography Coalition |, accessed October 19, 2025, https://pqcc.org/post-quantum-cryptography-migration-roadmap/
38. Post-Quantum Cryptography (PQC) Migration Roadmap, accessed October 19, 2025, https://pqcc.org/wp-content/uploads/2025/05/PQC-Migration-Roadmap-PQCC-2.pdf
39. Cyber chiefs unveil new roadmap for post-quantum cryptography migration, accessed October 19, 2025, https://www.ncsc.gov.uk/news/pqc-migration-roadmap-unveiled
40. The EU's Roadmap for Post-Quantum Cryptography - Utimaco, accessed

October 19, 2025, https://utimaco.com/news/blog-posts/eus-roadmap-post-quantum-cryptography

41. Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001) - Canadian Centre for Cyber Security, accessed October 19, 2025, https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001
42. Post-Quantum Cryptography Coalition Unveils PQC Migration Roadmap | MITRE, accessed October 19, 2025, https://www.mitre.org/news-insights/news-release/post-quantum-cryptography-coalition-unveils-pqc-migration-roadmap
43. Post-Quantum Crypto Agility - Thales, accessed October 19, 2025, https://cpl.thalesgroup.com/encryption/post-quantum-crypto-agility