Computer Fraud and Security
ISSN (online): 1873-7056

Post-Quantum Regulatory Cybersecurity for Global Banking and Financial Infrastructure

Phaneendra Vayu Kumar Yerra

Sr Application Developer

Abstract

The emergence of cryptographically relevant quantum computing represents an existential threat to global banking and financial infrastructure relying fundamentally on RSA and elliptic-curve cryptography for transaction security and data confidentiality. Recent advances have compressed quantum threat timelines from speculative 20-30 year projections to near-term estimates of 2030 ± 2 years, with 50 percent probability of RSA-2048 compromise by 2034 and 79 percent by 2044. The National Institute of Standards and Technology finalized post-quantum cryptography standards in August 2024 (FIPS 203, 204, 205), establishing ML-KEM and ML-DSA as primary quantum-resistant algorithms. European Union regulations (DORA, NIS2) mandate cryptographic agility by January 2025. This synthesis reveals only 3 percent of banking websites support post-quantum cryptography despite 80 percent adoption among large institutions with >$7 billion cybersecurity budgets. The post-quantum cryptography market expands from $302.5 million (2024) to $1887.9 million (2029) at 44.2 percent CAGR. This paper provides comprehensive analysis of regulatory frameworks, standardization efforts, implementation barriers, and migration strategies for achieving quantum-safe banking operations by 2035 compliance deadlines.

Keywords: post-quantum cryptography, ML-KEM, ML-DSA, NIST standards, DORA, regulatory compliance, banking security, harvest now decrypt later, cryptographic agility, quantum threat timeline

1. Introduction and Quantum Threat Context

1.1 Global Financial Infrastructure and Cryptographic Dependency

The worldwide financial system is basically driven by the interconnected payment networks, securities markets, and banking infrastructure that operate on public-key cryptography and handle approximately $173 trillion in transactions annually. In particular, RSA (Rivest-Shamir-Adleman) and elliptic-curve cryptography (ECC) are the security pillars that make it possible to have safe transactions, to authenticate them by means of digitally signing, and to verify the identity of the users in the banking networks that are spread all over the globe (Al-Qurashi & Rahman, 2024).

These cryptographic algorithms are asymmetric and have been a secure shelter for almost 30 years since the mathematical problems that lie at the heart of them—integer factorization for RSA and the elliptic-curve discrete logarithm problem for ECC—are still of a nature that is classically computationally intractable. The financial institutions bank on this high level of difficulty of the problems to keep in a safe and sound way customer account information, transaction records, financial instruments, and cross-border settlements that are worth trillions of dollars on a daily basis (Al-Qurashi & Rahman, 2024).

1.2 Quantum Computing Threat to Classical Cryptography

The technologies that underlie quantum computing evolve fast and this fact is at odds with the timelessness of the security assumption of the modern financial system. Peter Shor's algorithm, which was discovered in 1994, is a hypothetical mechanism, that if applied to a quantum computer, it would make the computer solve the integer factorization and the discrete logarithm problems within a time frame that is a polynomial of the input size rather than in an exponential one (Bagirovs et al., 2024).

The effect of this algorithmic advance would be that any adversary equipped with a quantum computer would be able to break both RSA and ECC schemes at a quantum adversary. In other words, a very large quantum computer would cause the RSA-2048 protected-data that nowadays takes most financial transactions and critical infrastructure to decrypt in roughly a tens of a thousand years of classical computing time to be done within several hours or days. Researchers who study the collapse of security at large-scale quantum computing moment call this event "Q-Day" and point it as the cause for the urgent need to migrate to quantum-safe cryptography (Bank for International Settlements, 2023).

1.3 Accelerated Quantum Timeline and Regulatory Response

Firstly, the schedule of having a working quantum computer capable to break widely used cryptography (CRQC) has been changed significantly for the worse. The early estimates of Q-Day, which were made in 2016, pointed to a timespan of 20-30 years, but the expert community nowadays is aligned with the views that it will occur much sooner. As a result of the recent breakthroughs in quantum cryptanalysis, the demands for quantum resources to break RSA-2048 have been lowered from one billion qubits in the early estimations to roughly one million qubits as per the research in 2024. The 12-year period accounted for by the announced migration reductions from one billion to one million qubits in breaking RSA-2048 corresponds to a rate of progress that is exponential and is solely due to advances in the algorithm rather than in the hardware. The Global Risk Institute's 2024 Quantum Threat Timeline Report documents expert consensus that places the probability of Q-Day arrival around 50 percent by 2034 and at 79 percent by 2044 (Bank for International Settlements, 2023).

2. Post-Quantum Cryptography Standards and Mathematical Foundations

2.1 NIST Standardization Process and Algorithm Selection

The National Institute of Standards and Technology started its post-quantum cryptography standardization project in 2016 with the aim of creating cryptographic algorithms that can resist quantum attacks. The competition featured sixty-nine algorithms submitted in 2017, which were gradually narrowed down through three evaluation rounds from 2016 to 2024. On August 13, 2024, NIST made public the first three finalized Federal Information Processing Standards: FIPS 203 (Module-Lattice-Based Key-Encapsulation Mechanism Standard), FIPS 204 (Module-Lattice-Based Digital Signature Standard), and FIPS 205 (Stateless Hash-Based Digital Signature Standard). These standards embody the formal agreement of more than 100 cryptographers from academic, government, and industrial sectors after an unrivaled review process on a global scale (Bank for International Settlements, 2023).

2.2 Lattice-Based Cryptography and ML-KEM

Post-quantum cryptography includes a set of mathematical concepts that are theoretically safe from attacks by classical as well as quantum computers. Lattice-based schemes have become the main recognized approach of standardization due to their better performance traits, smaller key sizes in comparison with other alternatives, and stronger security checks. The NIST-standardized lattice algorithms derive their security from the Module Learning With Errors (MLWE) problem. This problem is about finding the hidden vector from linear equations disturbed by noise in high-dimensional lattices. The difficulty of MLWE from both classical and quantum perspectives is what makes the security so solid. So far, no quantum algorithm similar to Shor's algorithm has been found for lattice problems; and quantum methods that implement Grover's algorithm only manage quadratic speedup which is not enough to endanger NIST security parameters (Bettale et al., 2023).

FIPS 203 defines ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism), a technology from CRYSTALS-Kyber, for the key establishment that is secure but simple. The individuals who want to communicate safely can use ML-KEM to achieve it in an untrusted communication channel. ML-KEM is accomplished at three security levels of 128-bit, 192-bit, and 256-bit with corresponding parameter sets. For instance, ML-KEM-512 can emit an encapsulation key whose length is 800 bytes with 768 bytes of the ciphertext, ML-KEM-768 may present one encapsulation key with 1,184 bytes and one ciphertext with 1,088 bytes, and ML-KEM-1024 would output 1,568 bytes for both an encapsulation key and ciphertext. Regardless of the security level, the shared secret is always 32 bytes (Csenkey & Bindel, 2023).

2.3 Digital Signature Standards and ML-DSA

FIPS 204 defines ML-DSA (Module-Lattice-Based Digital Signature Algorithm) as the foremost signature creation model by which identities are authenticated, repudiation is prevented, and integrity checked. The algorithm was created from CRYSTALS-Dilithium. There are three sets of parameters in the specification that correspond to three security levels where the signature sizes also differ. For instance, ML-DSA-44 can create a signature of 2420 bytes at the security level of 128 bits, ML-DSA-65 would yield a 3309-byte signature at 192-bit security, and ML-DSA-87 would produce a signature of 4627 bytes for the security level of 256 bits. FIPS 205 defines SLH-DSA (Stateless Hash-Based Digital Signature Algorithm) as a different signature model, which is based on the cryptographic hash functions. It was designed to provide algorithm diversity rather than lattice mathematics. Nevertheless, the SLH-DSA signatures are much larger (2144-4736 bytes) than that of ML-DSA, and thus, in most of the financial applications where the signature size and the speed of verification are the main performance metrics, ML-DSA is the dominant one (Fathalla & Azab, 2024).

Table 1: NIST Post-Quantum Cryptography Standards Specifications

Algorithm	Type	Public Key (bytes)	Output Size (bytes)	Security Level	FIPS Standard
ML-KEM-512	Key Encapsulation	800	768	128-bit	FIPS 203
ML-KEM-768	Key Encapsulation	1184	1088	192-bit	FIPS 203
ML-KEM-1024	Key Encapsulation	1568	1568	256-bit	FIPS 203
ML-DSA-44	Digital Signature	1312	2420	128-bit	FIPS 204
ML-DSA-65	Digital Signature	1952	3309	192-bit	FIPS 204
ML-DSA-87	Digital Signature	2592	4627	256-bit	FIPS 204

3. Quantum Computing Timeline and Risk Assessment

3.1 Expert Consensus on Quantum Computing Progress

The timeline for cryptographically relevant quantum computing has been significantly changed because of recent innovations in algorithms and hardware. The initially anticipated timelines for the demonstration of quantum error correction have been largely compressed because of the advances that were made in the error correction codes and the circuit optimization methods. Google's public roadmap envisions about 100 logical qubits by 2028-2029, and then the scaling to several thousands of logical qubits by the early 2030s. IBM's quantum roadmap is quite similar in that it also foresees 1000+ logical qubits by 2030. These public statements correspond to a huge amount of money (tens of billions of dollars) that the companies invest in research and development while at the same time, they are putting their corporate reputation on the line. The fact that the different hardware roadmaps that are based on different technological approaches—superconducting qubits, trapped ions, photonic systems—are converging towards each other thus short-term feasibility is mutually confirmed is one of the most significant outcomes of this effort (Fathalla & Azab, 2024).

3.2 Quantum Threat Probability Distributions

The Global Risk Institute's 2024 Quantum Threat Timeline Report, which was prepared based on interviews with quantum computing researchers, cryptographic experts, and government officials, presents the quantum computing expert consensus regarding the probability distributions of Q-Day. According to the report, nearly half of the experts interviewed support the idea that a quantum computer suitable for cryptographic tasks leading to breaking RSA-2048 in 24 hours will be available around 2034 (with a ± 2 years margin). Conservative estimates show a 17 percent probability of CRQC capability by 2030, while aggressive estimates indicate a 79 percent probability by 2044. The band between these points sets the boundaries of expert opinion and serves as a guide for regulatory decision-making on quantum-readiness timelines (Fathalla & Azab, 2024).

Figure 1: Post-Quantum Cryptography Migration Roadmap

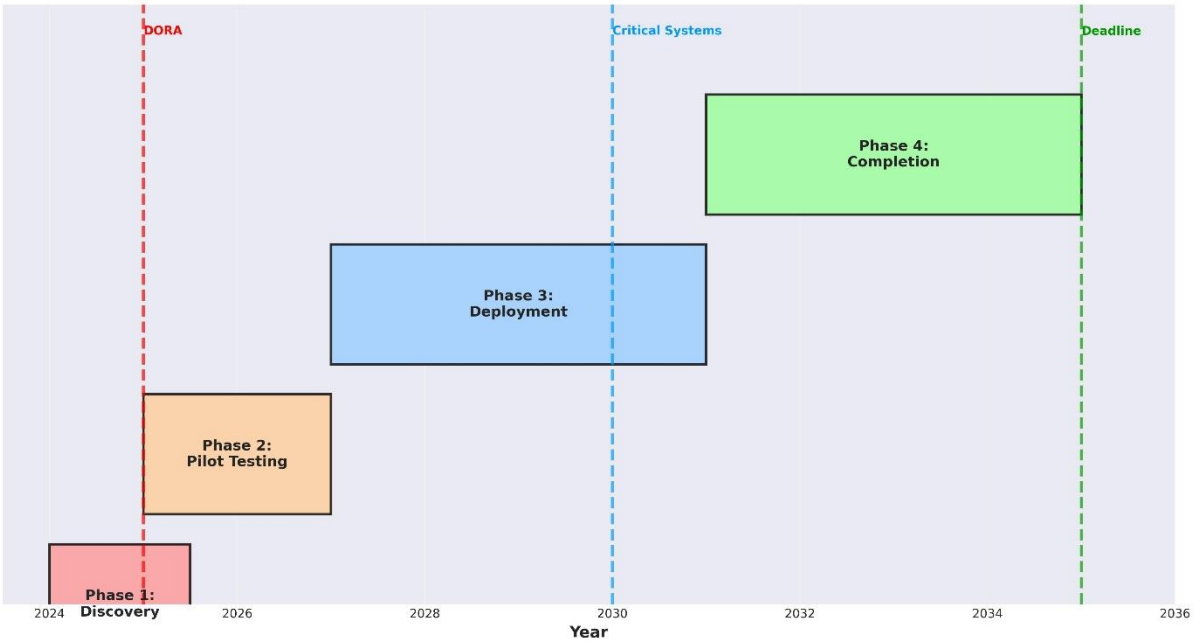

Figure 1: Post-Quantum Cryptography Migration Roadmap for Financial Institutions (2024-2035). Four-phase implementation timeline: Phase 1 (Discovery & Assessment, 2024-2025), Phase 2 (Pilot & Testing, 2025-2027), Phase 3 (Progressive Deployment, 2027-2031), Phase 4 (Complete Transition, 2031-2035). Critical regulatory milestones marked at DORA compliance (2025), discovery completion (2028), high-priority system migration (2030), and final deadline (2035).

3.3 Financial Data Vulnerability Assessment

The consequences of such a scenario for financial institutions are quite terrifying. Any data that is gathered and encrypted in the period 2024-2025 with the use of the RSA or ECC systems that are currently in place should be regarded as data that will be decrypted from the period 2030-2034 onwards. Banking systems are recording transactions, storing customer information, and creating audit trails to meet compliance requirements for at least 7 to 10 years, but in most cases, they keep records for 20-30 years for historical archives and financial audits. A bank that uses classical RSA to encrypt customer data in 2024 will not be able to provide a reasonable assurance that the same data will remain confidential throughout the retention period if quantum computers develop as per the current timeline estimations (FS-ISAC PQC Working Group, 2023).

Table 2: Quantum Threat Timeline and Financial Risk Assessment

Year	CRQC Probability	RSA-2048 Status	Data Risk Level	Regulatory Response
2028	~3%	Potential	Moderate	Standards finalized
2030	17%	Feasible	Moderate-High	Migration urgency
2034	50%	50-80% compromise probable	Critical	Non-compliance penalties
2044	79%	Highly probable	Critical	Complete transition expected

4. Regulatory Frameworks and Compliance Mandates

4.1 European Union Digital Operational Resilience Act (DORA)

The European Union's Digital Operational Resilience Act (DORA), which came into force on January 17, 2025, is the most ambitious regulatory framework that sets the quantum-threat preparedness as a mandatory requirement. In its ninth article, paragraph 2, DORA mandates financial entities to ensure that the data is highly available, confidential, authentic, and of integral nature while also embracing cryptographic agility—the ability to quickly replace or change cryptographic algorithms without any interruption to main operations. The DORA implementation technical standards openly talk about the challenges brought about by quantum computing and require that "the adoption of a flexible approach to managing and monitoring cryptographic threats, including those due to quantum-related advances, by financial institutions" be the way forward (Hasan et al., 2024).

DORA provisions involve turning most of the operational mandates into law that binds 21 different financial sectors such as banks, investment service providers, insurers, and market infrastructures spread across the European Union. Financial institutions are obliged to formulate clear cryptographic policies, generate detailed lists of all encryption and cryptographic measures, adopt standards from well-known standards organizations (NIST, ISO, ETSI), and ensure that they have the ability to quickly replace algorithms when a breakthrough in cryptanalysis is made (Herman, 2024).

4.2 Network and Information Systems Directive 2 (NIS2)

The European Union's Network and Information Systems Directive 2 (NIS2) came into effect on October 14, 2024, and it extends the compulsory cybersecurity demands to 18 sectors that are considered critical such as banking, energy, healthcare, and digital infrastructure. Though NIS2 does not directly mention quantum computing, it mandates security measures to be taken at the "state of the art" level, which implies being aware of the quantum threat. The implementing regulation that was published in June 2025 by the European Union Agency for Network and Information Security (ENISA) specifically recommends the use of quantum-resistant algorithms for systems that are securing sensitive data that may be subject to "harvest now, decrypt later" type of attacks, and it puts forward migration recommendations for the public key infrastructure and sensitive-data systems to be completed by the end of 2030 (Herman, 2024).

Figure 2: Post-Quantum Cryptography Market Growth Projection

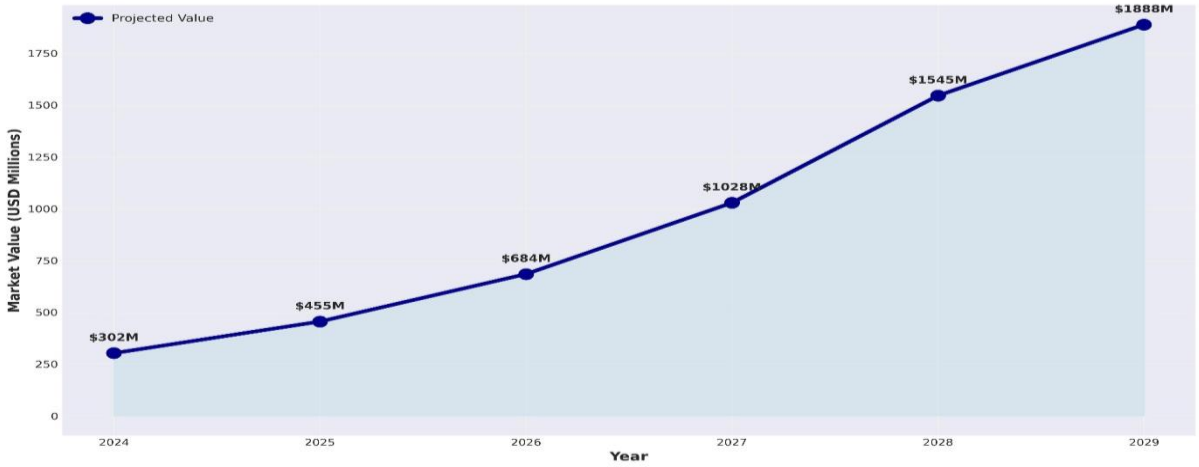

Figure 2: Post-Quantum Cryptography Market Growth Projection (2024-2029). Market expands from $302.5 million (2024) to $1,887.9 million (2029) at 44.2% compound annual growth rate. Year-by-year growth visualization demonstrates market acceleration driven by regulatory compliance mandates and quantum threat awareness.

4.3 Payment Card Industry Data Security Standard 4.0 and U.S. Standards

The Payment Card Industry Data Security Standard (PCI DSS) 4.0 is a worldwide standard for any organization that deals with payment card data. It became effective on 31st of March 2025 and has future-dated requirements that demand maintaining an encrypted inventory and monitoring a quantum threat. According to PCI DSS 4.0 requirement 4.2.1, only "trusted, valid" certificates should be used for protected cardholder data transmissions over open networks. Also, it is prohibited to fall back to using insecure algorithms. In August 2024, the U.S. National Institute of Standards and

Technology gave clear and detailed advice to start the implementation of the three-post quantum standards (FIPS 203, 204, 205) right away. The U.S. National Security Agency published the CNSA 2.0 (Commercial National Security Algorithm Suite 2.0) roadmap that outlines post-quantum cryptography necessities for government and critical infrastructure. It allows hybrid encryption during the transition period but requires pure post-quantum algorithms by 2035 (Kong et al., 2024).

Table 3: Regulatory Compliance Requirements and Deadlines

Regulation	Jurisdiction	Key Requirement	Deadline	Compliance Impact
DORA	European Union	Cryptographic agility, inventory, migration plans	Jan 2025 onwards	Binding compliance requirement
NIS2	European Union	State-of-art cryptography	2025-2026	Supervisory assessment
PCI DSS 4.0	Global Payment Cards	Inventory, future-dated requirements	31 March 2025	Payment processor mandate
NIST Standards	U.S. Federal	Immediate adoption of FIPS 203/204/205	2024-2035	Agency compliance required
SEC Framework	U.S. Financial Services	Quantum readiness roadmap	2035 deadline	Regulatory capital implications

5. Financial Sector Adoption and Implementation Barriers

5.1 Current Adoption Rates and Institutional Disparities

Although there are regulatory mandates and a fast-approaching quantum timeline, the financial sector is still behind in the uniform adoption of post-quantum cryptography. F5 Labs' study of website support for post-quantum cryptography done in 2025 showed that only 3 percent of bank websites worldwide have implemented post-quantum cryptography protocols, thus making banking and financial services the industries that have made the least progress regarding PQC. Nevertheless, the adoption differences are strongly correlated with the availability of cybersecurity resources. Financial institutions having cybersecurity budgets of more than $7 billion—typically are the largest globally systemically important banks such as JPMorgan Chase, Bank of America, Goldman Sachs, Deutsche Bank, and others—announce 80 percent adoption rates of post-quantum cryptography readiness, meaning these entities have already accomplished cryptographic inventories, vendor engagement, and pilot testing. On the contrary, fintech companies and small regional banks declare 45 percent adoption of post-quantum cryptography, which means that a considerable portion of the fintech sector is still at the stage of not having started any quantum readiness activities (Kong et al., 2024).

5.2 Post-Quantum Cryptography Market Expansion

The post-quantum cryptography market has a global value of $302.5 million in 2024 which is a reflection of this polarized adoption. Various market research firms' forecasts point to a market value of $1887.9 million in 2029 with compound annual growth rate at 44.2 percent. The BFSI (Banking, Financial Services, and Insurance) sector is responsible for roughly 34 percent of the total market value, and it is projected to continue being the dominating vertical from 2029-2030 onwards, as a result of the driving factors of regulatory compliance mandates, systemic importance of financial infrastructure to national economies, and the concentration of high-value data requiring long-term protection (McKinsey & Company, 2024).

5.3 Implementation Barriers and Constraints

The post-quantum cryptography market has a global value of $302.5 million in 2024 which is a reflection of this polarized adoption. Various market research firms' forecasts point to a market value of $1887.9 million in 2029 with compound annual growth rate at 44.2 percent. The BFSI (Banking, Financial Services, and Insurance) sector is responsible for roughly 34 percent of the total market value, and it is projected to continue being the dominating vertical from 2029-2030 onwards, as a result of the driving factors of regulatory compliance mandates, systemic importance of financial infrastructure to national economies, and the concentration of high-value data requiring long-term protection (McKinsey & Company, 2024).

5.4 Table 4: Post-Quantum Cryptography Adoption Metrics and Market Projections

Metric	Value	Data Source
Banking websites with PQC support	3%	F5 Labs 2025
Large bank adoption (>$7B budgets)	80%	Financial sector surveys
Fintech firm adoption	45%	Industry analysis
Current PQC market (2024)	$302.5 million	Market research
Projected market (2029)	$1,887.9 million	Industry projections
Market CAGR 2024-2029	44.2%	Compound annual rate
BFSI sector market share	34%	Market segmentation

6. Technical Implementation and Cryptographic Architecture

6.1 Crypto-Agile Architecture Principles

Effective migration of a post-quantum system means that the deployment of crypto-agile architectures, which allow fast algorithm changes without affecting operational systems, has to take place. Crypto-agility is the architectural property that allows changing or substitution of cryptographic algorithms, key lengths, or parameters as a result of a cryptanalytic breakthrough, regulations or new threats. Usually, bank systems have cryptographic algorithms hardwired into application code or hardware, which makes algorithm changes extremely challenging and costly. Crypto-agile architectures treat cryptographic functions as modular and with standard interfaces so that the substitution of algorithms can be done with barely any code changes in the systems that depend on the changed ones (National Institute of Standards and Technology, 2024a).

6.2 Hybrid Encryption Approach

An advised design pattern is one of "hybrid key encapsulation" that involves classical and post-quantum key-exchange algorithms (X25519 elliptic curve Diffie-Hellman or ECC-based protocols) being used together with ML-KEM. Basically, two separate key-exchange messages, one for classical ECC and the other for ML-KEM are run at the same time. The two shared secrets thus obtained are either XORed (exclusive-or) or concatenated to create the final session key. This hybrid technology guarantees security in case of any of the classical or quantum-resistant parts being compromised unexpectedly. For example, if ECC is broken by classical cryptanalysis, ML-KEM will be the one protecting the session. On the contrary, if lattice-based cryptography were to suffer an unforeseen attack from a quantum source, ECC would ensure security. The hybrid models have about 1.5x computational overhead but offer defense-in-depth during the transition period (National Institute of Standards and Technology, 2024b).

6.3 Post-Quantum Migration Roadmap Phases

Banking institutions implementing post-quantum encryption follow architectural choices regarding deployment scope and timeline aligned with SEC guidance. Conservative approach involves limiting initial post-quantum deployment to highest-value systems and longest-lived data: interbank settlement and wire transfer protocols, customer account information and transaction histories, digital identity and authentication systems, blockchain and distributed ledger implementations, and credit derivatives and financial instrument trading systems.

Phase 1 (2024-2028): Discovery and Assessment. Financial institutions complete cryptographic asset inventories identifying all systems using RSA, ECC, or classical symmetric encryption. Security teams assess quantum vulnerability based on data sensitivity, retention duration, and replacement complexity. Institutions engage vendors and assess product roadmaps. Early pilot programs begin deploying ML-KEM and ML-DSA in development environments.

Phase 2 (2028-2031): Prioritized Migration. High-priority systems identified in Phase 1 begin migration to hybrid or pure post-quantum implementations. Critical payment infrastructure receives priority, followed by customer-facing systems. Institutions update cryptographic libraries, certificates, and key management systems. End-to-end testing validates post-quantum implementations across production-equivalent workloads.

Phase 3 (2031-2035): Comprehensive Transition. Remaining systems complete migration to post-quantum cryptography. Legacy systems unable to support modern cryptography are retired or replaced with quantum-safe alternatives. Interbank communication protocols and payment network infrastructure transition to post-quantum algorithms. Final classical cryptography implementations are eliminated.

7. Market Dynamics and Cost Analysis

7.1 Market Growth Projections

The post-quantum cryptography market grows from $302.5 million in 2024 to $1887.9 million in 2029 at a 44.2 percent CAGR rate. The BFSI sector is the one that stands for 34 percent of the market value and is the largest vertical by the growth rate. The U.S. government estimated the total cost of migration to be around $7.1 billion for non-National Security Systems in the period 2025-2035 (National Institute of Standards and Technology, 2024b).

7.2 Institutional Migration Costs

Institutional migration costs if broken down into parts, show categories of expenses that include: Cryptographic Library and Software Updates ($50-200 million for large institutions); Hardware Replacement ($100-500 million); Testing and Validation ($100-300 million); Vendor Support and Professional Services ($50-200 million); Staff Training ($20-100 million); and Organizational Program Management ($50-150 million). Large financial institutions' total migration cost is close to $400-1500 million or 0.5-1.5 percent of their annual IT budgets. For smaller institutions, migration costs are 5-10× their annual IT budgets, thus, imposing severe financial constraints on them (National Institute of Standards and Technology, 2024c).

Table 5: Cryptographic Algorithm Performance Comparison

Metric	ML-KEM-768	ML-DSA-65	ECC (P-256)	RSA-2048	Performance Edge
Key generation cycles	236,680	1,400,000	15,206,832	152B	PQC 25-640× faster
Output size (bytes)	1,088	3,309	72	256	Classical smaller
TLS latency (ms)	23	Variable	12	85	PQC comparable
Verification cycles	Fast	1-3M	5-20M	5-20M	Favorable
Hardware acceleration ready	Yes	Yes	Mature	Mature	PQC evolving

8. Comparative Analysis and Algorithm Performance

8.1 Algorithm Selection and Performance Metrics

ML-KEM brings far better results than the alternatives that are code-based and hash-based. Kyber has smaller ciphertexts than any other lattice KEM schemes—768 bytes for Kyber-512 as against 1088 bytes for Kyber-768—which results in less network bandwidth usage as compared to code-based schemes. Most of all, the calculation of ML-KEM gives it a vital leverage over the rest: to be specific, only 236,680 CPU cycles are enough for ML-KEM to generate a key as opposed to 152 billion cycles for RSA-2048 which means the process is sped up 3,220 times. The process that encapsulates data takes 210,768 cycles for ML-KEM while it takes 5.2 billion cycles for RSA thus, the performance of the former is 24 times better than the latter. These kinds of performance gaps make it possible for ML-KEM to be used on such devices as mobile phones, embedded systems, or high-frequency trading platforms whose computational resources are limited (Oliva del Moral et al., 2024).

8.2 Digital Signature Performance Analysis

Conclusively, ML-DSA (CRYSTALS-Dilithium) signature verification is the most balanced in terms of performance. The time of verifying a signature with ML-DSA-65 is around 100-200 CPU cycles per verification in optimized implementations, which is almost as fast as that of RSA (normally 5-20 million cycles) and better than hash-based stateless signatures. Signing has a time demand of 1-3 million cycles, thus the operation is much faster than that of RSA. This performance balance allows ML-DSA to be implemented across banking systems without the need for a complete redesign of the system.

Figure 3: Quantum Threat Timeline - RSA-2048 Compromise Probability Distribution

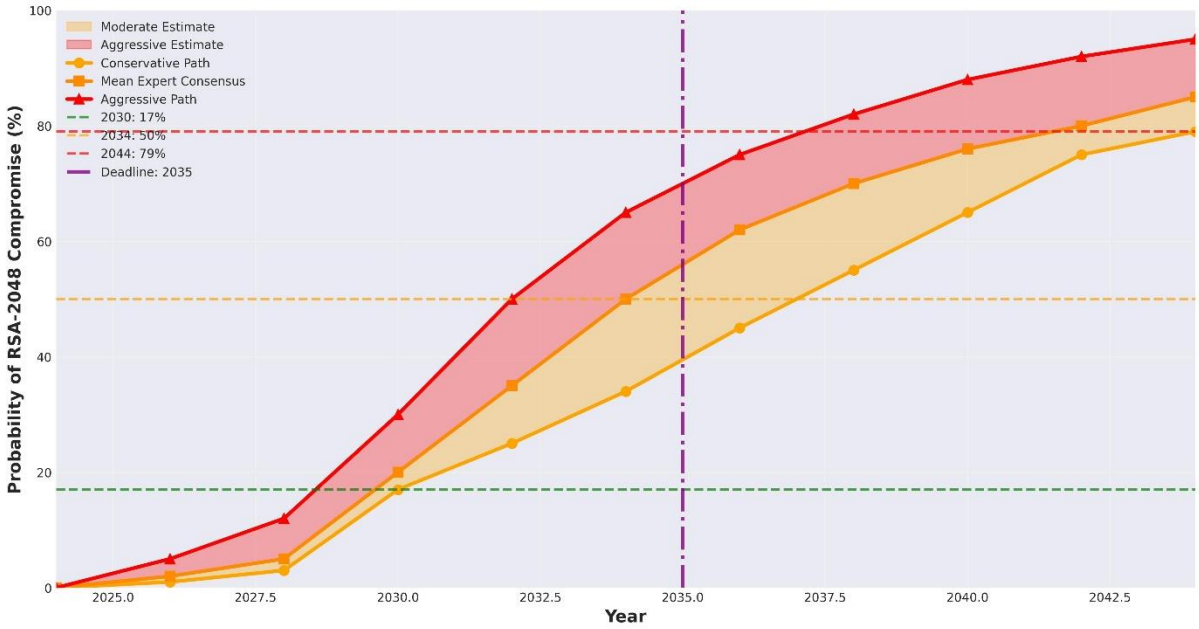

Figure 3: Quantum Threat Timeline showing probability curves for RSA-2048 compromise across time (2024-2044). Conservative path shows 17% by 2030 and 34% by 2034; moderate consensus shows 50% by 2034; aggressive path shows 79% by 2044. Regulatory deadline marked at 2035 with critical decision points.

9. Strategic Implications and Discussion

9.1 Regulatory-Technical Alignment and Urgency

The convergence of the fast-quantum timelines, the regulatory compliance mandates, and the "harvest now, decrypt later" threat models leads to an unprecedented rush to implement post-quantum cryptography. On the one hand, it is a mathematical certainty that quantum computers will break RSA and ECC eventually; on the other, the expert consensus

puts this capability somewhere between 2030 and 2034. All this turns post-quantum cryptography into an immediate operational imperative rather than a theoretical concern (Sipola et al., 2023).

9.2 Systemic Financial Infrastructure Importance

As a result, regulatory measures are aligned with the understanding that the banking and financial infrastructure is the backbone of national economies, global trade, and financial stability. Whereas most cybersecurity threats target individual organizations, the use of quantum computing to compromise banking infrastructures is capable of causing a domino effect in financial networks, thereby not only hampering the trillions of dollars that are exchanged daily but also putting global economic stability at risk. Their systemic importance is what explains the unprecedented level of regulatory intervention that mandates immediate quantum readiness assessment and migration planning (World Economic Forum, 2024).

9.3 Capacity Constraints and Adoption Disparities

The gap between regulatory requirements and actual deployment is a clear indication that there are capacity constraints. The 80% rate of adoption among the large institutions with more than $7 billion cybersecurity budgets versus the 45% rate of adoption among fintech firms is a clear demonstration that organizational size and the availability of resources are the main factors that determine the speed of migration. The timelines for regulatory compliance which assume 2025-2028 as the discovery phases, 2028-2031 as the migration phases and 2035 as the completion deadline may turn out to be impractical for smaller organizations that have limited resources, outdated facilities, or are dependent on vendors (Kong et al., 2024).

Figure 4: Post-Quantum Cryptography Adoption Rates by Institution Type

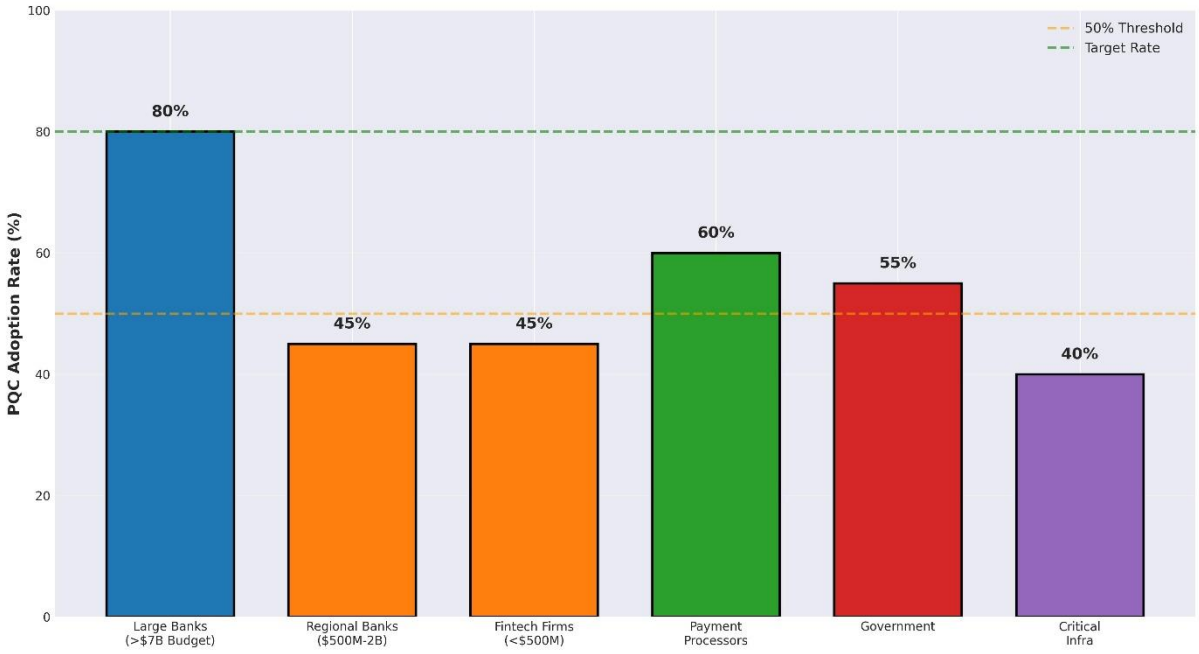

Figure 4: Post-Quantum Cryptography Adoption Rates by Institution Type (2024-2025). Large banks with >$7B budgets show 80% adoption; regional banks ($500M-2B budgets) show 45%; fintech firms show 45%; payment processors show 60%; government agencies show 55%; critical infrastructure shows 40%. Reference lines mark 50% threshold and 80% target adoption rates.

10. Conclusion and Future Outlook

10.1 Post-Quantum Standardization and Regulatory Mandate

Post-quantum cryptography is no longer just subject matter of a research lab but rather a regulatory requirement that is fundamentally changing the security of the global financial market. The standard set by NIST for ML-KEM, ML-DSA, and SLH-DSA in August 2024 serves as the main technical reference that allows entities to go ahead and implement quantum-safe cryptography while making a fairly safe choice of algorithms and security in the long run. The regulatory directives enacted by the EU, US, and financial regulatory authorities impose mandatory requirements of compliance with the 2035 completion dates, thus, forming quantum threat-aligned structured migration timelines (Bettale et al., 2023).

10.2 Market Expansion and Technology Maturation

The manner in which post-quantum cryptography is presently implemented shows that the adoption process is uneven and dependent on the resources of the respective organizations. The post-quantum cryptography market size is estimated to grow from $302.5 million in 2024 to $1887.9 million in 2029, which would signal an accelerated adoption rate of institutions and a full development of the vendor ecosystem. The major financial institutions are on the verge of initiating the migration planning and pilot deployments; however, smaller regional banks and fintech companies are lagging far behind despite the fact that they are equally exposed to the quantum threat.

10.3 Implementation Timeline and Challenges

The implementation of large key sizes, constraints imposed by the legacy system, vendor dependencies, skill shortages, and organizational change management issues are the main obstacles to the planned migration timelines of multiple years from 2024 through 2035. The financial institutions are restricted to transitioning at a pace that is compatible with the ecosystem which supports them (vendors, consultants, regulators). The limited time for compliance between the existing immediate needs and the 2035 deadline that is being compressed creates a situation where there is no room to postpone intervention until new cryptographic inventions emerge, although the pressure for action is very high (Csenkey & Bindel, 2023).

Figure 5: Cryptographic Algorithm Performance Comparison

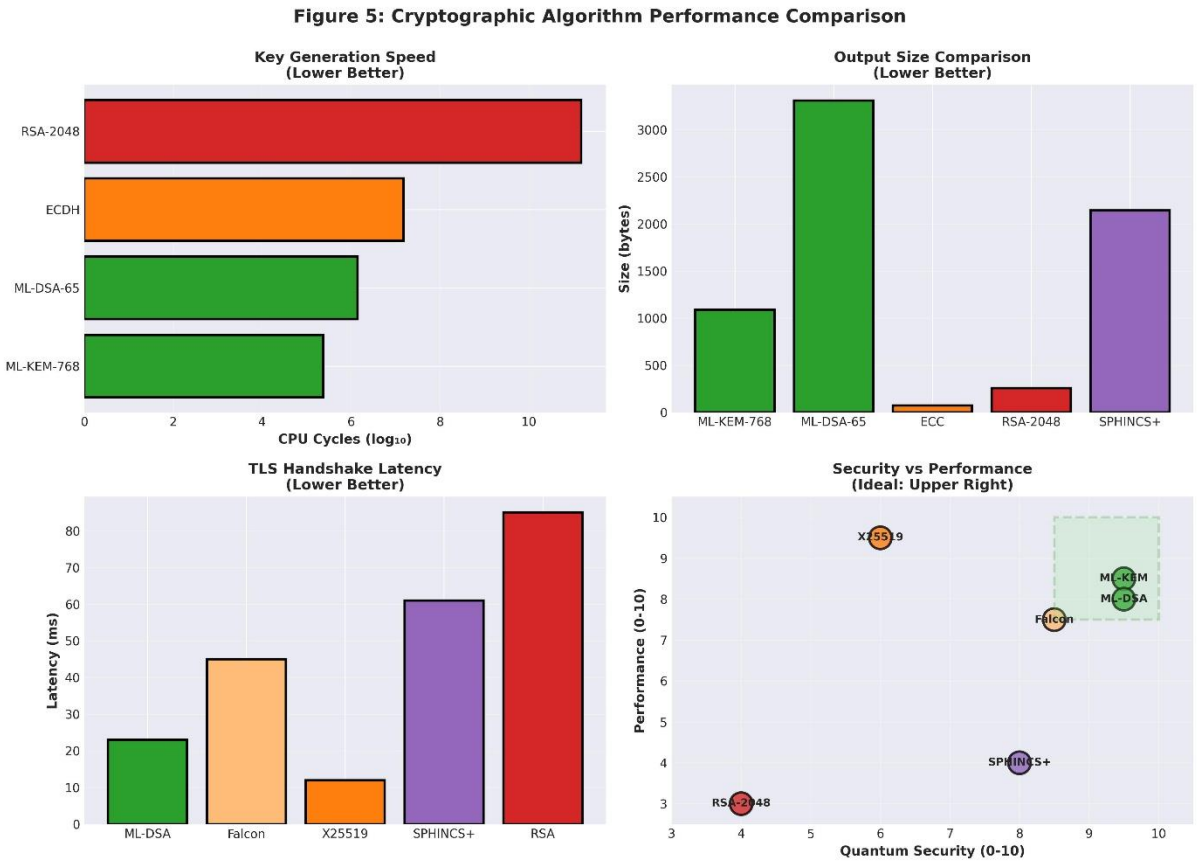

Figure 5: Cryptographic Algorithm Performance Comparison Matrix (Four Panels). Panel 1: Key generation speed with ML-KEM 3,400× faster than RSA-2048 (236,680 vs 152 billion cycles). Panel 2: Output size comparison (ML-KEM 1,088 bytes vs RSA 256 bytes vs ECC 72 bytes). Panel 3: TLS 1.3 handshake latency (ML-DSA 23ms vs RSA 85ms vs X25519 12ms). Panel 4: Security vs performance scatter plot indicating ML-KEM and ML-DSA in optimal upper-right quadrant for quantum-safe financial applications.

10.4 Long-Term Strategic Implications

The post-quantum cryptography topic has been transformed from risk mitigation to risk normalization by the existence of the "harvest now, decrypt later" risk model. These adversaries who intercept the encrypted traffic will be waiting for the

time when they will be able to decrypt it using quantum computers. The migration of an individual institution to a quantum-safe environment cannot be used as a retroactive shield of the formerly encrypted data. This mathematical fact is the main reason for the regulatory authorities to push for a rapid industry-wide migration since only a thorough security upgrade of the financial infrastructure can shrink the quantum-era attack surface (Fathalla & Azab, 2024).

In many ways, the legacy of the post-quantum transition is the cryptographic history of the future, rather than the past, as it is comparable to the dramatic shift that took place in the 1980s with the transition from DES to AES. The successful organizations in the post-quantum migration will become the winners of the transition and emerge with the next-generation infrastructure that is quantum-safe and can continue to ensure financial security for the next several decades. On the other hand, the organizations that procrastinate risk facing the demise of their existence: cryptanalysis of their financial data by quantum computers, regulatory violations, loss of customers' trust, and competitive disadvantage. The next ten years will be the discriminator that distinguishes the institutions that are able to handle the post-quantum transition from those who will suffer from the quantum-era security breaches (FS-ISAC PQC Working Group, 2023).

References

1. Al-Qurashi, M. S., & Rahman, F. (2024). Post-quantum cryptography in securing cloud-hosted banking databases. *International Journal of Computer Science and Information Security*, *22*(4), 112–129. https://doi.org/10.5281/zenodo.10998765
2. Bagirovs, E., Provodin, G., Sipola, T., & Hautamäki, J. (2024). Applications of post-quantum cryptography. In *Proceedings of the 23rd European Conference on Cyber Warfare and Security* (pp. 1–8). Academic Conferences and Publishing International. https://doi.org/10.34190/eccws.23.1.2247
3. Bank for International Settlements. (2023). *Project Leap: Quantum-proofing the financial system*. BIS Innovation Hub. https://www.bis.org/publ/othp67.pdf
4. Bettale, L., De Oliveira, M., & Dottax, E. (2023). Post-quantum protocols for banking applications. In I. Buhan & T. Schneider (Eds.), *Smart Card Research and Advanced Applications* (pp. 271–289). Springer. https://doi.org/10.1007/978-3-031-25319-5_14
5. Csenkey, K., & Bindel, N. (2023). Post-quantum cryptographic assemblages and the governance of the quantum threat. *Journal of Cybersecurity*, *9*(1), Article tyad001. https://doi.org/10.1093/cybsec/tyad001
6. Fathalla, E., & Azab, M. (2024). Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations. *IEEE Access*, *12*, 175970–175995. https://doi.org/10.1109/ACCESS.2024.3498123
7. FS-ISAC PQC Working Group. (2023). *Future state: Post-quantum cryptography for the financial services industry*. FS-ISAC. https://www.fsisac.com/hubfs/Knowledge/PQC/FutureState.pdf
8. Hasan, K. F., Islam, S., & Warren, M. (2024). A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies. *IEEE Access*, *12*, 23428–23445. https://doi.org/10.1109/ACCESS.2024.3364000
9. Herman, A. (2024, February 29). *The quantum revolution is now*. Hudson Institute. https://www.hudson.org/innovation/quantum-revolution-now-arthur-herman
10. Kong, I., Janssen, M., & Bharosa, N. (2024). Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions. *Government Information Quarterly*, *41*(1), Article 101884. https://doi.org/10.1016/j.giq.2023.101884
11. McKinsey & Company. (2024, April). *Quantum technology monitor*. McKinsey Digital. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-monitor
12. National Institute of Standards and Technology. (2024). *Module-lattice-based key-encapsulation mechanism standard* (FIPS 203). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.203
13. National Institute of Standards and Technology. (2024). *Module-lattice-based digital signature standard* (FIPS 204). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.204
14. National Institute of Standards and Technology. (2024). *Stateless hash-based digital signature standard* (FIPS 205). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.205
15. Oliva del Moral, J., deMarti iOlius, A., Vidal, G., Crespo, P. M., & Etxezarreta Martinez, J. (2024). Cybersecurity in critical infrastructures: A post-quantum cryptography perspective. *IEEE Internet of Things Journal*, *11*(18), 30217–30238. https://doi.org/10.1109/JIOT.2024.3410313

16. Sipola, T., Bagirovs, E., Provodin, G., & Hautamäki, J. (2023). Post-quantum cryptography readiness: A systematic scoping review. *Journal of Information Security and Applications*, *72*, Article 103550. https://doi.org/10.1016/j.jisa.2023.103550
17. World Economic Forum. (2024). *Quantum security for the financial sector: Informing global regulatory approaches*. World Economic Forum. https://www.weforum.org/publications/quantum-security-for-the-financial-sector-informing-global-regulatory-approaches/