Global Financial Banking Post Quantum Security Migration White Paper (2025)

Jintai Ding Hong Xiang Rui Liu

December 2025

Document History

Version	Date	Description
1.0.0	December 2025	The official version for 2025 has been released, consolidating the latest global advancements as of December, including the BIS Phase II report and the Kyber-208 breakthrough.
1.0.1	December 2025	Minor formatting adjustments.

Authors

Professor Jintai Ding

Dean, School of Mathematics and Physics, Xi'an Jiaotong-Liverpool University (XJTLU)

Director, Post-Quantum Migration Interdisciplinary Laboratory (PQC-X), XJTLU

Core Designer of NIST PQC Standards

Professor Hong Xiang

Deputy Director, Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University) Ministry of Education (CPS-DSC)

Rui Liu

Visiting Professor/Deputy Director, Post-Quantum Migration Interdisciplinary Laboratory (PQC-X), XJTLU

Chairman/CEO, Suzhou Langkong Post-Quantum Technology Co., Ltd. (LK Quantum)

Editor’ s Note: Rebuilding the Foundation of Financial Trust in the Quantum Era

The essence of finance is trust, and cryptography is the mathematical bedrock of trust in the digital age. With the rapid development of quantum computing technology, this foundation is facing unprecedented challenges. The risk of "Harvest Now, Decrypt Later" (HNDL) is no longer a distant theoretical hypothesis, but a Sword of Damocles hanging over the global financial system.

As a joint research team deeply committed to Post-Quantum Cryptography (PQC) for a long time, we closely follow global technological evolution. Core members of our team have been deeply involved in the entire process, from basic theoretical exploration to the development of NIST international standards. We are deeply aware that theoretical completeness does not equate to a smooth engineering path. In undertaking the National Key R&D Program of China's Ministry of Science and Technology, "Research on Post-Quantum Cryptography Migration Technology for the Banking Sector and Its Critical Infrastructure Information Systems," the entire project team faced an extremely challenging task: how to achieve a smooth, imperceptible quantum security migration in a financial environment with immense business scale, complex legacy systems, and extremely high stability requirements?

This Global Financial Banking Post-Quantum Security Migration White Paper (2025) is a systematic summary of the project team's journey of exploration. It not only aggregates our in-depth analysis of the latest strategies from the Bank for International Settlements (BIS), NIST, and major global economies but also, for the first time, discloses the "Data-Driven Migration Framework" and the "RegTech Theory" based on large-scale practice within the Chinese banking sector.

Here, we need to particularly emphasize: the "technological autonomy" and "supply chain resilience" advocated by this report are not a move towards isolation, but rather for building a more inclusive and interoperable security defense line within a diversified global technological ecosystem. We firmly believe that, in the face of quantum computing power, a challenge common to all humanity, the consistency of standards and the synergy of the ecosystem are paramount.

This White Paper aims to provide a pragmatic action guide for global financial institution decision-makers, technology executives, and industry experts. Regardless of the jurisdiction, the technical challenges we face are common. We hope this report, which embodies the cross-disciplinary wisdom of industry, academia, and research, along with solid engineering experience, can serve as a bridge to connect different technical standards and promote global experience sharing, jointly safeguarding the future of the digital economy.

Global Financial Banking Post-Quantum Security Migration White Paper Drafting Group

December 2025

Legal Notice and Disclaimer

Copyright Notice

Disclaimer

1. Nature of Information: The content contained in this White Paper is for reference only, intended to provide a strategic framework and technical guidance for the migration of Post-Quantum Cryptography (PQC) in the financial banking sector, and does not constitute final advice on legal, financial investment, or technological implementation in any form.

2. Accuracy: Although the drafting team has made every effort to ensure the accuracy of the data in the text, given the rapidly evolving nature of quantum technology, we do not assume legal responsibility for the absolute accuracy, completeness, or timeliness of the information.

3. Risk Warning: The technical solutions mentioned in the report should be evaluated in conjunction with the actual circumstances of each organization. The drafting group and personnel do not assume responsibility for any direct or indirect losses arising from the use of the information in this report.

Contents

Abstract

This White Paper, starting from a Chinese perspective, systematically elaborates on the disruptive challenges and strategic opportunities that quantum computing poses to the global financial system. The development of quantum computing technology is reshaping the future technology landscape at an unprecedented speed. While its powerful computing capabilities bring enormous potential to areas such as financial optimization and risk modeling, they also pose a fundamental threat to the existing public-key cryptography system. Facing the urgency of the "Harvest Now, Decrypt Later" (HNDL) attack [1], the global financial industry has entered a critical strategic window period for Post-Quantum Cryptography (PQC) [22] migration.

Against this backdrop, this report first comprehensively and in-depth analyzes the strategic layout, implementation paths, and latest progress of major global economies and their financial banking sectors in addressing this challenge, revealing the differences in national strategic models. Subsequently, the report focuses on presenting the "China Solution" for addressing the quantum threat. With foresight, through top-level design and centralized research of major national projects, China has achieved world-leading phased results in migration frameworks, core technologies, application verification, and management specifications. This aims to provide authoritative guidance and a strategic roadmap for building a secure, autonomous, and controllable quantum-safe new infrastructure for China’s financial industry.

Key Findings:

Strategic Divergence:

Global PQC migration paths show significant divergence. Unlike the US's "demand-pull" model [2], which is market-oriented with government agencies leading the way; the UK and Canada's "coordinated-push" model [3], which centers on regulatory directives and national roadmaps; and Japan's model [5], which is driven by regulatory leadership and industry consensus; China has adopted a top-down strategy of "top-level design, data-driven approach, and unified standards." This

model fully leverages the organizational and collaborative advantages of unified planning and centralized effort, enabling more efficient resource allocation, a more unified technical roadmap, and more thorough industry coordination, thus demonstrating unique advantages in addressing systemic risks.

Technological Autonomy:

The Chinese financial industry has preliminarily established an autonomous technological "toolkit" covering algorithms, hardware, software, protocols, and evaluation tools. Particularly in the field of lattice-based cryptography security analysis, which is the mainstream technological route for international PQC standards, China has demonstrated a "defining-level" assessment capability: following the global first efficient solution of the 200-dimensional Shortest Vector Problem (SVP) in March 2025 [6], the project team achieved another major breakthrough in November 2025, successfully solving the Kyber-208 instance in the Bochum Challenges [7], verifying the rationality and security boundary of the current international standard parameter selection. This series of consecutive victories, from fundamental mathematical problems to specific algorithm instances, eloquently proves the team's profound academic capability for independent security auditing and parameter boundary verification of international mainstream standards (such as NIST ML-KEM). This deep understanding of underlying mathematical problems allows us to more accurately assess the security margin of algorithms, thereby building a defense system for China's financial security based on "rigorous mathematical proof and in-depth analysis."

Practical Feasibility:

Through systematic, end-to-end migration verification in three typical financial business scenarios—mobile banking, online banking, and interbank clearing—the Chinese financial industry has successfully confirmed the technical feasibility, performance acceptability, and business continuity of the proposed migration path in a real business environment. These practical experiences not only validated the maturity of the technical solutions but also accumulated valuable engineering data and operational paradigms for large-scale migration across the entire industry.

Core Recommendations:

Under the unified guidance of management departments such as the People's Bank of China, the Chinese financial industry should follow the three-phase strategic roadmap proposed in this White Paper, taking the "Data-Driven PQC Agile Migration Framework for Banking" as the core methodology, adhering to the principles of crypto-agility and hybrid deployment, and accelerating the systemic and coordinated migration across the entire industry. This timeline is consistent with the goals set by US executive branch directives, such as OMB Memorandum M-23-02, which requires federal agencies to mitigate quantum risks as much as possible before 2035 [2]. Through these measures, China will seize the strategic initiative in the profound transformation of the global financial landscape.

Chapter 1: Foresight: Assessing the Global Financial Quantum Security Landscape

1.1 The Duality of Quantum Computing: Strategic Opportunity and Fundamental Threat

Quantum computing is a revolutionary computing technology based on the principles of quantum mechanics. It utilizes the superposition and entanglement characteristics of quantum bits (qubits) to exhibit computing power far exceeding classical computers when solving specific types of complex problems [8]. For the modern financial system, which heavily relies on complex computation, the rise of quantum computing is undoubtedly a double-edged sword, bringing both unprecedented development opportunities and an imminent existential threat.

From an opportunity perspective, quantum computing is expected to trigger a paradigm shift in several core financial areas. In investment and portfolio management, quantum optimization algorithms can more efficiently solve large-scale, multi-constraint optimization problems that are intractable for traditional computers, leading to more precise asset pricing and optimized portfolio strategies [9]. In risk management, quantum algorithms are expected to significantly accelerate compute-intensive tasks such as Monte Carlo simulations, making the calculation of financial derivatives pricing and Value-at-Risk (VaR) faster and more accurate [9], thereby enhancing financial institutions' risk measurement and management capabilities. Turkey's Yapi Kredi Bank, in collaboration with D-Wave, has successfully used quantum computing to analyze systemic risk in its corporate customer network, reducing calculations that would have taken years to just seconds [12]. Furthermore, in macroeconomics modeling and artificial intelligence, the powerful computing capabilities of quantum computing also foreshadow more complex economic model simulations and stronger machine learning capabilities, potentially leading to breakthroughs in fraud detection and algorithmic trading [8].

This characteristic of being dual-use—both offensive and defensive—forms a strategic driving force: defensive investments made to counter the quantum threat will inevitably build up an institution's knowledge, talent, and infrastructure related to quantum technology, resources that can then be strategically leveraged for offensive applications that generate significant business value. Financial institutions must invest in PQC migration for survival [10], a process that requires them to build internal expertise, acquire quantum-related hardware and software resources, and establish connections with the quantum ecosystem [13]. These capabilities—talent, infrastructure, and partnerships—established for defensive purposes are precisely the prerequisites for exploring offensive quantum computing applications (such as portfolio optimization) [9]. Thus, the quantum threat itself becomes an involuntary catalyst, compelling financial institutions to participate in this technological revolution that is likely to reshape the industry's future.

However, beneath the promise of opportunity lurks a disruptive threat. The security foundation of the current global financial system—the public-key cryptography system—faces the risk of being completely dismantled by quantum computing. Encryption algorithms widely used in identity authentication, digital signatures, and secure communication protocols (such as TLS), including RSA and ECC, rely on mathematical problems like large-number factorization and discrete logarithms that are difficult for classical computers to solve in an effective time [14]. However, the Shor's algorithm [16], proposed by mathematician Peter Shor in 1994, theoretically proves that a sufficiently powerful quantum computer can crack these problems at an exponential speed [13], reducing computations that would take classical computers millennia to hours or even minutes. This means that once a practical quantum computer emerges, the core security mechanisms of the global financial system—identity authentication, transaction signing, data encryption—will instantly become obsolete [17], and the foundation of trust for the entire system will face collapse [18]. This threat is not a distant future speculation but a direct challenge to real-world financial stability. It compels us to re-examine and rebuild the security infrastructure of the entire digital financial world.

1.2 "Harvest Now, Decrypt Later" Attack: The Urgency of

Asymmetric Risk

The most urgent and insidious feature of the quantum threat is the so-called "Harvest Now, Decrypt Later" (HNDL) attack model [1]. The logic of this attack model is that the attacker does not need to wait for the emergence of a practical quantum computer; they can begin now to massively and continuously intercept and store sensitive data currently protected by classical encryption algorithms [1]. This data may include national-level economic and financial data, core transaction records of financial institutions, corporate trade secrets, and personal privacy information. Although this data is currently secure, the attacker can "shelve" it, patiently waiting for quantum computing technology to mature in the future, and then use its powerful computing power to decrypt this historical data [21].

The existence of the HNDL attack model completely changes our traditional understanding of the cybersecurity risk time window, turning a seemingly distant future threat into an ongoing, continuous reality [23]. It reveals a profound "asymmetric urgency": the defender (financial institution) must complete the upgrade of the cryptographic system before the data loses its long-term value, while the attacker has relatively ample time to wait for technological breakthroughs. A theorem put forward by cryptographer Michele Mosca eloquently illustrates this dilemma: if an organization wishes its information to remain confidential for X years, and migrating to a post-quantum cryptographic system takes Y years, then the migration work must be completed Z − Y years before the quantum computer can crack the current encryption system (expected in Z years) [24]. For the financial sector, the confidentiality period (X) for many types of data (such as long-term loan contracts, strategic planning, and personal identity information) spans decades, and a systemic migration across the entire industry (Y) is also expected to take 5 to 10 years or even longer. Considering that experts predict that a quantum computer capable of cracking current cryptographic systems (Z) may appear within the next 10 to 20 years [11], this means that the "deadline" for migration is very close, perhaps even already passed.

This temporal asymmetry between offense and defense is the fundamental reason driving the global financial industry, especially China, which bears the mission of

maintaining national financial security, to adopt a "one step ahead," urgent strategic response. It explains why, both in China and globally, such a large-scale, high-investment national post-quantum security migration research and preparation effort must be initiated before quantum computers are fully mature. Waiting means handing over the security of historical data to future quantum attackers.

1.3 Transmission Mechanism and Impact Assessment: Systemic Challenges of Quantum Risk to Financial Stability

The destructive power of a quantum attack on the financial system goes far beyond the leakage of individual data. Its true danger lies in the potential to trigger a systemic trust crisis and chain reaction, thereby shaking the foundation of financial stability. The transmission mechanism of quantum risk can be understood on two levels: micro and macro.

At the micro level, once the public-key cryptography system is breached, attackers can easily forge digital signatures and identity certificates. This means they can impersonate banks, corporations, or even management authorities to conduct fraudulent transactions, tamper with payment instructions, and disseminate false information. For example, an attacker could intercept and modify an interbank transfer message, redirecting funds to an illegal account, and the existing signature verification mechanism would be unable to detect the forgery. Similarly, they could forge identities to log into online banking and steal customer funds. These actions would directly lead to enormous economic losses and a loss of individual trust.

At the macro level, the collapse of trust at the micro level would quickly transmit to the entire system. If the communication security and transaction integrity of critical financial infrastructures (such as large-value payment systems and securities settlement systems) are called into question, it could lead to widespread transaction interruptions and clearing failures. Market participants would refuse to trade due to an inability to trust their counterparties, triggering a liquidity crunch. Once public confidence in the banking system is shaken, it could trigger large-scale bank runs.

This panic would rapidly spread through the highly interconnected financial network, ultimately escalating into a systemic financial crisis.

The essence of this threat is the introduction of a new category of systemic risk—"systemic trust risk" or "infrastructure risk." Traditional financial systemic risk models primarily focus on credit defaults, market crashes, or liquidity shortages, while the quantum threat directly attacks the infrastructure that guarantees asset authenticity and ownership itself. This means that existing risk management frameworks are incomplete, and cryptographic vulnerability must be elevated to the same level of importance as market risk and credit risk. This also fundamentally reshapes the roles of Chief Information Security Officers (CISOs) and Chief Technology Officers (CTOs), transforming them from technical support roles into a critical part of the institution's core risk management function.

The Bank for International Settlements (BIS) previously predicted that quantum attacks could lead to losses exceeding 1% of GDP within the next 15 to 20 years [11]. However, reviewing this prediction at the end of 2025, the time window is significantly narrowing. With the breakthrough progress in quantum error correction technology this year, the industry (such as Forrester, etc.) has advanced the expectation of 'Q-Day' to within the next 10 years or even shorter. This means the 'security realization period' of HNDL (Harvest Now, Decrypt Later) attacks will come faster than expected, and financial institutions' risk exposure assessment must adopt correspondingly more aggressive time parameters. The essence of quantum risk is "trust" risk, and trust is the lifeblood of the financial system. Therefore, post-quantum security migration is not just a technical upgrade task but a strategic, fundamental project to maintain national financial sovereignty and market confidence.

Chapter 2: Strategic Competition: Strategic Layout and Path Divergence of PQC Migration in Major Economies

Facing the disruptive challenge posed by quantum computing, a multi-layered global governance and collaboration framework is taking shape. This framework consists of technical standards bodies, international strategic coordination platforms, and regional/industry implementation organizations, collectively guiding the PQC migration for the global financial sector. Concurrently, major world economies are exhibiting diverse strategic paths and implementation rhythms, shaped by their national circumstances and management cultures, providing us with a rich comparative analytical perspective.

2.1 Global Governance Framework: Standards, Alliances, and Roadmaps

2.1.1 The Standard Setter: NIST's PQC Standardization and Its Global Impact

The U.S. National Institute of Standards and Technology (NIST) plays a central leading role in the global PQC standardization process [25]. Starting in December 2016, NIST launched a global public call for and evaluation of PQC algorithms, aiming to select a new generation of public-key cryptographic standards that can resist attacks from both classical and quantum computers [26]. After nearly eight years of multiple rounds of rigorous public review, NIST officially published the first three final standards in August 2024 [25]:

FIPS 203 (ML-KEM): Based on the CRYSTALS-Kyber algorithm, used for general encryption and key encapsulation [25].
FIPS 204 (ML-DSA): Based on the CRYSTALS-Dilithium algorithm, used for digital signatures [25].
FIPS 205 (SLH-DSA): Based on the SPHINCS+ algorithm, serving as an alternate digital signature scheme [25].

NIST's standardization work provides the crucial technical "what" blueprint for global PQC migration. Its open, transparent, and collaborative process has earned it widespread international credibility, leading regulatory bodies globally, such as the UK’s National Cyber Security Centre (NCSC) and Japan's Financial Services Agency (FSA), to explicitly state their alignment with NIST standards [3]. This not only avoids technological fragmentation and interoperability issues caused by chaotic algorithm selection but also lays a common technical foundation for the smooth transition of the global financial system.

2.1.2 Building Consensus: The World Economic Forum (WEF) Initiative

If NIST solved the technical "what," the World Economic Forum (WEF) is committed to building the global consensus on the strategic "how" [10]. Through its "Quantum Security in the Financial Sector" project, the WEF has brought together major global financial institutions, regulatory bodies, and technical experts to issue a series of reports, providing a strategic framework for the financial industry's quantum security migration [10]. The WEF's proposed four-phase roadmap (Prepare, Clarify, Guide, Transition & Monitor) and four guiding principles (Reuse & Repurpose, Establish Non-Negotiable Baselines, Increase Transparency, Avoid Fragmentation) offer clear action guidelines for C-level executives and decision-makers in global financial institutions [10]. The WEF's role is that of a key "translator" and "coordinator," converting complex technical challenges into manageable business and policy issues, thereby promoting coordinated action globally [10].

2.1.3 European Coordination: The Roles of ETSI and Europol QSFF

In Europe, multiple organizations are driving PQC migration coordination at different levels, forming a regional implementation support network. The European Telecommunications Standards Institute (ETSI), as a technical standards organization, focuses on the practical application of PQC, researching quantum-safe primitives, protocol performance, implementation capabilities, and architectural considerations in specific applications, offering pragmatic deployment advice to the industry [14].

The Europol Quantum Safe Financial Forum (QSFF) is a multi-stakeholder platform specifically established for the European financial sector, launched in April 2024 [15]. Its goal is to coordinate the PQC transition in the financial industry, share best practices, identify challenges, and collaborate with other similar global initiatives [28]. The establishment of the QSFF itself sends a strong signal: PQC migration is viewed as a systemic issue concerning financial stability, rather than a mere cybersecurity technology upgrade, thus requiring specialized, cross-border coordination among financial institutions.

2.2 Bank for International Settlements (BIS): The Global Central Bank System's "Quantum Compass" and Practice Pioneer

As major economies globally launch their Post-Quantum Cryptography (PQC) migration plans, the Bank for International Settlements (BIS), with its unique global position, plays a critical role transcending any single nation or region. BIS is not only a keen observer of technology trends but also the "thought leader," "practice pioneer," and "coordination facilitator" for the global central bank system's response to the quantum threat. Through its authoritative research, groundbreaking experimental projects, and the construction of a global governance framework, BIS has successfully elevated PQC migration from a purely technical topic to a core strategic issue concerning global financial stability, providing an indispensable "Quantum Compass" and practical example for the smooth transition of the entire financial system.

2.2.1 Strategic Positioning: Elevating the Issue from Technical Warning to Financial Stability

BIS’s primary contribution lies in systematically leveraging its authoritative platform as the "central bank for central banks" to reshape the global financial decision-making layer's cognitive framework on quantum risk. Before BIS’s involvement, PQC migration was primarily seen as the domain of technical standards bodies (like NIST) and cybersecurity experts, with discussions often confined to algorithmic complexity and technical implementation details. Through a series of impactful research reports,

BIS successfully elevated this topic from the technical staff's "algorithm replacement" discourse to the "systemic risk" and "macroeconomic impact" concerns of central bank governors and finance ministers, achieving a "dimensional upgrade" in the issue's importance.

The core of this strategic elevation is BIS's accurate "translation" and quantification of quantum risk. BIS research reports prospectively assessed the potential economic impact of a quantum attack, clearly stating that an expected economic loss from a systemic cyber-attack enabled by quantum computing could exceed 1% of GDP within the next 15 to 20 years [11]. This astonishing quantified data provided a powerful, economically supported basis for central banks and governments worldwide to designate PQC migration as a national strategic priority and commit significant resources to proactive deployment.

Concurrently, BIS publications repeatedly emphasize the real threat of the "Harvest Now, Decrypt Later" (HNDL) attack model [20]. BIS analysis points out that the existence of the HNDL attack fundamentally changes the cybersecurity risk time window, making the protection of financial data with long-term confidentiality value (such as long-term loan contracts, strategic M&A plans, and personal identity information) an urgent task. This temporal asymmetry between offense and defense compels financial institutions to act immediately, as waiting today means handing over the security of historical data to future quantum attackers [11].

More fundamentally, BIS's analysis profoundly reveals that the essence of quantum risk is "trust" risk. Once the public-key cryptography system, which is the security cornerstone of the current financial system, is breached, digital signatures and identity authentication mechanisms will fail, and the foundation of trust for the entire system will face collapse, potentially triggering a systemic trust crisis and chain reaction, ultimately threatening financial stability [17]. By directly linking an abstract technical vulnerability (like Shor's algorithm's threat to RSA) to the core concept of financial stability (trust), BIS successfully shifted the PQC migration narrative from a technical problem for the IT department to a fundamental governance issue concerning institutional survival and market confidence that must be directly addressed by the board and top regulatory layers.

2.2.2 “Project Leap”: Defense-in-Depth from Network Pipes to Core Business

If BIS's research reports answered the "why" of migration, its leading initiative, "Project Leap" [42], answered the critical "how" of implementation within real financial infrastructure through rigorous, phased experiments. Project Leap, led by the BIS Innovation Hub Eurosystem Centre, proceeded through two progressive stages, demonstrating a full-stack migration path from the network communication layer to the core payment business layer.

Phase 1: Encrypted Tunnel Verification at the Network Layer (2023)

In Phase 1, BIS, in collaboration with the Banque de France and Deutsche Bundesbank, successfully verified the feasibility of transmitting data between central banks across borders using quantum-safe VPNs. This phase focused on "pipe security," establishing a secure channel using a reinforced open-source IPsec VPN solution in a hybrid mode (classical + PQC). It demonstrated that the additional latency introduced by PQC was mainly concentrated during the handshake phase, with negligible impact on data transmission throughput.

Phase 2: Deepening to the Core—Business Layer Verification of the Target2 Payment System (December 2025)

The Phase 2 report, published in December 2025 [43], marked a significant strategic deepening of the testing. This experiment not only expanded the collaboration—incorporating the Bank of Italy and key global financial infrastructure providers Swift and Nexi-Colt—but, more importantly, the test object directly targeted the Eurosystem’s core real-time gross settlement system, Target2 (T2).

The Phase 2 testing was no longer confined to external encrypted tunnels but delved into the internal structure of payment messages. The experiment successfully replaced the traditional RSA algorithm for digital signatures on liquidity transfer messages (Liquidity Transfers, camt.050) with the NIST-standardized PQC algorithm, CRYSTALS-Dilithium, within the T2 system's test environment. The focus was on signature and verification at the Business Application Header (BAH) layer in the ISO 20022 message standard.

This phase of testing revealed more severe engineering challenges and key findings than Phase 1:

Quantification of the Performance Gap: Unlike the network layer test, the introduction of PQC at the business layer led to a noticeable performance degradation. Actual measurements showed that PQC digital signature verification took an average of 209.9 milliseconds, compared to only 28.1 milliseconds for traditional RSA, a performance difference of nearly an order of magnitude. This issued a clear warning to the industry: PQC migration may require a significant increase in computing resources or a reassessment of Service Level Agreements (SLAs) for transaction processing in future high-frequency trading systems.

"Hybrid Mode" Implementation Challenge: Although BIS repeatedly emphasized that "hybrid mode" (running both classical and PQC algorithms in parallel) is the optimal strategy for the transition period, the actual modification of the T2 system revealed that existing application layer software architectures (such as signature verification modules) struggled to directly support processing both signatures simultaneously in the same message header. To complete the test, the project team had to develop specialized components for traffic splitting. This finding profoundly revealed that "crypto-agility" is not just about replacing algorithms but also requires deep restructuring of the underlying logic architecture of existing core systems.

Interoperability Verification: Despite the performance and architectural challenges, the experiment successfully proved that PQC signatures could achieve interoperability between different institutions (central banks and network service providers) and different technology stacks (vendor solutions and open-source solutions). All injected valid PQC-signed messages were correctly processed, while invalid signatures were successfully identified and rejected by the system, validating the effectiveness of PQC in ensuring transaction non-repudiation and integrity.

Table 2-1: Key Findings of "Project Leap" and Strategic Implications for Financial Institutions

Discovery Area	Key Technical Observation (Phase 1 & Phase 2)	Strategic Implication for Financial Institutions
Feasibility	Phase 1: Verified the feasibility of PQC encryption for cross-border VPN tunnels. Phase 2: Verified the functional integrity of using the CRYSTALS-Dilithium algorithm for signing ISO 20022 messages in the Target2 core payment system.	PQC migration has moved from "perimeter communication protection" to "core business logic reconstruction." Institutions must prepare for code-level modifications to core accounting and payment systems.
Performance Trade-off	Phase 1: VPN handshake slowed down, but data transmission throughput was minimally affected. Phase 2: Business layer signature verification performance degraded significantly. PQC verification time (209.9ms) was 7.5 times slower than RSA (28.1ms).	Hardware computing resource requirements for core trading systems must be reassessed. For high-frequency, low-latency scenarios (e.g., HFT, instant payments), PQC may become a performance bottleneck, requiring advance planning for hardware expansion or dedicated accelerator cards.
Hybrid Mode Challenge	Phase 2 Finding: Many existing traditional application software architectures (e.g., signature verification modules) do not support "hybrid mode" processing of two algorithms simultaneously, requiring complex custom development or architectural decoupling.	"Hybrid Mode" is easier said than done. Institutions must mandate that vendors provide native "multi-algorithm parallel support" capability when purchasing new systems or retrofitting old ones, making this a key metric for acceptance testing.
Supply Chain Dependency	Phase 2 Emphasis: Migration heavily depends on cooperation from network service providers (NSPs) and software vendors like Swift and Nexi.	Banks cannot complete the migration alone. Joint working groups must be established with key vendors to actively intervene in and collaboratively test their product roadmaps.

2.2.3 Thought Leadership: Building the Global Quantum Readiness Roadmap

Building on the success of its practical exploration, BIS published the milestone

report Quantum-readiness for the financial system: a roadmap in July 2025 [29], further cementing its thought leadership in global PQC migration. The uniqueness of this report lies in its transcendence of mere technical guidance, offering the global financial system a dual-layer action framework that is both macro-systemic and micro-actionable, aiming to effectively unify the cognition and action pace of regulators and market participants.

The report profoundly recognized that PQC migration is a classic "collective action dilemma": for an individual financial institution, being the first to migrate entails high costs and uncertain risks, making the rational choice to wait and observe; but if all institutions choose to wait, the entire financial system will be jointly exposed to immense systemic risk. BIS's roadmap systematically solves this dilemma by providing clear, interlocking action guides for regulators and market executors, respectively.

For Regulators, BIS proposed a Systemic Roadmap (A systemic roadmap), comprising three core phases [29]:

Engage: The regulator's primary task is to break the market's wait-and-see deadlock by issuing guidance, organizing workshops, and communicating with the industry to initiate ecosystem participation and provide market certainty.

Plan: Based on consensus building, regulators should lead the development of a system-level migration timeline and a common technical selection framework (e.g., algorithms, key lengths), coordinating with international standards and other jurisdictions.

Monitor: Regulators need to establish monitoring mechanisms to track migration progress in the public and private sectors, ensuring the entire financial system achieves the desired security level through system-wide stress tests and penetration tests.

For Financial Institutions such as commercial banks, BIS provided an Institutional Roadmap (Quantum-readiness for financial system participants), also comprising three key actions [29]:

Raise Awareness: Institutions should respond to regulatory signals, build internal consensus on quantum risk, appoint senior leaders, form cross-functional teams, and conduct preliminary risk assessment and budget planning.

Plan: This is the most critical phase, where institutions need to conduct a thorough cryptographic asset inventory, map the cryptographic environment, assess internal and external dependencies, coordinate with vendors, and develop a detailed, phased internal migration plan and pilot projects.

Execute: Institutions should start migrating high-priority systems first, implementing changes gradually, and conducting rigorous testing and validation. Experience and data from the execution phase should feed back into the planning phase, forming a continuous improvement dynamic loop.

The brilliance of this dual-layer framework lies in its synergistic effect: the "Engage" phase of the regulator provides the external driving force for commercial banks to start the "Awareness" phase; and the "Execute" results from commercial banks become crucial evidence for the regulator's "Monitor" phase. In this way, BIS's roadmap organizes fragmented, hesitant individuals into a collective with clear goals and coordinated steps, systematically resolving the global "tragedy of the commons" risk inherent in PQC migration. The report also emphasizes that the migration process should adhere to a series of core principles, including Defence in depth, Cryptographic agility, Hybrid models, and Phased migration, cautioning institutions against treating this change as a simple algorithm replacement [29].

2.2.4 Conclusion: BIS as the "Infrastructure" for Global Financial PQC Migration

Overall, the role BIS plays in promoting global financial PQC migration far exceeds that of a mere participant or coordinator. It is, in essence, providing crucial, indispensable "soft infrastructure" for this complex and profound global technological transformation—namely, a complete risk analysis framework, technical verification platform, governance roadmap, and international coordination

mechanism.

Risk Analysis Framework: By linking the quantum threat to macroeconomic indicators like GDP loss and emphasizing the urgency of HNDL, BIS provides central banks and financial institutions worldwide with a common language and standardized model for assessing, quantifying, and reporting quantum risk [11].

Technical Verification Platform: The success of "Project Leap" has made it a de facto technical verification reference platform. Its publicly released experimental data and engineering experience offer valuable, credible engineering benchmarks for global peers when making technology choices, performance evaluations, and solution designs [17].

Governance Roadmap: The dual-layer roadmap published by BIS provides a standard governance and project management template for PQC migration that can be directly adopted or adapted by regulators and financial institutions globally, significantly lowering the barrier for countries to initiate migration work [29].

International Coordination Mechanism: Owing to its neutrality and authority, BIS acts as an indispensable coordinator in international multilateral platforms such as the G7 Cyber Experts Group, promoting a globally consistent direction of action and thus preventing the "digital Balkanization" and interoperability barriers that could arise from non-uniform national standards and progress.
In summary, through its systematic and pioneering work in risk perception, technical practice, and policy coordination, BIS is building a stable, synergistic, and efficient PQC migration environment for the global financial system. It is not only a guide for direction (compass) and a pioneer in action but also the underlying support and key node for the healthy evolution of the entire ecosystem.

2.3 North American Progress: A Comparison of Two Collaborative Paths

In North America, while the US and Canada share the same goal, their strategies for

driving PQC migration show two distinct yet highly synergistic models.

2.3.1 United States: Market-Driven, Institution-Led Migration

The US PQC migration strategy can be described as a "demand-pull" model. Its core feature is to create a stable and predictable market demand through mandatory requirements for the government's own systems, thereby spurring the private sector (especially technology vendors) to develop and offer PQC solutions, ultimately benefiting the entire economy, including the financial sector.

Federal Strategy and Legislative Authorization: The US government has set clear migration timelines for federal agencies through a series of acts and executive orders, such as the Quantum Computing Cyber Security Preparedness Act (Public Law 117-260), signed into law in December 2022, and the Office of Management and Budget (OMB) Memorandum M-23-02 [2]. This timeline aligns with the goals set by US executive branch directives, such as OMB Memorandum M-23-02, which requires federal agencies to mitigate quantum risks as much as possible before 2035 [2]. These directives compel IT vendors and service providers supplying the government to accelerate their PQC product R&D and verification, creating a mature PQC product and service ecosystem for the private sector to choose and adopt [30].

Commercial Bank Pioneers: In this market environment, large US commercial banks, leveraging their abundant resources and foresight, have become industry pioneers in PQC migration. Their actions stem not from direct regulatory mandate but from their own risk assessment and strategic considerations.

> JPMorgan Chase: As a recognized industry leader, JPMorgan Chase has developed a detailed five-phase migration framework: cryptographic asset inventory, infrastructure enablement, risk assessment, prioritization, and remediation/upgrade [13]. This framework profoundly highlights the huge engineering challenges of migration for large financial institutions with heterogeneous technology stacks, vast legacy systems, and complex vendor dependencies. Its core work on "inventory" and "coordination" has become an important reference for global peers.

Bank of America: The bank has elevated the quantum threat to a strategic level, with its global strategist, Haim Israel, calling the quantum race "the most important technological race of our generation" [31]. The bank is actively recruiting "post-quantum cryptography engineers," requiring deep knowledge in PQC, NIST standards, and cloud security, indicating a systematic effort to build internal expertise in preparation for large-scale migration.

Goldman Sachs: Goldman Sachs's quantum strategy reflects a dual focus on offense and defense. On the defense side, they recognize the necessity of PQC; on the offense side, they are more actively collaborating with partners like Amazon Web Services (AWS) to explore quantum algorithms in areas such as financial derivatives pricing and portfolio optimization, striving to capture the commercial opportunities presented by quantum computing [32].

2.3.2 Canada: Coordinated National Strategy

In contrast to the US, Canada's PQC migration strategy is a more centralized "coordinated-push" model. There is stronger synergy and unified planning among the government, regulatory agencies, and key industries.

Government and Regulatory Framework: The Canadian Centre for Cyber Security (Cyber Centre) published a PQC migration roadmap for government systems, setting clear milestones: planning complete by April 2026, migration of high-priority systems by 2031, and completion of all system migration by the end of 2035 [4]. This guidance is backed by policy authorization from the Treasury Board, making it mandatory [4]. Crucially, the strategy explicitly requires the inclusion of PQC capability and crypto-agility in new procurement contracts to avoid future redundant investment [4].

Institutional Initiatives:

Bank of Canada: As the central bank, the Bank of Canada is active in PQC research, publishing academic papers on PQC-fortified privacy-preserving payment schemes and exploring cutting-edge applications like using quantum annealing

to optimize liquidity [11]. This indicates the development of deep technical reserves and understanding.

Royal Bank of Canada (RBC): RBC is an exemplary case of the private sector driving PQC readiness through industry-academia collaboration. The bank has invested heavily in the University of Waterloo to establish a dedicated cybersecurity lab, focusing on research in PQC, privacy-enhancing technologies, and more. By sponsoring educational programs like CryptoWorks21, RBC is making a long-term strategic investment in addressing the future talent shortage in quantum security.

2.4 European Progress: Diversified National Strategies and Cross-Border Collaboration

PQC migration progress in Europe presents a "mosaic" picture, featuring explicit national directives, groundbreaking cross-border central bank cooperation, and active practices by large commercial banks, collectively forming a complex and vibrant ecosystem.

2.4.1 UK Model: Clear Regulatory Timeline

The UK has set a clear and binding roadmap for PQC migration at the national level, serving as a global exemplar.

NCSC and CMORG: Setting the National Pace: Guidance documents from the UK National Cyber Security Centre (NCSC) set explicit deadlines for critical sectors: inventory and planning complete by 2028, migration of the highest-priority systems by 2031, and PQC migration of all systems complete by 2035 [3]. This timeline provides stable expectations and a planning basis for businesses. Concurrently, the Cross-Market Operational Resilience Group (CMORG), the coordination body for the financial sector, issued detailed guidance consistent with the NCSC, emphasizing the fundamental importance of cryptographic asset inventory, risk assessment, and prioritization.

Banking Sector Action: HSBC and Barclays PQC Projects:

HSBC: As a global leader in PQC practice, HSBC's actions are far beyond the planning phase. They are actively involved in actual trials, for instance, joining the UK’s first commercial quantum-safe metropolitan area network, collaborating with technology partners BT and Toshiba to apply PQC and Quantum Key Distribution (QKD) technologies to protect financial transactions [34]. The bank established a Global Head of Quantum Technology position and emphasized the foundational role of cryptographic asset inventory, indicating a comprehensive commitment from strategy to execution [35].

Barclays: Having explored quantum computing since 2017, its strategic focus similarly encompasses risk mitigation and the exploration of quantum-safe systems. Barclays actively engages with the quantum technology ecosystem through programs like its TechStars accelerator and has openly expressed its awareness of the "Harvest Now, Decrypt Later" threat and the necessity of early preparation.

2.4.2 Franco-German Engine and Pan-European Leadership

Central Banks Leading: Insights from BIS "Project Leap": "Project Leap," jointly conducted by the BIS Innovation Hub, Banque de France, and Deutsche Bundesbank, is a landmark practice in the central banking system's response to the quantum threat [17]. The project successfully established an IPsec VPN secure channel using a hybrid mode (classical + PQC algorithms) between Frankfurt and Paris and transmitted ISO 20022-compliant payment messages [17]. Key findings of the project include: verifying the feasibility of deploying PQC on existing network infrastructure; revealing the performance trade-off where PQC increases latency during connection establishment but has minimal impact during data transfer; and re-emphasizing the crucial importance of crypto-agility [17]. This project provided invaluable early engineering experience for central banks and financial institutions globally.

Commercial Bank Participation:

Deutsche Bank: As a participant in "Project Leap," Deutsche Bank also has dedicated cryptographer architects internally responsible for driving the introduction of PQC and the realization of crypto-agility to prepare for "Q-Day."

BNP Paribas: The bank was rated as an "active" bank in quantum technology by an Evident research report. It not only assesses quantum risks but also invests in PQC startups like CryptoNext through its venture capital arm, Opera Tech Ventures, demonstrating a strategic vision of shaping the future through investment.

2.4.3 Switzerland: Proactive, Risk-Based Model

Regulatory Stance and Industry Guidance: Switzerland’ s model is unique; its Financial Market Supervisory Authority (FINMA) has not issued a mandatory migration timeline but expects financial institutions to proactively manage technological risks. In response, industry organizations play a more active role. The Swiss Financial Innovation Desk (FIND) published a seven-step action plan urging the financial industry to act [36]. The Swiss Bankers Association (SBA) released a detailed expert report, providing banks with a roadmap including analysis, data classification, and migration planning, reflecting a mature, risk-based self-regulatory culture [36].

Institutional Participation: The UBS Case: UBS's quantum strategy focuses on seizing opportunities and ecosystem building. As a key partner of the Open Quantum Institute (OQI), UBS collaborates with the European Organization for Nuclear Research (CERN) and the Swiss government to explore using quantum computing to achieve UN Sustainable Development Goals. This investment in high-level, foundational research indicates UBS's commitment to maintaining a technological edge in the quantum era and deeply integrating into the global quantum ecosystem.

2.4.4 Other Key Players: Santander's Proactive Stance

Spain's Santander bank stands out in global PQC migration. Its core strategy is "going beyond internal readiness to actively shape the external ecosystem." The bank has not only developed an internal "Quantum Threat Program" but also actively collaborates with the US NIST's National Cybersecurity Center of Excellence (NCCoE) on PQC migration projects [30]. Crucially, Santander is playing a key role, alongside GitHub and Microsoft, in developing a Cryptographic Bill of Materials (CBOM) tool called "Cryptobom-Forge," aimed at helping the entire developer community better identify and manage cryptographic dependencies in software.

2.5 Asia-Pacific and Middle East Progress: The Emergence of Diverse Paths

In the Asia-Pacific and Middle East, Japan, Singapore, Israel, and Hong Kong, China, are rapidly becoming regional focal points for PQC migration readiness, each with unique strategies that reflect their national circumstances, regulatory philosophies, and global financial system positioning.

2.5.1 Japan: Regulation-Driven, Consensus-Based Migration

Japan's PQC migration strategy exhibits a typical model: dominated by authoritative regulatory bodies and driven by consensus achieved through industry consultation. The core of this model is ensuring the stability and coordinated action of the entire financial sector.

FSA-BOJ-NISC Linkage Mechanism: The core of Japan's action lies with its financial regulatory bodies. The Financial Services Agency (FSA), in collaboration with the Bank of Japan (BOJ) and the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), organized a "Study Group on Countermeasures for Deposit-Taking Institutions Against Post-Quantum Cryptography" between July and October 2024 [5]. The workshop brought together representatives from the three mega-banks, various banking associations, and cybersecurity/standards organizations, forming a

broad coalition of stakeholders.

Official Guidelines: The report published in November 2024 by the study group constitutes the official guidelines for Japan's financial industry PQC migration. The language of the report is firm, urging "all financial institutions, regardless of size," to "immediately begin" PQC migration [27]. The core recommendations align closely with global best practices, including: immediate commencement of a comprehensive cryptographic asset inventory (which must include critical outsourced systems), setting priorities and migration roadmaps based on risk assessment, ensuring "crypto-agility," and securing strong management commitment. This approach, led by regulators to convene industry leaders and achieve a unified action plan, aims for a coordinated, synchronized migration across the entire industry, thus minimizing systemic risk.

2.5.2 Singapore: The Hub of Quantum Innovation and Readiness

The Monetary Authority of Singapore (MAS) has adopted a flexible, pragmatic, and forward-looking multi-pronged strategy, aiming to establish its financial center as a key global hub for PQC readiness and innovation.

MAS Strategy: Consultation, Funding, and International Cooperation: MAS's strategy comprises three interconnected pillars:

Issuing Guidance: In February 2024, MAS issued a Consultation Paper on Proposed Measures to Address Quantum-Related Cybersecurity Risks to all financial institutions. The document explicitly advises institutions to monitor quantum developments, maintain a cryptographic asset inventory, assess system crypto-agility, and actively engage with vendors regarding their PQC roadmaps.

Providing Financial Incentives: In July 2024, MAS announced a commitment of S$100 million under its Financial Sector Technology and Innovation (FSTI 3.0) scheme to support quantum and AI capability building. A dedicated "Security

Grant" was established, offering up to 30% co-funding for pilot projects exploring the use of PQC and QKD [37]. This reduces the experimental cost for financial institutions, directly incentivizing their exploration and verification of cutting-edge technologies.

Engaging in International Collaboration: MAS actively seeks international cooperation to gain firsthand experience. A notable example is the successful completion of a cross-continental PQC joint experiment with the Banque de France, testing quantum-safe algorithms for email signing and encryption [38]. This not only enhances MAS’ s own expertise but also showcases Singapore’ s proactive stance in quantum security globally.

2.5.3 Israel: National Security-Driven Mandatory Compliance Model

Israel’ s PQC migration strategy is one of the most mandatory and urgent models globally, with its core driver stemming from profound national security considerations. The country uses binding directives issued by regulatory bodies to transform quantum risk from a future technological issue into a compliance issue that must be immediately addressed.

Regulatory Heavy Hand: Bank of Israel’ s Mandatory Directive: In January 2025, the Banking Supervision Department of the Bank of Israel issued a landmark directive explicitly addressing "cybersecurity risks arising from quantum computing capabilities" [39]. The issuance of this directive marked a shift from guidance to mandate. Its core argument is that, due to technological advancements, the timeline for the emergence of a quantum computer capable of cracking current encryption systems has shortened to the next decade or less. The directive explicitly identifies "Harvest Now, Decrypt Later" (HNDL) as the most immediate risk—where attackers steal encrypted data today, awaiting future decryption [39]. Unlike advisory guidelines issued by many countries, Israel's directive is mandatory. It requires all banks to develop a preliminary readiness plan detailing quantum risks, cryptographic challenges, and mitigation strategies, which must be submitted to the board for review and approval. More crucially, the directive sets a strict compliance timeline:

banks must submit a final, executable migration plan to the Banking Supervision Department’s Technology, Innovation, and Cyber Unit within one year [39]. This measure effectively converts PQC readiness from voluntary corporate action into a regulatory task with a clear deadline.

National-Level Coordination and Governance: The Bank of Israel’s directive is not an isolated action but part of Israel's national-level coordinated strategy. The Israel National Cyber Directorate (INCD) and the National Digital Agency had already paved the way for this moment. The INCD's Best Practices for Organizational Cyber Readiness in the Post-Quantum Era, published in January 2022, provided organizations with an action framework, recommending asset mapping, risk analysis, and mandating crypto-agility requirements in vendor contracts. The National Digital Agency further reinforced this requirement, directing all government ministries to complete a comprehensive 'threat assessment' by the end of 2025 (this month). As the deadline approaches, the Israeli public sector is concluding a massive asset inventory phase. This includes: identifying cryptographic assets that could be targets for data harvesting, assessing the damage potential of a breach, and formulating response plans. Simultaneously, government agencies must explicitly require post-quantum encryption capabilities in all new technology vendor contracts. This government-led procurement demand creates a powerful market pull for the private sector (including bank vendors), forcing the entire technology ecosystem to accelerate PQC product development and deployment.

Geopolitics and Innovation Ecosystem: Israel’s quantum strategy goes far beyond defense. Its National Quantum Initiative (NQI) is viewed as an important geopolitical tool. A proposed US-Israel joint AI and Quantum fund, valued at $200 million, has one of its public goals as counterbalancing China’s growing influence in the field, with plans to strengthen regional alliances under the "Abraham Accords" framework by including countries like the UAE and Saudi Arabia. The confidence for this grand strategy stems from Israel's vibrant quantum technology innovation ecosystem. The country is home to over 22 quantum technology startups, 9 of which focus on core quantum computing, having collectively raised about $650 million, and boasts one of the world's highest densities of quantum technology talent. This ecosystem provides the critical talent and technology reserve needed to meet mandatory domestic PQC migration demands.

The Gap Between "Mandate" and "Reality": However, Israel's model also reveals a profound contradiction: while regulatory directives are decisive, officials and the industry admit that fully tested, commercially deployable PQC solutions are not yet fully mature. Officials have noted that NIST-standardized algorithms are still in their early stages, with performance and reliability issues yet to be resolved. This creates a "compliance paradox" for banks: they are mandated to prepare for a technological transformation, yet the ultimate tools for this transformation are not fully in place. Consequently, the banks' actual response strategy is necessarily two-fold: first, immediately satisfy the procedural requirements of the regulator, i.e., complete asset inventory, risk assessment, and plan formulation by the deadline to ensure compliance; second, at the technical level, focus on building "crypto-agility," waiting for PQC technology and standards to mature before proceeding with large-scale system migration. In this context, crypto-agility is not just a best practice but a core survival strategy for Israeli financial institutions under regulatory pressure.

2.5.4 Hong Kong, China: Pragmatic, Ecosystem-Driven Evolution Model

In stark contrast to Israel’s mandatory compliance model, Hong Kong, China’s path to PQC migration exhibits a pragmatic, ecosystem-led, and market-practice-first evolutionary characteristic. Following the successful conclusion of the "Fintech 2025" strategy, the Hong Kong Monetary Authority (HKMA) officially launched the "Fintech 2030" new strategy in November 2025. In the new strategy's "DART" framework, HKMA elevated "Quantum Resilience" for the first time as a core pillar, marking Hong Kong's shift from "monitoring and observation" of quantum technology to the substantial phase of "defense and infrastructure" construction, striving to build immediately available quantum-safe financial infrastructure within the new five-year cycle.

Management Foundation: Accumulation and Status from the "Fintech 2025" Period: Although the new strategy is established, the data and insights accumulated by HKMA under the "Fintech 2025" framework [40] remain the foundation for current actions. In the Fintech Adoption: Progress and Future Direction circular published in

July 2025, HKMA data showed that the banking sector's adoption rate for quantum computing is currently low (only 7%) but future intention is significant, projected to grow to 53%. Based on this assessment, HKMA defined its role during the strategy transition period: promoting education and raising awareness. Its focus remains on collaborating with the industry to explore the potential applications of quantum computing in areas such as risk modeling and portfolio optimization, while emphasizing the importance of "quantum safety," particularly through adopting PQC to mitigate future risks. In its official publications, the focus still largely remains on more mature fields such as Distributed Ledger Technology (DLT), Central Bank Digital Currency (CBDC), and Artificial Intelligence (AI). This suggests HKMA is taking a patient, incremental approach, awaiting the maturation of technology and the market.

Industry Practice: The Paradigm of "Practice Preceding Policy": The most distinctive feature of the Hong Kong model is the emphasis on "practice preceding policy." Global banking giant HSBC’s PQC pilot in Hong Kong provides a world-class example of this model. HSBC did not wait for regulatory directives but proactively integrated PQC as a core security guarantee for its innovative financial products [35]. In its tokenized gold product launched for Hong Kong retail investors, HSBC collaborated with quantum computing company Quantinuum, using PQC algorithms still undergoing NIST standardization, along with quantum random number generation technology, to protect its digital asset platform, HSBC Orion. The significance of this pilot is profound: first, it is not a proof-of-concept in a lab but is used to secure a real, market-facing, novel financial product. Second, it successfully demonstrated how PQC can resist HNDL attacks and ensure the interoperability of digital assets safely flowing across different distributed ledgers. This successful practice provides a strong, market-driven business case for PQC application in Hong Kong, shifting the PQC narrative from a mere "cost of risk defense" to an "enabler of business innovation."

Infrastructure Construction: "Invisible" Migration Preparation: The deep investment of Hong Kong's financial sector in DLT and CBDC infrastructure objectively constitutes "invisible preparation" for PQC migration. Several large-scale projects led by HKMA, such as the cross-border Multiple Central Bank Digital Currency (mBridge) project in collaboration with the BIS Innovation Hub and multiple central banks, and the local e-HKD pilot program, are systematically training the Hong Kong banking sector's

capability to master next-generation financial infrastructure. While these projects are not directly aimed at PQC, they force participating banks to resolve a series of core technical and operational challenges highly relevant to PQC migration, such as: complex digital asset key management, ensuring cryptographic interoperability between different technical platforms, and building modular and crypto-agile system architectures. By solving today’ s commercial problems posed by DLT and CBDC, Hong Kong banks are unknowingly building the necessary technical platform and organizational capabilities for tomorrow's PQC migration.

Industry Collaboration: The Role of the Hong Kong Association of Banks (HKAB): As the industry coordination body, the HKAB plays a key role in collaboration with HKMA, for instance, jointly developing industry guidelines such as the Secure Three-Level Data Backup (STDB). Although there are currently no dedicated PQC guidelines from HKAB, its past statements on cybersecurity issues (such as supporting risk-based and principle-based approaches rather than rigid rules) suggest that when the time for PQC migration is mature, HKAB will likely become the core platform for driving industry consensus and forming pragmatic solutions.

2.5.5 Comparative Analysis of Asia-Pacific and Middle East Models

A comparison of the PQC strategies in these four key financial centers—Japan, Singapore, Israel, and Hong Kong, China—reveals four distinct strategic archetypes. These differences provide important strategic reference for global financial institutions operating in multiple jurisdictions simultaneously.

Table 2-2: Comparative Analysis of PQC Strategies in Key Asia-Pacific and Middle East Financial Centers

Jurisdiction	Strategic Archetype	Primary Driver	Regulatory Stance	Key Initiatives	Pace and Timeline
Japan	Regulation-Driven Consensus	Financial System Stability	Directive Guidance	FSA/BOJ/NISC Joint Study Group	Coordinated, Prudent Progression

Singapore	Innovation Hub and Testbed	Innovation and Competitiveness	Consultation and Incentives	MAS Consultation and FSTI Grants	Proactive, Encouraging Experimentation
Israel	National Security Mandate	National Security	Mandatory Compliance	Bank of Israel Directive and INCD Mandate	Urgent, Forced Execution
Hong Kong, China	Pragmatic Ecosystem Evolution	Business Enablement and Fintech Growth	Awareness and Observation	HKMA "Fintech 2025" Strategy and HSBC Pilot	Gradual, Market-Led

This comparison clearly shows that global financial institutions must adopt a highly differentiated regional approach when formulating their PQC migration strategy. In Israel, compliance is the top priority, and banks must immediately respond to regulatory directives and initiate planning. In Hong Kong, the opportunity lies in participating in market-led innovation and exploring the commercial value of PQC through pilot projects. For banks with operations in multiple Asian financial centers, understanding and adapting to these different regulatory philosophies and market dynamics are crucial for successfully navigating the global quantum security migration wave.

2.6 The Regulator's Dilemma: How Uncertainty Makes Crypto-Agility a Strategic Imperative

Global financial regulators face a profound strategic dilemma in promoting PQC migration. This predicament stems from two intertwined, unavoidable uncertainties: first, the uncertainty of "when" migration must be complete—the exact emergence time of a cryptographically relevant quantum computer (CRQC) capable of cracking current cryptographic systems (often called "Q-Day") is unclear [19]; second, the uncertainty of "what to migrate to"—PQC algorithm standards are still evolving and maturing, and their long-term security and performance have not been tested by

decades of real-world use [15].

A regulator's core duty is to maintain financial stability, meaning they cannot wait until the threat is completely certain before taking action. The real threat of "Harvest Now, Decrypt Later" (HNDL) compels them to immediately drive the industry toward readiness [29]. However, if they prematurely mandate the entire industry to migrate to a specific new algorithm standard, they face a huge risk: that standard might be found vulnerable in the future or superseded by a more performant, more secure new standard. This would lock the entire financial system into a sub-optimal or even insecure technology, potentially requiring another costly and risky systemic migration in the future.

This double bind—neither inaction nor rash action is acceptable—fundamentally shifted the focus of regulatory attention. The ultimate goal of regulatory policy is no longer simply "replacing algorithm X with algorithm Y," but ensuring the financial system possesses an inherent capability to cope with future uncertainties. This capability is Crypto-Agility.

Crypto-agility is the ability of a system, platform, or application to rapidly adapt its cryptographic mechanisms and algorithms in response to evolving threats, technological advancements, or newly discovered vulnerabilities, without requiring a core architectural overhaul [13]. For regulators, mandating crypto-agility as a strategic requirement perfectly resolves their dilemma. By forcing financial institutions to build crypto-agile systems, regulators can:

Initiate Immediate Action: Regulators can require financial institutions to immediately begin modifying their systems for crypto-agility, without waiting for PQC standards to be fully finalized. This satisfies the urgency requirement of addressing the HNDL threat.

Mitigate Technology Bet Risk: Regulators do not have to pick a "winner" algorithm for the entire industry. They delegate the responsibility and flexibility of choice to the market while ensuring that regardless of which algorithm becomes the final standard, or if the standard changes, the system can transition smoothly.

Build Long-Term Resilience: Crypto-agility not only solves the immediate PQC migration problem but also prepares for any future cryptographic changes (e.g., new attacks driven by AI), thereby transforming a one-time emergency response into a sustainable, future-proof risk management capability.

Therefore, crypto-agility is elevated from a technical "best practice" to the core "strategic imperative" for regulators to manage uncertainty. It is the most rational and responsible policy choice regulators can make when they cannot predict the future. This shift also foreshadows the future trend of financial regulation: the oversight of FinTech systems will increasingly focus on the flexibility and adaptability of their architecture, rather than just their compliance with a static security standard. A system that cannot easily replace its core cryptographic engine will be considered inherently and unacceptably vulnerable in the future.

Chapter 3 The China Solution: Building an Autonomous and Secure Financial Post-Quantum Security Migration System

Facing the global quantum security challenge, China has put forward a set of "China Solutions" that are both forward-looking and systematic. This approach builds upon advanced international experience (such as NIST standards and the BIS framework) while incorporating the specific characteristics of the country's vast banking business scale and complex scenarios. Spearheaded by the national key Research and Development program and executed through top-level design, this solution constructs an innovative migration framework and management theory system, demonstrating the unique governance advantage of a "dual-wheel drive" powered by technological R&D and management specification.

3.1 National Strategic Layout: Major Special Project for Research on Post-Quantum Security Migration Technology in the Financial Sector

China's post-quantum security migration work is conducted under the unified layout of a national strategy. The core vehicle for this strategic layout is the "14th Five-Year" National Key R&D Program project, initiated by the Ministry of Science and Technology, titled: "Research on Post-Quantum Cryptography Migration Technology for the Banking Sector and Its Critical Infrastructure Information Systems." The project is led by the Financial Research Institute of the People's Bank of China and unites top domestic universities, scientific research institutions, and financial technology enterprises, such as Tsinghua University, to form a powerful national team for collaborative research across "industry, academia, and research." The establishment and development of the Post-Quantum Migration Cross-Disciplinary Laboratory (PQC-X) at Xi’ an Jiaotong-Liverpool University, as one of the important landmark achievements of this national key R&D program, typically embodies the vitality of this strategic layout, ensuring that the national special project can not only theoretically conquer world-class problems such as the SVP-200 problem and the Kyber-208

instance but also rapidly translate the technical insights of the "strongest spear" into the "most solid shield" protecting the digital economy.

This organizational model itself reflects China's unique advantage in responding to major strategic challenges: by being led by the national will, it can concentrate the highest quality resources, break down institutional barriers, and conduct efficient collaboration around a common goal. The overall design of the project also embodies a high degree of systematicity, distilling a vertical dual-closed-loop system from theory to practice:

Overall Project Framework:

Data-Driven Agile Migration Framework: Defines the methodology for post-quantum cryptography migration in banking information systems.

Quantum Security Early Warning Model and Management Specifications: Proposes full-process management recommendations for pre-event, in-event, and post-event risk prevention and control.

Various Common Key Technologies:

Post-Quantum Cryptography Algorithms: Design and evaluate algorithms based on lattice, multivariate, hash, and other technology routes.

Efficient Software and Hardware Implementation: Research and development of efficient implementation technology for algorithms on different platforms (servers, mobile terminals).

Security Protocols: Design multi-source heterogeneous post-quantum cryptographic basic protocols that support smooth transition.

The project also includes 4 technical engines (algorithm library, implementation resource pool, protocol library, evaluation toolset) and 3 major application scenario verifications (mobile banking, online banking, interbank clearing), ultimately aiming to form an implementation path for post-quantum cryptography migration

applicable to the Chinese banking sector. This structure covers the entire lifecycle of PQC migration from theory, technology, tools, to application, demonstrating an overall design with clear goals, a well-defined path, and systematic completeness.

3.2 Top-Level Framework Innovation: Detailed Explanation of the "Data-Driven PQC Agile Migration Framework for Banking"

Among the many achievements, the "Data-Driven PQC Agile Migration Framework for Banking" proposed by the project team is the most methodologically innovative. This framework embodies China's unique innovation in PQC migration methodology.

The Western model (such as JPMorgan Chase) starts with "Inventory" of existing assets, which is a static, technology-component-centric perspective. The core question is, "Which cryptographic algorithms and certificates in our system need to be replaced?" [13]. In contrast, China's "Data-Driven" framework is a dynamic, business-process-centric perspective, representing an important complement and evolution to existing international general frameworks. This difference in methodology is not a simple procedural adjustment but a fundamental philosophical shift. It does not first ask a technical question ("What do we have?") but first asks a business and risk question ("What is the data and how does it flow?"). The core question is, "What is our most important financial data? How is it generated, transmitted, processed, and stored in the business process? What level of security protection is needed at which key nodes?"

This cognitive upgrade from "replacing cryptography" to "protecting data" has brought about a fundamental change in methodology and inherently links the migration project to business priority and risk management. It ensures that limited resources are first invested in protecting the highest-value assets, providing a risk-based prioritization mechanism that is highly convincing to both the board and supervisory authorities. The framework takes "data" as the core element throughout the entire migration process:

With Data Flow as the Main Line: Tracks the complete life cycle of core data in

business systems and identifies all contact points.

With Data Type as the Criterion: Classifies and prioritizes migration work based on data sensitivity, confidentiality period, and other attributes.

With Data Compatibility as the Benchmark: Measures the compatibility of the new PQC solution with existing data formats and processing procedures as a standard for assessing the "agility" of the migration solution.

With Data Effectiveness as the Basis: Evaluates the final effectiveness of the migration work by verifying whether the availability, integrity, and confidentiality of the migrated data are guaranteed.

The framework is specifically divided into five major steps: identification of existing cryptographic module functions, analysis of important business data assets, migration risk assessment, migration implementation, and effect verification. This design not only draws upon the ideas of international general frameworks such as NIST but is also deeply customized and optimized for the actual scenarios of the Chinese banking sector, giving it stronger operability and foresight. This framework has been introduced at the international conference on "Quantum Readiness" for central banks organized by the Bank for International Settlements (BIS) and has attracted high attention from central bank representatives from various countries.

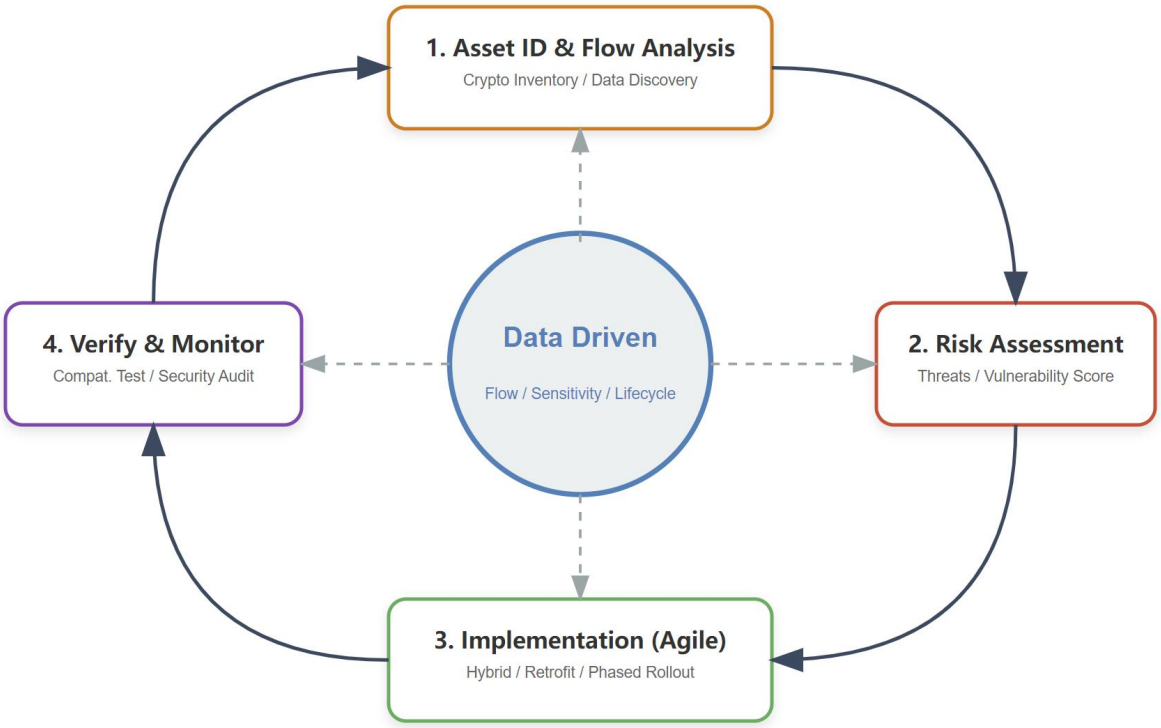

Figure 3-1: Data-Driven Agile Post-Quantum Migration Framework for Banking

3.3 RegTech Foresight: The "Risk Identification - Assessment and Early Warning - Migration Management" Trinity Theory System

Another major feature of the China Solution is the "dual-wheel drive" of technological R&D and management specification. In the West, technical standards and industry practices usually lead, and regulatory policies often lag. In contrast, the Chinese model advances technological research in parallel with the formulation of compliance theory and specifications, which demonstrates a unique governance advantage that can effectively shorten the cycle from technical feasibility to industry compliance, ensuring that the national strategy can be implemented quickly and collaboratively.

The project team has achieved a series of forward-looking results in RegTech, systematically constructing the "Risk Identification - Assessment and Early Warning - Migration Management" trinity theory framework for the entire chain:

Risk Identification: Through on-site research and system architecture analysis of domestic commercial banks, the project team for the first time systematically sorted out the quantum vulnerabilities of banking information systems at the algorithm layer (such as RSA, SM2), protocol layer (such as TLS), hardware layer (such as servers, cryptographic machines), and business layer (such as digital signatures, data storage). Based on this, it innovatively created a "Risk Point Checklist and Contagion Map," which intuitively reveals how a quantum attack can trigger systemic risk through paths such as bank runs and financial market volatility.

Assessment and Early Warning: Innovatively constructed an intelligent early warning model that includes three core modules: Threat Perception, Risk Assessment, and Early Warning Response. The model comprehensively uses risk matrices, complex network analysis, and other methods to organically combine asset classification, threat level, and vulnerability score, achieving full-cycle risk management from pre-event prediction, in-event monitoring, to post-event disposal, providing a precise quantitative risk monitoring tool for management departments.

Migration Management: More significantly, the project team took the lead internationally in providing compliance guidance for commercial banks to mitigate the quantum computing threat, filling a gap in domestic management specifications. This means that future migration work will have laws to follow and standards to rely on, providing clear basis for Chinese banking management departments and ensuring that migration work across the entire industry is unified in standard and coordinated in pace.

This means that when China's PQC technical solutions and toolsets mature, their promotion and implementation across the entire industry will be backed by clear regulatory basis and management guidelines. This model of coordinated advancement of technology and compliance can effectively overcome the "migration inertia" that a single commercial bank might have due to cost, risk aversion, and other factors, ensuring the integrity, synergy, and timeliness of the national financial security upgrade.

Chapter 4 Strengthening the Foundation: Solidifying the Core Post-Quantum Cryptography Capabilities for National Financial Security

If the top-level design maps out the blueprint for China's PQC migration, then a series of autonomous breakthroughs in core technologies provide the solid "materials" and "tools" for realizing this blueprint. Through focused efforts on major national special projects, China has achieved a series of world-leading results in key areas such as algorithms, software and hardware implementation, protocols, and supporting tools, preliminarily constructing an autonomous technological post-quantum cryptography “toolkit.”

4.1 Building the Algorithm System: Autonomous Innovation in Lattice-Based, Multivariate, and Hash-Based Cryptography

Algorithms are the cornerstone of the cryptographic system. In PQC algorithm research, China has not only tracked and optimized international mainstream algorithms but also achieved a defining-level breakthrough in the core security analysis domain, realizing a leap from "algorithm application" to "algorithm definition."

Lattice-based Cryptography: Lattice-based cryptography is the core technological route for the first batch of NIST standardized algorithms [25]. The Chinese project team has achieved significant breakthroughs in this field. By innovatively designing "efficient lattice-based cryptography attack implementation for multi-level cache architecture" and "mixed-precision computing and storage compression technology," the team has greatly enhanced the engineering efficiency of solving the core difficult problem of lattice cryptography—the Shortest Vector Problem (SVP).

Special Topic: The "Duet" of Chinese Power—From Solving the SVP-200 Problem to Conquering the Kyber-208 Instance

Based on the aforementioned technological innovations, the project team, leveraging

the top scientific research strength of the PQC-X Laboratory, set two world records in lattice cryptography analysis in 2025, completing full-dimensional verification from the "underlying mathematical foundation" to the "upper-layer algorithm standard":

Foundation Breakthrough (March 2025): The team globally pioneered the efficient solution of the SVP-200 problem. The measured overall attack efficiency was more than 30 times higher than international mainstream tools (such as G6K), proving China's computing power and algorithmic advantages in tackling core lattice cryptography mathematical challenges.

Instance Conquest (November 2025): The team successfully cracked the Kyber-208 instance in the Bochum Challenges. Kyber-208 is a "non-standard" and intentionally weakened challenge version of the NIST final standard ML-KEM (Kyber).

Strategic Significance: Casting the "Most Solid Shield" with the "Strongest Spear"
The strategic significance of these two breakthroughs far exceeds the academic level. Conquering Kyber-208 is not just a Deep Security Evaluation of the algorithm parameters but also precisely delineates the boundary of current cryptanalysis technology. As the core logic of the PQC-X Laboratory suggests: constructing a highly trusted defense system must be built upon a profound understanding of the most advanced cryptanalysis techniques. Because the team deeply understands (and is even inventing) the most cutting-edge attack techniques like BKZ, they can accurately reserve sufficient "security margin" when designing or evaluating PQC standards adopted by the national financial system, rather than just passively accepting international parameters. This "Algorithm Definition and Auditing" capability is the core confidence ensuring the long-term security of the Chinese financial system against future unknown attacks.

4.2 Coordinated Software and Hardware Implementation: From Post-Quantum Server Cryptographic Modules to Mobile SDKs

Powerful algorithms require efficient and secure software and hardware carriers to be effective. The core principle of the soft- and hardware system design in this solution

is "standard compatibility and smooth evolution." We particularly emphasize deep compatibility with current commercial cryptographic standards, ensuring PQC migration is an upgrade and integration of existing financial cryptographic infrastructure, rather than a destructive replacement, thereby maximizing business continuity.

4.2.1 Hardware Core—Multi-Modal Post-Quantum Server Cryptographic Module

The project team successfully developed a high-performance prototype of an "Post-Quantum Server Cryptographic Module." This device exhibits a high degree of flexibility and inclusiveness in its technical implementation: it not only efficiently supports international mainstream post-quantum cryptographic standards but also is fully compatible with locally widely used current commercial cryptographic standards.

More critically, the device has completed deep adaptation and performance stress tests in diverse computing environments, covering everything from international mainstream general architectures to localized high-performance computing platforms and operating systems. This broad adaptability proves that the solution possesses the capability to operate stably across different supply chain environments, providing financial institutions with reliable hardware options for building highly resilient, diversified security infrastructure, effectively reducing reliance on a single hardware supply chain.

4.2.2 Software Ecosystem—Full-Stack Adaptation Solution

Centered around the hardware core, the project built an end-to-end software support system aimed at addressing performance bottlenecks in different computing scenarios:

Heterogeneous Computing Acceleration Modules (GPU/FPGA): Specifically optimized for high-throughput, high-concurrency high-performance computing scenarios.

General Platform Cryptographic Modules: Implemented an efficient post-quantum cryptographic algorithm library on mainstream general processor architectures, ensuring widespread applicability.

Mobile SDK Development Package: Conducted deep instruction set optimization for mainstream mobile operating systems, solving the resource limitation challenges of mobile devices and providing lightweight security support for mobile applications like mobile banking.

This full-stack software ecosystem provides banks with end-to-end smooth migration capability from cloud-based core systems to mobile terminals.

4.3 Protocol Library and Toolset: Certificates, Protocols, and Evaluation Tools Supporting Smooth Migration

To translate the underlying algorithmic and software/hardware capabilities into usable services and support complex migration engineering, the project also developed a series of upper-layer protocols and supporting tools.

4.3.1 Protocol Innovation

Targeting "asynchronous migration" scenarios where different institutions have varying migration progress, the project team designed a flexible "heterogeneous key exchange mechanism," allowing communicating parties to establish connections using different types of long-term keys during the transition period (e.g., one party uses a signature, the other uses key encapsulation). Concurrently, mainstream secure communication protocols were adapted for post-quantum/hybrid mode, and the standard format for digital certificates was extended as necessary to accommodate hybrid signatures of classical and post-quantum algorithms. These improvements ensure that new and old protocols can coexist in complex legacy systems, achieving a smooth transition and backward compatibility during the migration process.

4.3.2 Supporting Toolset

The project developed a complete set of professional tools to support the migration project, transforming migration from a purely code upgrade into a manageable, evaluable, knowledge-retaining system engineering:

Next-Generation Digital Certificate Management Tool: Used to generate and issue post-quantum and hybrid-mode digital certificates supporting new-generation encryption protocols.

Migration Security Evaluation Software: Provides a standardized set of evaluation metrics and automated tools for objectively assessing the security and compliance of migration solutions.

Post-Quantum Cryptography Migration Knowledge Base: Compiles a wealth of algorithm characteristics, configuration strategies, and best practice entries, providing a shared knowledge repository for the industry.

This complete set of autonomous technological "tools" fundamentally guarantees that the Chinese financial industry, when conducting post-quantum security migration, will have secure, reliable, and efficient technical support, thereby building a financial security infrastructure with high resilience and supply chain independence.

4.4 The Diversity of the Global Cryptographic Ecosystem: Building Technological Resilience

post-quantum cryptography migration is a systemic project concerning the stability of global financial infrastructure. With the deepening of digitalization, the diversity of the technology supply chain and its resilience against risks have become core strategic considerations for all nations. "Cryptographic Technology Autonomy Capability"—the ability of a country or region to independently evaluate, implement, and maintain its digital security infrastructure—has become the key driver for building a highly resilient financial system.

This geopolitical contest is playing out along three main paths:

United States: Driving Global Consensus through Standardization. The US NIST established globally adopted technical benchmarks through an open and transparent PQC algorithm solicitation process [25]. This strategy, by converging global scientific wisdom, effectively reduced the complexity and fragmentation risk of industry migration, providing a vital public technical product for the smooth transition of the global financial system.

China: Pursuing Autonomous Control to Promote Equal Cooperation. The core of China's strategy is "autonomous control," but this does not imply a move towards "isolation"; rather, it aims to establish a solid foundation for equal international cooperation. Its core objective is to ensure that the nation's critical information infrastructure, especially the financial system, possesses the independent survival capability that does not rely on external technology [21]. Therefore, China adopts a strategy of "self-reliance while being inclusive": while investing massive resources in developing an autonomous PQC algorithm system and building a technological "moat," it maintains an open posture, actively participating in international standard discussions and development. This approach is designed to ensure the capability for independent security auditing and underlying principle verification in any geopolitical environment, which aims to avoid systemic risk due to potential unknown vulnerabilities in a single global algorithm standard, thereby ensuring the digital economy infrastructure has a high degree of autonomy and survival resilience [41], and thus deepening international cooperation from a position of profound technological accumulation.

Europe: Seeking Strategic Autonomy. While largely aligned with NIST standards, Europe also has a strong demand for "digital sovereignty" internally [28]. The EU's goal is to avoid complete reliance on the US for critical technologies. Therefore, it actively supports local European PQC research and industry ecosystems, and may, in future standard adoption, favor algorithms where European researchers have deep contributions and understanding, to maintain strategic flexibility and autonomy.

This developing landscape means that global financial institutions will operate in a more complex and fragmented cryptographic environment in the future, which

can be termed "Balkanization of Trust." A multinational bank may need to deploy a NIST-standard system in one jurisdiction and support local autonomous standards in another. This will greatly increase the difficulty of interoperability and compliance costs, elevating the choice of cryptographic algorithms from a purely technical decision to a strategic decision that requires comprehensive consideration of geopolitical risks. In the future, network infrastructure may need complex new functions like "cryptographic routing" and "policy-based encryption," which dynamically select the appropriate encryption standard based on the transaction's source, destination, and jurisdiction law.

Mutual Recognition of PQC Standards is becoming the cornerstone of cross-border financial cooperation. Shared encryption standards help build technological mutual trust between different jurisdictions and reduce compliance costs. For example, some countries are establishing mutual recognition mechanisms to build regional trustworthy technology ecosystems. Conversely, standard incompatibility can lead to the risk of global financial infrastructure fragmentation, increasing the operational complexity for multinational banks.

Chapter 5 Early Adoption: Migration Demonstration and Path Confirmation in Key Financial Business Scenarios

The advancement of theory and the breakthroughs in technology must ultimately be tested through practice in a real business environment. China's PQC migration research has not remained at the laboratory stage but has delved into actual financial business scenarios, carrying out systematic engineering verification. This series of verification efforts has gone beyond simple "Proof of Concept" and entered the deeper "Proof of Engineering" stage, with the core goal of answering "How can PQC work at scale and with low risk in complex production systems."

5.1 Customer Access Scenarios: Agile Migration Verification for Mobile Banking and Online Banking

Customer access scenarios are the front lines of banking services, directly affecting user experience, and their migration faces unique challenges.

Scenario Characteristics and Pain Points:

Mobile Banking: Features complex business logic (login, transfer, password reset), faces high-concurrency access pressure, and runs on mobile terminals with limited computing and memory resources, as well as diverse operating systems and hardware models. The larger computational overhead and memory footprint of PQC algorithms are the main challenges.

Online Banking: Generally relies on physical hardware—USB-based cryptographic tokens (U-Shields)—for transaction signing. The embedded environment of the U-Shield has extremely limited computing power, making it difficult to bear complex PQC signature algorithms. Furthermore, compatibility with browser security plugins is a major difficulty.

Verification System Design and Outcomes: Targeting the above pain points, the

project team designed and developed specialized migration verification systems.

Mobile Banking Verification System: Integrated the mobile PQC SDK developed by the project team and conducted full-link testing on core processes like login and transfer under simulated real high-concurrency loads. The verification results showed that, through deep optimization of the SDK, acceptable user response latency can be achieved on mainstream mobile devices, ensuring the smoothness of business operations.

Online Banking Verification System: Simulated the complete process of a user using a U-Shield for transaction signing, focusing on verifying the smooth switching between PQC signature algorithms and Chinese National Standard Algorithms (SM series) in embedded hardware and browser plugin environments. Through synergy with hardware cryptographic modules and other achievements, feasible solutions were explored for offloading some computing load to the back-end.

5.2 Core System Scenario: End-to-End Migration Verification of Interbank Clearing Systems

Interbank clearing is the "aorta" of the financial system, and its migration verification is the ultimate test of PQC solutions in scenarios requiring the highest security and reliability.

Scenario Characteristics and Pain Points: Interbank clearing business is characterized by high single-transaction amounts, coordination among multiple parties (originating bank, receiving bank, central bank payment system), long transaction links, and extremely stringent requirements for business continuity and data consistency. A signature or verification failure at any single node could lead to clearing blockage and trigger a chain reaction. Therefore, synchronized upgrade and seamless switching among multiple nodes are the greatest difficulties.

Verification System Design and Outcomes: The project team built a highly simulated

interbank clearing migration verification system, mimicking the end-to-end transaction link of commercial banks clearing through the People's Bank of China's High-Value Payment System (HVPS). By injecting real clearing messages into this link, the stability, fault tolerance, and performance of the PQC algorithm were systematically tested in a multi-node, long-link complex environment. In particular, the system verified the effectiveness of gray release and risk rollback mechanisms: it could switch a portion of the transaction traffic to the new PQC channel in batches while monitoring clearing latency and failure rates in real-time, and in case of an anomaly, immediately roll back to the traditional Chinese National Standard Algorithms (SM series) channel, ensuring seamless connection and high availability of core business.

5.3 Migration Pain Point Analysis and Chinese Characteristic Solutions

Combining international experience and in-depth domestic verification, five major common pain points for PQC migration can be summarized:

Performance Overhead: Computational, storage, and network bandwidth overhead brought by PQC algorithms.

Algorithm Uncertainty: Algorithms are still evolving, and there is a risk of future breaches.

Business Continuity: The migration process requires zero or minimal interruption.

Multi-Node Coordination Risk: In complex systems, single-point failures can be magnified in cascade.

Multi-Environment Compatibility: The need to adapt to heterogeneous software and hardware technology stacks.

To systematically address these pain points, the China Solution proposes a critical

infrastructure: the "Post-Quantum Cryptography Migration Experimental Platform." This platform, led by the national project, is not a simple testing tool but a public "PQC Migration Firing Range" and "Drill Center" for the entire banking industry. It integrates two core capabilities, Engineering Verification and Gray Evolution, providing a unified algorithm library, protocol library, key management, policy scheduling, and monitoring capabilities for the verification systems of the three scenarios mentioned above.

This "Platform + Scenario" systemic verification model is a major innovation of the China Solution. It avoids the need for individual banks to invest heavily in repetitive algorithm selection, performance testing, and compatibility verification, greatly reducing the barrier and cost of migration for the entire industry. By conducting collaborative drills on this unified platform, industry consensus and best practices can be formed more quickly, accelerating the overall migration process of the entire industry—an achievement difficult to realize through purely market-driven, fragmented models.

Chapter 6 Foresight: Global Synthesis and Strategic Outlook

As the global financial industry's PQC migration moves from concept to practice, the strategic paths of different countries and the explorations of industry pioneers reveal shared challenges, emerging best practices, and profound shifts in the future competitive landscape.

6.1 Comparative Analysis: Comparison of National Migration Models

Countries worldwide have adopted distinct strategic models in response to PQC migration, shaped by their political systems, economic structures, and regulatory cultures. The core differences in these models lie in the primary driving force for migration, the method of regulation, the strategic focus, and the most critical risk concern underlying their approach.

Table 6-1: Comparative Analysis of National PQC Migration Strategies

Country/ Region	Primary Driving Force	Regulatory Method	Strategic Focus	Core Risk Concern
United States	Market/Vendor Ecosystem	Mandatory directives for federal agencies; guidance for the private sector	Fostering a robust PQC product and service market, with market forces driving private sector adoption	Federal Business Continuity/Market Cultivation
United Kingdom	Regulatory Mandate	Clear, cross-industry migration deadlines for critical infrastructure	Ensuring the overall resilience of national critical infrastructure, avoiding weak links	Critical Infrastructure Resilience

Canada	National Coordinated Strategy	Government roadmap with mandatory force, emphasizing unified procurement standards	Coordinated migration of critical infrastructure, reducing overall transition costs	Critical Infrastructure Coordination/Cost-Effectiveness
Japan	Regulatory Body/Industry Consensus	Regulatory body-led workshops forming unified industry guidance	Maintaining the systemic stability of the entire financial sector, avoiding disorderly migration	Systemic Financial Stability
Switzerland	Industry Self-Regulation/Risk Management Culture	Principle-based regulation, expecting institutions to proactively manage risk, no hard timeline	Encouraging proactive, risk-based defense, maintaining the reputation and competitiveness of the financial center	Reputation Risk/Market Trust
China	National Strategic Will	Top-down design and unified standard directives	Achieving technological self-reliance and national-level cryptographic autonomy	Technological Sovereignty/Systemic Stability
Israel	National Security	Mandatory compliance directives	Rapid mitigation of risks to sensitive national data	National Security/Data Anti-Infiltration

6.2 Unifying Theme: Common Challenges and Emerging Global Best Practices

Despite diverse strategic paths, global financial institutions face highly consistent challenges in PQC migration, which have led to a set of widely accepted best practices.

Common Challenges:

Talent Scarcity: Globally, talent with PQC expertise is extremely scarce, a key bottleneck constraining migration speed.

Complex Vendor Ecosystem: Financial institutions are highly reliant on third-party software and hardware vendors and cloud service providers, making the coordination of synchronized PQC upgrades across the entire supply chain a daunting management task [30].

Heavy Legacy System Burden: Numerous legacy systems with hard-coded old cryptographic algorithms are difficult, costly, and risky to retrofit, presenting a major obstacle in the migration process [33].

High Costs and Resource Investment: PQC migration is a systemic project involving the entire institution and lasting many years, requiring significant financial and human resource investment [41].

Hybrid Deployment Architectural Pitfalls: The real-world experience from Phase 2 of the BIS "Project Leap" indicates that the theoretically perfect "Hybrid Model" faces significant challenges in engineering implementation. Many legacy financial software systems were not designed to support multiple cryptographic schemes simultaneously, making dual-signing difficult to implement at the application layer (e.g., in message header signatures) and often requiring intrusive restructuring of the software architecture.

Emerging Best Practices:

Universal Adoption of the "Inventory-Assess-Prioritize-Remediate" Framework: From JPMorgan Chase to Japan's Financial Services Agency, this clear logical migration process has become a global standard [13].

Emphasis on Senior Management Support: Given the long-term and complex nature of the migration, securing support and commitment from the board and CEO level is considered a prerequisite for project success.

Proactive Vendor Management: Leading institutions no longer passively wait for vendors but actively communicate PQC requirements, evaluate vendor roadmaps, and incorporate these requirements into contracts [30].

Establishing Collaboration and Alliances: Whether joining industry alliances like FS-ISAC, QSFF, or establishing partnerships with academia and technology companies, sharing costs and knowledge through collaboration has become a consensus [28].

6.3 The Catalyst for Modernization: Implicit Strategic Benefits of PQC Migration

While the direct driver for PQC migration is to mitigate future quantum threats, the process itself brings profound "implicit" strategic benefits to financial institutions that go beyond the scope of security. It is becoming a powerful catalyst for enterprise IT governance and infrastructure modernization.

For a long time, many financial institutions have accumulated significant, poorly recognized and managed "cryptographic debt"—outdated, hard-coded, and unmanaged cryptographic implementations scattered across legacy systems [24]. This debt not only poses potential security risks but also makes system maintenance and upgrades exceptionally difficult and expensive.

The mandatory requirement of PQC migration fundamentally changes this situation. The first step of migration, a comprehensive cryptographic asset inventory, compels institutions to thoroughly examine all cryptographic dependencies across their entire technology landscape for the first time [2]. This unprecedented visibility provides Chief Information Security Officers (CISOs) and Chief Technology Officers (CTOs) with a powerful, risk-based business case to address a range of long-standing, deep-seated IT governance issues. This external threat-driven internal change offers a rare opportunity for technology leaders to gain the budget and executive authorization previously unattainable.

Specifically, PQC migration becomes a "catalyst" for the following modernization processes:

Improved Asset Management and Cybersecurity Hygiene: By establishing a dynamic, comprehensive Cryptographic Bill of Materials (CBOM), institutions not only prepare for PQC migration but fundamentally enhance their asset management capability and overall cybersecurity hygiene.

Accelerated Retirement of Legacy Systems: The inventory process clearly identifies legacy systems that cannot undergo cryptographic upgrades due to rigid architecture. This provides undeniable evidence to drive the retirement or restructuring of these systems, thereby helping enterprises shed technological burdens and reduce operational costs and risks [33].

Strengthened Software Supply Chain Security: The migration process requires in-depth communication with all third-party vendors, evaluation of their PQC roadmaps, and making crypto-agility a contractual requirement [30]. This greatly enhances the institution's security visibility and control over its software supply chain.

Driving Architectural Modernization: To achieve crypto-agility, institutions must decouple cryptographic functions from business logic in system design. This naturally drives an evolution toward more modern, flexible modular or microservices architectures, making the entire IT system capable of not only addressing future cryptographic changes but also responding faster to business needs.

Therefore, the most strategically minded financial institutions will not view PQC migration merely as a cost of compliance. Instead, they will seize this once-in-a-generation opportunity to leverage the budget and executive authorization for PQC migration as a lever to drive broader digital transformation and IT infrastructure modernization. Institutions that succeed in this will, upon completion of the migration, gain not only quantum security assurance but also a leaner, more agile, and more competitive technology platform.

6.4 Strategic Recommendations: Quantum Security Migration Action Manual for Global Chief Information Officers

Based on global progress and challenges, the following strategic actions are recommended for financial institution leaders:

Immediately Establish a Quantum Governance System: Appoint a dedicated quantum project lead or team and ensure the issue is regularly reviewed and supported at the board level.

Treat Cryptographic Asset Inventory as a Strategic Asset: Go beyond a one-time checklist by committing to building a dynamic, automated Cryptographic Bill of Materials (CBOM), making it the basis for real-time risk management and decision-making.

Embrace a Dual "Offense and Defense" Strategy: Develop a comprehensive quantum roadmap that includes both defensive PQC migration to mitigate risk and the exploration of offensive quantum computing applications to create new business value.

Prioritize Crypto-Agility in All Procurements: Make crypto-agility a non-negotiable requirement for all new technology procurements and system designs, preparing for future uncertainty.

Invest in the Talent Pipeline: Emulate the model of the Royal Bank of Canada by collaborating with universities and investing in internal training and certification systems to build a sustainable internal talent pool.

Actively Participate, Collaborate, and Lead: Avoid being a passive observer. Actively join industry forums like FS-ISAC and QSFF, participate in pilot projects, and have a voice in open-source tools and standard setting, collectively shaping the industry's future by sharing the burden.

Finally, PQC migration is revealing a new geopolitical dimension—"cryptographic

technology autonomy." The Chinese White Paper explicitly links it to technological self-reliance, while Western countries, alongside aligning with US NIST standards, are also developing their own cryptographic capabilities. In the future, a nation or economy's choice of PQC algorithm and standard may not just be a technical decision, but a strategic and political tool that influences the interoperability of the global financial system. This requires global financial institution leaders to view and plan for this inevitable quantum security migration with a higher strategic vision.

6.5 Executive-Level Authorization: Quantum Security Migration Action Manual for Commercial Bank Decision-Makers

The threat posed by quantum computing is no longer a distant theoretical discussion but a real and increasingly imminent challenge to banks' core businesses. The "Harvest Now, Decrypt Later" (HNDL) attack model means that the long-term sensitive data encrypted by banks today is exposed to the future risk of quantum computer decryption [1]. Therefore, addressing the quantum threat has transcended the technical scope of the IT department and risen to a strategic and governance issue that the board and top management must directly confront, concerning the bank's long-term survival and reputation. This manual aims to provide a clear action framework for commercial bank boards and C-level executives, breaking down the complex quantum security migration task into five manageable and supervisable strategic pillars.

Pillar I: Governance and Board-Level Accountability—"Asking the Right Questions"

Quantum risk is a foreseeable major risk, and effective oversight of management's response to this risk is an inherent part of the board's Fiduciary Duty. The board does not need to be cryptographic experts but must drive the organization's preparedness by asking the right questions.

Establish Ownership: The board should ensure a C-level executive (such as the Chief Risk Officer CRO or Chief Operating Officer COO, not just the Chief Information

Security Officer CISO) is appointed as the overall lead for the quantum readiness program. This ensures the program receives cross-business resources and attention, preventing it from being treated as an isolated IT project.

Board's Quantum Risk Checklist: The board should include the following questions in their regular agenda to query management:

> Risk Quantification: "Have we quantified the potential financial and reputational losses to our bank's most sensitive data (e.g., M&A plans, core customer long-term financial data, strategic intellectual property) from a quantum attack? What is the extent of the impact?"
>
> Asset Inventory Progress: "What is the timeline for completing a bank-wide cryptographic asset inventory? What is the current progress? Does the scope cover all legacy systems, subsidiaries, and cloud environments?"
>
> Supply Chain Risk: "How are we assessing the quantum readiness of key third-party vendors (especially core banking systems and cloud service providers)? Have we incorporated crypto-agility and PQC migration requirements into new procurement contracts and renewal terms?[30]"
>
> Dual Offense-Defense Strategy: "Beyond defensive PQC migration, what is our bank's 'offensive' strategy? Are we exploring the use of quantum computing to create new business value in areas like risk modeling, portfolio optimization, or new drug discovery?"

Pillar II: Strategic Investment and Resource Allocation—"Beyond the Cost of Compliance"

Viewing PQC migration merely as an IT compliance cost is strategically shortsighted. Decision-makers must re-position it as a fundamental strategic investment in the bank's digital resilience and customer trust for the next decade.

Redefine the Investment Narrative: Management must clearly articulate to the board that the essence of this investment is to maintain the bank's core competitiveness in the digital age—trust. Its importance is no less than building a new data center or entering a new strategic market.

Measure the Cost of Inaction: Historical major data breaches have proven that the cost of cleanup (including fines, lawsuits, customer attrition, and brand damage) far exceeds the upfront cost of prevention. A systemic breach triggered by a quantum computer would have catastrophic consequences. While proactive migration is costly, it is minimal compared to potential losses [11].

Approve Multi-Year Special Budget: The board should approve a multi-year, protected (ring-fenced) special budget for quantum readiness. This budget should be separate from the annual IT operating budget to ensure project continuity and stability, preventing interruption due to short-term performance pressure. The budget should comprehensively cover all critical elements, including asset inventory, risk assessment, system modification, talent development, and pilot projects.

Special Note: Implicit Cost of Computing Infrastructure The board must realize that PQC migration is not just a software upgrade but a computing power challenge. BIS test data shows that PQC digital signature verification takes about 7.5 times longer than traditional RSA algorithms (209.9ms vs 28.1ms). This means that existing server resources may face severe bottlenecks if current transaction speed (TPS) and user experience are to be maintained. Therefore, budget planning must include the cost of large-scale high-performance server expansion or dedicated hardware accelerator card (e.g., FPGA/GPU) procurement to cope with the surging computational load of the "post-quantum era."

Pillar III: Integration into Enterprise Risk Management (ERM)—"Making the Threat Measurable"

As long as quantum risk remains in the jargon of the IT department, it will not receive the attention it deserves. It must be liberated from the technical silo and fully integrated into the bank's Enterprise Risk Management (ERM) framework.

Definition and Classification: Like credit risk, market risk, and operational risk, quantum risk needs a clear definition within the bank's ERM framework. Management should instruct the risk department to use the bank's existing risk quantification models as templates to assess and grade quantum risk.

Quantifying the Risk Level: Quantum risk levels (e.g., High, Medium, Low) can be set for different systems and data assets based on the following dimensions:

Data Confidentiality Period: How long does the data's value last? Strategic data needing 50 years of confidentiality poses a far higher risk than transactional data needing only 24 hours.

System Criticality: Is the system essential for the bank's survival? The risk level of the payment clearing system is much higher than that of the internal human resources system.

Migration Difficulty and Time: The time and resources required to retrofit a large, aging core system far exceed those needed to upgrade a modern, microservices-based application.

Setting Risk Tolerance: Based on the above assessment, the board must formally review and approve the bank's "Quantum Risk Tolerance Statement." For example, the board might decide on a "zero-tolerance" strategy for payment systems and core customer data, while accepting higher residual risk for some non-critical systems. This statement will serve as the supreme guideline for prioritizing migration and allocating resources across the entire bank.

Pillar IV: Capturing Quantum Opportunity—"Developing a Forward-Looking Innovation Strategy"

A strategy that only defends is destined to be mediocre. The same quantum revolution that triggered PQC migration also brings disruptive commercial

opportunities to the banking sector [10]. A comprehensive quantum strategy must balance defense and innovation, mitigating risks by steadily advancing PQC migration while also innovating on the business side.

Identify Value Pools: Decision-makers should drive strategic departments to identify core areas where quantum computing can create significant commercial value:

Risk Management: Turkey's Yapi Kredi Bank has partnered with D-Wave to use quantum computing to analyze systemic risk in its corporate customer network, reducing calculations that would have taken years to just seconds [12]. This enables more precise and real-time risk monitoring [11].

Portfolio Optimization: Quantum algorithms can handle large-scale, multi-constraint optimization problems intractable for traditional computers, thereby constructing portfolios with better risk-return ratios [9].

Financial Derivatives Pricing: By accelerating compute-intensive tasks like Monte Carlo simulations, quantum computing is expected to achieve faster and more accurate pricing of complex derivatives [9].

Take Action: The board should support management in establishing an independent "Quantum Enablement Exploration Group" to work synergistically with the PQC migration team responsible for infrastructure security. The group's mission is to establish partnerships with leading quantum computing companies and research institutions and carry out small-scale, high-impact proof-of-concept projects, establishing a first-mover advantage for the bank's new business growth points in the quantum era.

Pillar V: Leading Ecosystem Transformation—"The Bank is Not an Island"

A bank's quantum security depends on the security level of its entire ecosystem (vendors, partners, customers). Therefore, bank leaders must act as catalysts for

ecosystem transformation.

Proactive Supply Chain Management: A bank's quantum readiness plan cannot stop at its own firewall. Top management must authorize procurement and legal departments to issue clear PQC roadmap inquiries to all key technology vendors (including software developers, hardware manufacturers, and cloud service providers) and make crypto-agility a mandatory clause in all future contracts [39].

M&A and Investment Due Diligence: Instruct the bank's M&A and venture capital teams to include "quantum risk" and "cryptographic debt" in the core due diligence checklist. Acquiring a company with a large amount of unmanaged, hard-coded encryption is equivalent to swallowing a massive, invisible liability.

Shape Strategic Communication: Develop a proactive and transparent communication strategy targeting regulators, major investors, and large corporate clients. Communicate the bank's quantum readiness plan as strong evidence of sound governance and strategic foresight, thereby transforming a risk mitigation effort into a strategic opportunity to build and consolidate market confidence.

By positioning quantum security migration within the grand framework of corporate governance, strategic risk, and commercial opportunity, bank decision-makers can effectively lead this profound, future-defining transformation, ensuring the bank not only survives but thrives in the quantum era.

Chapter 7 China’ s Action Blueprint

Based on a profound insight into global trends, the solid support of autonomous core technologies, and successful practice in typical scenarios, this White Paper proposes a clear, pragmatic, and phased strategic roadmap for China's financial sector's post-quantum security migration from the perspective of national strategy. This is not just a technological upgrade plan, but a grand project to build a quantum-safe financial "New Infrastructure" for the future.

7.1 China’ s Financial Sector Post-Quantum Security Migration Three-Phase Roadmap: Inventory, Planning, and Execution

This roadmap draws upon the general framework proposed by the Bank for International Settlements (BIS) [29] and the practical experience of major international banks. It deeply integrates China's national conditions and institutional advantages, forming an implementation blueprint guided by competent authorities and collaboratively advanced by the entire industry.

Phase I: Comprehensive Inventory and Risk Assessment (2026-2027)

Goal: To take stock of current assets, identify risks, and clarify direction.

Key Tasks:

Management Initiation and Pilot: Relevant management departments formally issue the Guidance on Preparation for Post-Quantum Cryptography Migration of Banking Information Systems to initiate industry-wide preparation. Concurrently, based on the established post-quantum security management specifications and compliance guidelines for the banking sector, pilot and solicitation work is first carried out in select institutions to verify the scientific validity and operability of

the management metrics.

Unified Inventory: Requires all banks and critical financial infrastructure operators to complete a comprehensive inventory of cryptographic assets within a specified timeframe, according to unified standards and templates, and report the results.

Risk Assessment: Institutions must adopt the "Data-Driven" framework proposed by the national project to conduct quantum risk assessments on their core business data and systems, identify high-risk assets, and tentatively determine migration priorities.

Phase II: Pilot First and Standard Setting (2028-2029)

Goal: To verify solutions, accumulate experience, and solidify standards.

Key Tasks:

National-Level Pilots: Select several large state-owned commercial banks and national critical financial infrastructures (such as CIPS, HVPS) as industry pilot units to first launch the PQC migration project for their core systems.

Experience Accumulation: Pilot units must use the support of the "Post-Quantum Cryptography Migration Experimental Platform" to conduct in-depth verification of various technical solutions, hybrid modes, and migration paths, forming reproducible and scalable best practices and engineering manuals.

Standard Release: Based on pilot experience, the National Financial Standardization Technical Committee formally issues the post-quantum security management specifications for the banking sector and related technical specifications and testing standards, providing clear compliance basis for the entire industry.

Phase III: Full Rollout and Normalized Operation (2030-2035)

Goal: To complete industry-wide migration and establish a long-term mechanism.

Key Tasks:

Industry-Wide Rollout: Guided by management directives and technical standards, promote the full-scale deployment of PQC migration across all banks and financial institutions nationwide, striving to complete the quantum security retrofit of the vast majority of critical information systems before 2035.

New System Requirements: Mandate PQC capability as a compulsory standard requirement for all newly built financial information systems, eliminating new security vulnerabilities at the source.

Normalized Operation: Establish a routine mechanism for quantum security risk monitoring, assessment, and emergency response, incorporating quantum security into the daily operation and compliance audit scope of financial institutions' cybersecurity.

Table 7-1: Phased Implementation Roadmap for Post-Quantum Security Migration in China's Banking Sector

Phase	Timeline	Core Tasks	Key Milestones
Phase I: Inventory and Assessment	2026-2027	Management initiation, unified inventory, risk assessment	Guidance issued, industry-wide cryptographic asset inventory completed, pilot of management specifications initiated
Phase II: Pilot and Standards	2028-2029	National-level pilots, experience accumulation, standard release	First batch of core system pilots completed, management specifications formally released
Phase III: Rollout and Operation	2030-2035	Industry-wide rollout, new system requirements, normalized operation	Migration rate of critical information infrastructure reaches over 90%

Figure 7-1: Three-Stage Roadmap for Post-Quantum Security Migration in China's Financial Sector (2026-2035)

7.2 Core Principles: Cryptographic Agility, Hybrid Deployment, and Full Ecosystem Collaboration

To ensure the successful implementation of the roadmap, the entire industry must collectively adhere to the following three core principles:

Cryptographic Agility: Cryptographic agility must be established as the core security principle in the design of future financial systems. System architecture should not be hard-coded to any specific cryptographic algorithm but should possess the ability to flexibly replace, upgrade, or combine different cryptographic algorithms through configuration changes. This is the fundamental guarantee for addressing the potential future cracking of PQC algorithms or the emergence of superior new algorithms.

Hybrid Deployment: During the transition phase and for a considerable period in the future, the "Classical Commercial Cryptography + Post-Quantum Cryptography" hybrid deployment model should be adopted as the main technical path. In this mode, both communicating parties use two algorithms simultaneously for key exchange or signature, and the final security strength depends on the stronger of the two. This not only utilizes PQC to resist future quantum attacks but also relies on long-tested commercial cryptographic algorithms (Chinese National Standard Algorithms (SM series)) to provide foundational security assurance, making it the most stable and reliable transition strategy [17].

Engineering Note: Architectural Restructuring – Easier Said Than Done: However, implementing the hybrid mode is not a simple "algorithm overlay." As tested by BIS

"Project Leap," many existing financial application architectures (especially legacy systems) struggle to support processing dual signatures in the same message header due to underlying logic, and forced introduction may lead to a sharp increase in system complexity. Therefore, financial institutions must allocate sufficient resources for deep adaptive modification or even restructuring of the application layer architecture when planning hybrid deployment, mandating vendors to provide native solutions that support multi-algorithm parallelism, and must not underestimate the engineering difficulty of "code-level" modification.

Ecosystem Collaboration: Post-Quantum security migration is by no means a task that a single financial institution can complete independently; it requires the synergistic efforts of the entire financial ecosystem. Banks, FinTech companies, software and hardware vendors, cloud service providers, and security vendors must all synchronously enhance their quantum security capabilities. To this end, it is recommended that, under the guidance of competent authorities, an "Alliance for Promoting Post-Quantum Security Migration in the Financial Sector" be established to jointly formulate supply chain security requirements, coordinate migration pace, and share threat intelligence and best practices.

7.3 Policy Recommendations: Promoting Standard Implementation, Talent Development, and International Cooperation

To ensure the smooth progress of the roadmap, strong policy support at the national level is required:

Promote Standard Implementation: It is recommended that management departments accelerate the final review and issuance of the post-quantum security management specifications for the banking sector and effectively link them with existing laws and regulations and management frameworks such as the Cybersecurity Law, the multi-level protection scheme for cybersecurity, and the regulations on critical information infrastructure security protection, ensuring their authority and enforceability.

Strengthen Talent Development: There is a huge talent gap in the quantum security

field. It is recommended that the Ministry of Education, the Ministry of Industry and Information Technology, and other departments jointly promote the inclusion of PQC-related knowledge into the curriculum of universities for computer science, cybersecurity, FinTech, and related majors. At the same time, encourage cooperation between enterprises and research institutes to establish dedicated PQC technology training and certification systems to reserve sufficient talent for industry-wide large-scale migration.

Deepen International Cooperation: China should proactively and actively participate in the work of international standardization organizations such as ETSI, IETF, and ISO/IEC. It should be committed to promoting the mutual recognition and interoperability between Chinese and international standards, preventing technological fragmentation of the global financial infrastructure. By leveraging China's engineering experience in SVP solving and large-scale scenario verification, it can contribute Chinese wisdom to the improvement and implementation of global PQC standards.

By treating quantum security as the national financial "New Infrastructure," and through the top-level design of national strategy and the collaborative efforts of the entire industry, China is sure to build a highly resilient, highly reliable digital security defense line in this profound transformation of the global financial system and contribute a Chinese-characteristic practice paradigm and engineering experience to the post-quantum migration of global financial infrastructure.

Core Glossary

Abbreviation	Full Name	Explanation/White Paper Context
BIS	Bank for International Settlements	The "thought leader" and "coordinator" for the global central bank system. Elevated PQC migration to a core strategic issue concerning global financial stability by publishing Quantum-readiness for the financial system: a roadmap and organizing "Project Leap."
CBDC	Central Bank Digital Currency	Digital currency issued by a central bank. The White Paper notes that deep investment in CBDC infrastructure in places like Hong Kong objectively compels banks to resolve complex key management issues, providing "invisible preparation" for PQC migration.
CBOM	Cryptographic Bill of Materials	A tool for dynamically managing cryptographic dependencies in software. The White Paper suggests it be used as the basis for real-time risk management and mentions that Santander Bank participated in the development of related tools to help identify cryptographic dependencies in software.
CISO	Chief Information Security Officer	The head of enterprise information security. The White Paper emphasizes that quantum risk elevates the CISO's role from purely technical support to a critical part of the institution's core risk management function, requiring direct reporting to the board.
CRQC	Cryptographically Relevant Quantum Computer	A quantum computer with sufficient performance to crack current public-key cryptography systems (e.g., RSA). The uncertainty surrounding its exact time of arrival is a major dilemma for regulators in setting migration timelines.

DLT	Distributed Ledger Technology	Distributed Ledger Technology (blockchain). The White Paper mentions that under the HKMA's "Fintech 2025" strategy, DLT projects like mBridge train the banking sector's capability to master next-generation security infrastructure.
ERM	Enterprise Risk Management	The enterprise-wide risk management framework. The White Paper suggests that quantum risk be liberated from the technological silo and fully integrated into the ERM framework, to be quantified and managed on par with credit risk and market risk.
ETSI	European Telecommunications Standards Institute	A European technical standards organization. Focuses on the practical application of PQC, researching quantum-safe primitives, protocol performance, and architectural considerations in specific applications.
FIPS	Federal Information Processing Standards	A series of public standards issued by NIST. The White Paper specifically refers to FIPS 203, 204, and 205, which are the main technical benchmarks for global financial institutions to select PQC technologies and plan migration.
FS-ISAC	Financial Services Information Sharing and Analysis Center	The global financial industry's cybersecurity intelligence sharing organization. The White Paper recommends that financial institutions actively join such alliances to share costs, threat intelligence, and best practices through collaboration.
HKMA	Hong Kong Monetary Authority	Hong Kong's financial regulator. Adopts a "pragmatic ecosystem evolution" model, guiding the banking sector to focus on quantum computing under the "Fintech 2025" strategy and supporting market-driven pilots by institutions like HSBC.

HNDL	Harvest Now, Decrypt Later	Describes an urgent attack model where attackers steal and store encrypted data now, waiting for future quantum computers to mature for decryption. This asymmetric risk compels the financial industry to act immediately.
HVPS	High Value Payment System	The People's Bank of China's large-value real-time payment system. The White Paper mentions that the Chinese project team built a simulation environment to verify the end-to-end PQC migration for commercial banks clearing through HVPS.
ISO 20022	International Organization for Standardization 20022	An internationally adopted financial communication standard. BIS's "Project Leap" verified the feasibility and performance impact of using PQC algorithms for digital signatures on payment messages compliant with this standard.
MAS	Monetary Authority of Singapore	Singapore's financial regulator. Adopts a strategy of consultation, funding, and international cooperation, providing funds through the FSTI 3.0 scheme to incentivize financial institutions to explore PQC and QKD applications.
ML-DSA	Module-Lattice-Based Digital Signature Algorithm	The core algorithm of the NIST FIPS 204 standard (derived from CRYSTALS-Dilithium). Used to replace RSA for message signing in BIS's payment system tests, verifying its feasibility at the business layer.
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism	The core algorithm of the NIST FIPS 203 standard (derived from CRYSTALS-Kyber). It is the mainstream technical route currently used for general encryption and key exchange in global PQC migration.
NCSC	National Cyber Security Centre (UK)	The UK's cybersecurity lead authority. Published a clear migration roadmap, setting a regulatory deadline of "completion of all system migration by 2035."

NIST	National Institute of Standards and Technology	The core leader of global PQC standardization. Its published PQC algorithm standards (FIPS 203/204/205) are widely adopted as the technical blueprint by global regulators and financial systems.
PQC	Post-Quantum Cryptography	A new generation of public-key cryptography systems capable of resisting attacks by quantum computers. The core theme of the White Paper, aimed at replacing soon-to-be-obsolete traditional algorithms like RSA and ECC to ensure financial security.
QKD	Quantum Key Distribution	A key distribution technology based on physical principles. The White Paper mentions that institutions like HSBC and MAS are exploring its use as a complementary technology to PQC in pilot projects.
QSFF	Quantum Safe Financial Forum	A multi-stakeholder platform established by Europol. Aims to coordinate the PQC transition in the European financial sector, identify challenges, and promote cross-border industry collaboration.
SDK	Software Development Kit	Software Development Kit. The White Paper mentions that the China Solution developed a dedicated "mobile PQC SDK" to solve the challenge of running PQC algorithms in the resource-constrained mobile banking environment.
SVP	Shortest Vector Problem	The core mathematical difficulty problem of lattice cryptography. The White Paper mentions that the Chinese team globally pioneered the efficient solution of the SVP-200 problem in 2025, proving China's leading capability in lattice cryptography security assessment.
TLS	Transport Layer Security	The fundamental protocol ensuring secure internet communication. The White Paper notes the need for "post-quantum/hybrid mode" modification to support a smooth transition between institutions during the migration period.

VaR	Value at Risk	A core metric in financial risk management. The White Paper notes that quantum computing's computational advantage is expected to significantly accelerate VaR calculation, creating business opportunities from defensive migration.
WEF	World Economic Forum	An international organization. Builds global consensus on PQC migration at the strategic level by publishing a strategic framework and guiding principles, helping decision-makers transform technical challenges into management issues.

Reference Documentation

[1] Wikipedia, "Harvest now, decrypt later," Wikipedia, n.d. [Online]. Available: https://en.wikipedia.org/wiki/Harvest_now,_decrypt_later

[2]PQShield, "A Plain English Guide to Recent White House Guidance and Post-Quantum Cryptography," PQShield, 2023. [Online]. Available: https://pqshield.com/guide-to-recent-white-house-guidance-post-quantum-cryptography/

[3]National Cyber Security Centre (NCSC), "Timelines for migration to post-quantum cryptography," NCSC, 2024. [Online]. Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[4]The Quantum Insider, "Canada Sets Timeline to Shield Government Systems from Quantum Threats," The Quantum Insider, 2025. [Online]. Available: https://thequantuminsider.com/2025/06/28/canada-sets-timeline-to-shield-government-systems-from-quantum-threat/

[5]Financial Services Agency (FSA), "FSA Weekly Review No.603," FSA Japan, 2024. [Online]. Available: https://www.fsa.go.jp/en/newsletter/weekly2024/603.html

[6] XJTLU, "Sharing Research that Breaks World Records! Professor Jintai Ding, Dean of the School of Mathematics and Physics, Attracts Attention at Banks in Quantum Days 2025," XJTLU News, 2025 (in Chinese). [Online]. Available: https://www.xjtlu.edu.cn/zh/news/2025/10/dingjintaijiaoshouzaibanksinquantumdays2025yinfaguanzhu

[7] Xi'an Jiaotong-Liverpool University (XJTLU), "XJTLU PQC-X Lab Sets New Global Record in Lattice Cryptanalysis, Advancing Post-Quantum Cryptography Research," XJTLU News, 2025 (in Chinese). [Online]. Available: https://www.xjtlu.edu.cn/zh/news/2025/11/pqcxshiyanshishuaxinquanqiugemimafenxijilu

[8]The Quantum Insider, "Quantum Could Reshape Industry, Says BofA—But No Coverage For Now," The Quantum Insider, 2025. [Online]. Available: https://thequantuminsider.com/2025/07/21/quantum-could-reshape-industry-says-bofa-but-no-coverage-for-now/

[9]SpinQ, "How Quantum Computing Benefits Financial Services [2025]," SpinQ, 2025. [Online]. Available: https://www.spinquanta.com/news-detail/how-quantum-computing-benefits-financial-services20250219023634

[10]World Economic Forum (WEF), "Quantum Security for the Financial Sector: Informing Global Regulatory Approaches," WEF, 2024. [Online]. Available: https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.p

df

[11]Bank for International Settlements (BIS), "Quantum computing and the financial system: opportunities and risks," BIS, 2024. [Online]. Available: https://www.bis.org/publ/bppdf/bispap149.pdf

[12]D-Wave Quantum, "Quantum Realized," D-Wave, n.d. [Online]. Available: https://www.dwavequantum.com/

[13]J.P. Morgan, "Quantum Computing Will Redefine Encryption," J.P. Morgan, n.d. [Online]. Available: https://www.jpmorgan.com/payments/payments-unbound/volume-2/quantum-computers-will-redefine-encryption

[14]European Telecommunications Standards Institute (ETSI), "Quantum - Safe Cryptography," ETSI, n.d. [Online]. Available: https://www.etsi.org/technologies/quantum-safe-cryptography

[15]Europol, "Quantum Safe Financial Forum," Europol, n.d. [Online]. Available: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/qsff

[16]QuEra Computing, "What is Shor's Algorithm," QuEra, n.d. [Online]. Available: https://www.quera.com/glossary/shors-algorithm

[17]Bank for International Settlements (BIS), "Project Leap - Quantum-proofing the financial system," BIS, 2023. [Online]. Available: https://www.bis.org/publ/othp67.pdf

[18]Investment Executive, "Urgent action needed to prepare for quantum threat," Investment Executive, 2024. [Online]. Available: https://www.investmentexecutive.com/news/from-the-regulators/urgent-action-needed-to-prepare-for-quantum-threat/

[19]F5, "The post-quantum imperative for financial institutions," F5, n.d. [Online]. Available: https://www.f5.com/pdf/infographic/the-post-quantum-imperative-for-financial-institutions-infographic.pdf

[20]Bank for International Settlements (BIS), "Project Leap: quantum-proofing the financial system," BIS, n.d. [Online]. Available: https://www.bis.org/about/bisih/topics/cyber_security/leap.htm

[21]Gracker.AI, "China's Quantum Strategy: Launching Quantum-Resistant Encryption Standards and Protecting Data from Emerging Threats," Gracker.AI, n.d. [Online]. Available: https://gracker.ai/blog/china-quantum-encryption-strategy

[22]Wikipedia, "Post-quantum cryptography," Wikipedia, n.d. [Online]. Available: https://en.wikipedia.org/wiki/Post-quantum_cryptography

[23]The White House, "REPORT ON POST-QUANTUM CRYPTOGRAPHY," The White House, 2024. [Online]. Available: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf

[24]KPMG International, "Quantum is coming," KPMG, 2024. [Online]. Available:

https://kpmg.com/dp/en/home/insights/2024/04/quantum-and-cybersecurity.html

[25]Wikipedia, "NIST Post-Quantum Cryptography Standardization," Wikipedia, n.d. [Online]. Available: https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization

[26]National Institute of Standards and Technology (NIST), "Report on Post-Quantum Cryptography," NIST, 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf

[27]So & Sato, "Quantum Technology and Japanese Law," So & Sato Law Offices, n.d. [Online]. Available: https://innovationlaw.jp/en/quantum-law-japan-en/

[28]Europol, "Quantum Safe Financial Forum First Meeting Report," Europol, 2025. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/Quantum-safe-financial-forum-2025.pdf

[29]PQShield, "The BIS publishes quantum-readiness roadmap for the financial system," PQShield, 2024. [Online]. Available: https://pqshield.com/the-bis-publishes-quantum-readiness-roadmap-for-the-financial-system/

[30]Cybersecurity and Infrastructure Security Agency (CISA), "Post-Quantum Cryptography Initiative," CISA, n.d. [Online]. Available: https://www.cisa.gov/quantum

[31]The Quantum Insider, "Bank of America Strategist Calls Quantum 'The Most Important Technological Race of Our Generation'," The Quantum Insider, 2025. [Online]. Available: https://thequantuminsider.com/2025/08/05/bank-of-america-strategist-calls-quantum-the-most-important-technological-race-of-our-generation/

[32]Goldman Sachs, "Engineering Quantum Algorithms," Goldman Sachs, n.d. [Online]. Available: https://www.goldmansachs.com/careers/blog/possibilities-quantum-computing

[33]Post-Quantum, "Government of Canada Launches Post-Quantum Cryptography (PQC) Migration Roadmap," Post-Quantum, n.d. [Online]. Available: https://postquantum.com/industry-news/canada-pqc-roadmap/

[34]Toshiba, "Quantum-Safe Security Solutions," Toshiba, n.d. [Online]. Available: https://www.toshiba.eu/solutions/quantum/

[35]HSBC, "HSBC pilots Quantum-Safe Technology for Tokenised Gold," HSBC, 2024. [Online]. Available: https://www.hsbc.com/-/files/hsbc/media/media-release/2024/240917-hsbc-pilots-quantum-safe-technology-for-tokenised-gold.pdf?download=1

[36]The Quantum Insider, "Swiss Finance Sector Urged to Act Fast to Avoid Quantum Threat," The Quantum Insider, 2025. [Online]. Available: https://thequantuminsider.com/2025/03/27/swiss-finance-sector-urged-to-act-fast-to-avoid-quantum-threat/

[37]The Quantum Insider, "Monetary Authority of Singapore Commits up to S$100 Million to

Support Quantum and AI in the Financial Sector," The Quantum Insider, 2024. [Online]. Available: https://thequantuminsider.com/2024/07/18/monetary-authority-of-singapore-commits-up-to-s100-million-to-support-quantum-and-ai-in-the-financial-sector/

[38]Chia Der Jiun, "Remarks on the MAS Annual Report 2024/2025," Bank for International Settlements (BIS), 2025. [Online]. Available: https://www.bis.org/review/r250717h.htm

[39]Bank of Israel, "Proper Conduct of Banking Business Directive 361: Cyber Defense Management," Bank of Israel, 2025. [Online]. Available: https://boi.org.il/media/sm4f1ssu/202501en.pdf

[40]Hong Kong Monetary Authority (HKMA), "Circular on Results of Tech Maturity Stock-take Enclosure: Fintech Adoption," HKMA, 2025. [Online]. Available: https://brdr.hkma.gov.hk/eng/doc-ldg/docId/getPdf/20250716-3-EN/20250716-3-EN.pdf

[41] The Central People's Government of the People's Republic of China, "The Outline of the 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Long-Range Objectives Through the Year 2035," March 2021 (in Chinese). [Online]. Available: https://www.gov.cn/xinwen/2021-03/13/content_5592681.htm

[42]Bank for International Settlements (BIS), "Project Leap: quantum-proofing the financial system," BIS, n.d. [Online]. Available: https://www.bis.org/about/bisih/topics/cyber_security/leap.htm

[43]Bank for International Settlements (BIS), "Project Leap phase 2: quantum-proofing payment systems," BIS, 2025. [Online]. Available: https://www.bis.org/publ/othp107.htm