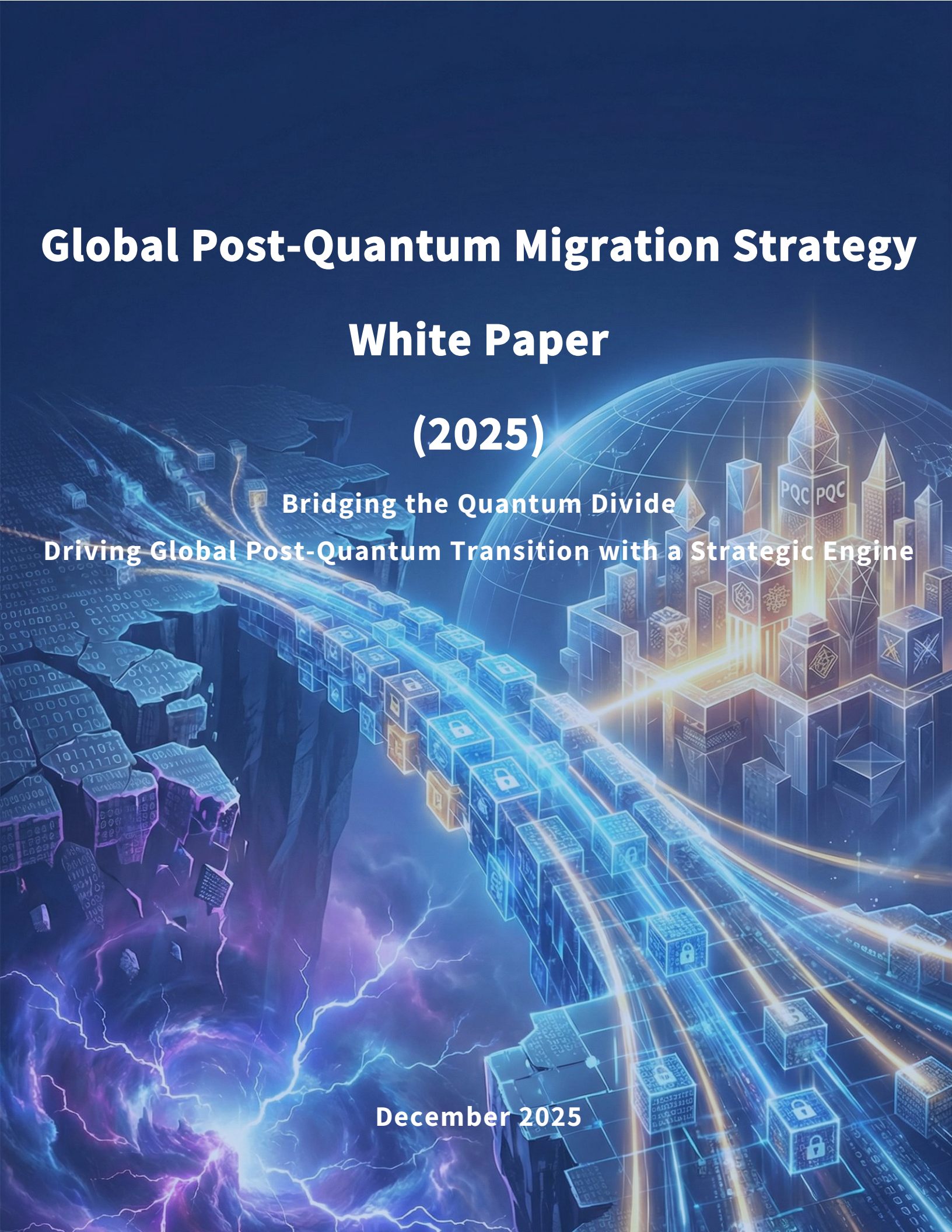
Global Post-Quantum Migration Strategy White Paper (2025)

Bridging the Quantum Divide

Driving Global Post-Quantum Transition with a Strategic Engine



December 2025

Document History

Version	Date	Description
1.0.0	December 2025	First published in 2025.
1.0.1	December 2025	Some wording has been revised.

Participating Organizations

Xi'an Jiaotong-Liverpool University Post-Quantum Migration Interdisciplinary Lab (PQC-X)

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

Yunchao Financial Services (Beijing) Co., Ltd.

C*Core Technology Co., Ltd.

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

Shanghai Xuntian Qianhe Space Technology Co., Ltd.

Steering Committee

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)

Professor Jiang Zheng

Chairman, C*Core Technology Co., Ltd.

Authors

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)

Neng Zeng

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

Legal Statement and Disclaimer

Copyright Statement

Disclaimer

Nature of Information: The content contained in this white paper is for reference only. It aims to provide a strategic framework and technical guidance for Post-Quantum Cryptography (PQC) migration and does not constitute any form of final advice for legal, financial investment, or technical implementation.

Accuracy: Although the drafting team has made every effort to ensure the accuracy of the data in the text (such as qubit demand forecasts, market size forecasts), given the rapid iterative nature of quantum technology development, we assume no legal liability for the absolute accuracy, completeness, or timeliness of the information.

Risk Warning: The technical solutions mentioned in the report (such as hybrid models, crypto-asset discovery) should be evaluated in combination with the actual situation of each organization. The participating units, steering committee, drafting units, and drafting personnel assume no responsibility for any direct or indirect losses arising from the use of the information in this report.

Contents

A Strategic Call to Decision-Makers: Crossing the Quantum Divide

Crossing the Quantum Divide — Transforming an Existential Threat into a Strategic Opportunity

Core Risk: A "Data Heist" That Has Already Begun

The security cornerstone of our digital world—the public key encryption systems represented by RSA and ECC—is facing a fundamental disruption. Quantum computers capable of breaking these systems are no longer distant theories, but a technological tipping point that is accelerating toward us.

However, the greatest threat is not some future attack "event," but a current risk that already exists and persists: the "Harvest Now, Decrypt Later" (HNDL) attack. Adversaries worldwide are intercepting and storing our currently encrypted data on a massive scale, patiently waiting for future quantum computers to emerge to decrypt it. This means that for any high-value data requiring long-term secrecy—core intellectual property, long-term financial contracts, state secrets, or personal privacy data—security vulnerabilities effectively already exist.

Delaying action is not a zero-cost decision; it is the continuous accumulation of a dangerous "Quantum Security Debt." Once quantum computers are ready, the repayment of this debt will be catastrophic, potentially leading to permanent loss of intellectual property, massive regulatory fines, and the complete collapse of brand reputation.

Strategic Countermeasure: Launching the "Quantum Security Migration Strategic Engine"

Facing this complex challenge, a simple algorithm replacement or a linear project-based migration is far from sufficient. This white paper proposes an authoritative and actionable all-new strategic framework—the Quantum Security Migration Strategic Engine.

This is a dynamic, self-reinforcing lifecycle model aimed at transforming Post-Quantum Cryptography (PQC) migration from a passive cost center into a strategic capability that builds long-term organizational resilience. Its core principle is "Crypto-Agility," which involves building a resilient technical architecture capable of flexibly adapting to future standard evolutions and unknown threats. With major global economies establishing mandatory migration timelines—such as the US (banning first-generation public key standards by 2035) and the EU (completing migration for critical infrastructure by 2030)[24]—PQC migration is no longer an option, but an urgent task with a clear deadline.

Immediate Action: "No-Regret Moves" and Your Top Priority

The window for hesitation and "wait-and-see" has closed. We strongly recommend that you immediately authorize and invest resources to launch initial steps widely recognized as "No-Regret Moves." [25] Regardless of when the quantum threat arrives, these actions can vastly improve the organization's current security visibility and management capabilities, serving as an opportunity to enhance overall "Cryptographic Maturity." Your primary task is to immediately initiate a comprehensive, enterprise-wide cryptographic asset inventory and quantum risk assessment. You cannot protect assets you are unaware of. This effort will provide the data-driven ignition energy for your migration

engine, transforming abstract risks into a concrete, quantifiable roadmap for risk mitigation actions.

From Risk to Opportunity: Investing in Future Competitiveness

PQC (Post-Quantum Cryptography) migration is not merely a defensive expense, but a strategic investment in an enterprise's future digital trust and market competitiveness. Enterprises that lead the migration can leverage it as a powerful competitive advantage, securing a head start in winning premium contracts, fostering customer loyalty, and gaining supply chain access.

Even more decisive is the fact that the mathematical foundation supporting one of the mainstream PQC standards—Lattice Cryptography—is entirely consistent with the "Holy Grail" of next-generation privacy-preserving computing: Fully Homomorphic Encryption (FHE). This profound mathematical connection completely transforms a compliance-driven defensive cost into a proactive strategic investment that empowers future business innovation. Every penny you invest in PQC migration today is a pre-investment in the infrastructure required to deploy next-generation secure AI applications, thereby building decisive future market competitiveness.

The time for strategic action is now. You must immediately launch your organization's migration engine to ensure survival and competitiveness in the future quantum era.

Abstract

The security cornerstone of the digital world is facing a fundamental disruption. The rise of quantum computing is not a distant theory, but a technological tipping point accelerating toward reality. It will render the encryption standards currently protecting global communications, commerce, and national security (such as RSA and ECC) completely obsolete. The fundamental threat posed by quantum computing to traditional public-key cryptography systems is driving the cryptography market with unprecedented force, propelling a profound evolution from 'one-dimensional' to 'three-dimensional'—characterized by technological diversification, scenario ubiquity, and ecosystem dynamism.

However, predictions regarding the timing of threats based on linear thinking are no longer applicable. This white paper aims to clarify that the quantum threat is not merely a future event, but an immediate risk existing in the form of "Harvest Now, Decrypt Later" (HNDL), requiring us to adopt continuous response strategies immediately. Recent industry reports indicate that executive awareness of this threat has become mainstream; for example, Capgemini's 2025 research shows that 65%[1] of organizations are concerned about the rise of HNDL attacks. A Thales report from the same period confirms this trend, pointing out that 58%[2] of organizations view "future decryption of today's data" as a primary quantum security threat.

Faced with this challenge, a simple algorithm replacement or a linear, project-based migration method is far from sufficient. The transition to Post-Quantum Cryptography (PQC) is essentially a comprehensive upgrade of an organization's overall information security posture, with the ultimate goal of achieving a sustainable state of "Cryptographic Maturity." Therefore, this white paper proposes an authoritative and

actionable new strategic framework—the Quantum Safe Migration Strategy Engine. This is a self-reinforcing lifecycle model aimed at providing a clear path for organizations to achieve and maintain long-term quantum resilience.

The nature of the threat is evolving. On one hand, the combined effects of emerging quantum technologies (such as surface codes and Cat Qubits[9]) are drastically compressing the threat timeline. On the other hand, we face a "dual threat" where quantum and classical risks coexist: future quantum computers will break the mathematical foundations of algorithms, while current AI-driven cryptanalysis tools are automating attacks on the engineering implementation of algorithms. Meanwhile, the rise of Quantum Computing as a Service (QaaS) is democratizing quantum attack capabilities from an economic standpoint, making them no longer the exclusive tools of a few nation-state actors.

The Quantum Safe Migration Strategy Engine framework is designed specifically to address this dynamic and persistent threat. It consists of five interrelated and mutually reinforcing stages, the feasibility of which has been validated by leading global practices. For instance, the migration projects organized by the National Cybersecurity Center of Excellence (NCCoE) under the US National Institute of Standards and Technology (NIST), utilize operational models that are highly aligned with this framework.

Core Principle (Engine Base): Cryptographic Agility[23] Design

Initial Power (Ignition Start): Strategic Foresight and Risk Intelligence

Building Momentum (Powertrain): Post-Quantum Cryptography Technology Stack

Acceleration Engine (Turbocharging): Simulation and Verification Modules

Sustaining Momentum (Intelligent Regulation): Governance and Evolution Cycle

Successful migration to post-quantum cryptography is inseparable from a mature and complete ecosystem of solutions.The alliance behind this white paper—comprising the Xi'an Jiaotong-Liverpool University Post-Quantum Migration Interdisciplinary Lab (PQC-X), Suzhou Langkong Post-Quantum Technology Co., Ltd. (LK Quantum), and partners including the Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University) Ministry of Education (CPS-DSC), Yunchao Financial Services (Beijing) Co., Ltd., C*Core Technology Co., Ltd., and Shanghai Xuntian Qianhe Space Technology Co., Ltd.—precisely represents such an ecosystem. This alliance constitutes a complete value chain ranging from foundational research to full-stack products and services, capable of powering every stroke and module of the migration engine.

We are standing on the edge of crossing the quantum divide. For global decision-makers, business leaders, and technical experts, the window for hesitation and waiting has closed. It is now imperative to start their respective migration engines to ensure the survival and competitiveness of their organizations in the future quantum era. The time for strategic action is now.

Chapter 1

Deconstructing Digital Trust - From Enigma to Crossing the Quantum Divide

Chapter 1: Deconstructing Digital Trust - From Enigma to Crossing the Quantum Divide

This section aims to establish a comprehensive historical and technical background regarding the urgency of the Post-Quantum Cryptography (PQC) migration. The report will demonstrate that "crossing the quantum divide" is not an isolated event, but the inevitable climax of a long history of cryptographic evolution and obsolescence, compelling us to take logical and urgent action.

1.1 Enigma's Herald: The Eternal Lesson of Cryptographic Failure

To understand the current quantum threat, we must first look back at history. The story of the Enigma machine used by the German military in World War II is not just a fascinating war legend, but a profound textbook on the vulnerability of cryptographic systems, providing a foundational case study for today's post-quantum cryptography strategy.

1.1.1 The Peak of the Symmetric Cryptography Era: The Golden Age of Mechanical Encryption

Before the birth of modern public-key cryptography, the world was in the era of symmetric cryptography for a long time. In this system, the sender and receiver of information must share the same key to encrypt and decrypt.

The Enigma machine, invented by German engineer Arthur Scherbius, was the pinnacle of mechanical encryption technology in this era. Through a series of configurable rotors, plugboards, and reflectors, it implemented an extremely complex polyalphabetic substitution cipher.

Its theoretical key space combinations reached astronomical figures, leading it to be widely considered unbreakable at the time.

1.1.2 The Polish Pioneers and the Industrialized Decryption at Bletchley Park: A Turning Point in Cryptography

However, the "myth of invincibility" of Enigma was first broken by a group of heroes often overlooked by history—the mathematicians of the Polish Cipher Bureau. As early as 1932, a team led by Marian Rejewski, working closely with Jerzy Różycki and Henryk Zygalski, successfully broke early versions of Enigma by applying rigorous mathematical group theory for the first time. Their success was the result of combining mathematical talent with key intelligence obtained by French intelligence from German spy Hans-Thilo Schmidt. In July 1939, on the eve of the invasion of Poland, they selflessly shared their research findings, decryption methods, and even replica Enigma machines with their British and French allies—a moment crucial to the course of the entire Second World War.

The legend of Bletchley Park began with the solid foundation laid by the Poles, while Alan Turing and Gordon Welchman completed the critical leap from theory to mechanization, designing the British version of the "Bombe" machine. However, to talk about the "industrialized production" and peak computing power that truly pushed decryption work to its limits, the entry of the United States across the ocean must be mentioned.

Inspired by the British design, the United States deployed its formidable industrial manufacturing capabilities (such as the NCR Corporation) to build the American version of the Bombe, which was faster, more stable, and capable of handling the four-rotor system. It was this transatlantic cooperation of "British design, American mass production" that transformed what was originally manual and semi-automated decryption into a true large-scale assembly line operation, drastically reducing the time required to break daily keys, and

ultimately enabling the large-scale decryption of the massive volume of German military cipher traffic.

1.1.3 An Analysis of Failure: The Fatal Flaws of Cryptographic Systems Do Not Originate from Mathematics

The collapse of Enigma did not stem from the mathematical theory of its core encryption algorithm being defeated, but rather from a series of cascading errors in design, operation, and cognition. This provides us with the most profound lessons on real-world cryptographic security:

Design Flaw: The design of the reflector ensured that a letter could never be encrypted into itself. This seemingly minor characteristic provided cryptanalysts with a valuable statistical "backdoor," greatly narrowing the scope of what needed to be guessed.

Operational Security (OPSEC) Catastrophe: This was Enigma's true "Achilles' heel". The negligence of German operators in daily use and the fixed habits they formed for convenience created a large number of fatal patterns.

Double Encryption of Message Keys: Before 1940, the German regulations mandated that the three-letter message key be encrypted twice using the daily key before transmission, as a safeguard against transmission errors. This "safety measure" ironically became a "fatal flaw," enabling Rejewski to analyze the two segments of ciphertext—which should have been identical but were encrypted differently—to separate the effects of the rotors and the plugboard, providing a decisive entry point for the initial decryption.

Rigid Message Formats: A large number of dispatches used fixed beginnings and endings, such as "Wetter" (weather report), fixed salutations, or "no new messages." This predictable content provided the Allies with what were known as "Cribs" (known plaintext segments), which could be compared with intercepted ciphertext to quickly verify the correctness of the key settings.

Operator Laziness: To save effort, some operators would use "lazy keys" such as "AAA" or letters along the keyboard's diagonal. Furthermore, after setting a new daily key, some would directly use the default rotor position as the starting position for the first message without randomizing the turnover. John Herivel, a cryptanalyst at Bletchley Park, keenly noticed this pattern, which led to the famous "Herivel Tip," greatly reducing the effort required to find the initial rotor position.

Organizational Arrogance and Prejudice: Despite indications that the code might have been broken, the German High Command maintained absolute confidence in Enigma's security, attributing Allied successes to coincidence, espionage, or betrayal by allies, rather than a problem with the cryptographic system itself. This institutional arrogance prevented them from promptly fixing the fatal operational security vulnerabilities.

This history reveals a core principle: real-world security is a chain, and the weakest link is often not profound mathematical theory, but rather mediocre engineering implementation and human error. This forms a striking historical parallel with the "dual threat" environment described in this white paper: current AI tools are automating attacks on the engineering implementation of cryptographic algorithms, while future quantum computers will attack their mathematical foundations. The Enigma story is the historical proof of this concept.

Furthermore, the German military's belief in the inviolability of the Enigma technology directly led to a relaxation of its operational security procedures, which serves as a warning for organizations today. If an organization declares itself "quantum-safe" simply by migrating to an NIST-approved PQC algorithm, it may fall into the same complacency, ignoring continuous classical attack threats and potential future weaknesses that may be discovered in the PQC algorithms themselves. Security is a process of continuous vigilance, not a one-time technical fix. This precisely validates the importance of continuous governance and evolution emphasized by the "Strategic Engine" model in the white paper.

Of greater strategic significance is the fact that the "Harvest Now, Decrypt Later" (HNDL) modern cyberattack model has a precedent in the history of Enigma's decryption. The Allies intercepted and stored vast amounts of Enigma ciphertext, never stopping even during periods when decryption was temporarily impossible. They were confident that a future breakthrough—whether obtaining a new "Crib," capturing codebooks, or technical upgrades to the Bombe machine—would eventually unlock this stored information. This mirrors the strategic logic of today's adversaries, who steal encrypted data and patiently wait for the advent of quantum computers for decryption. The Enigma story makes the abstract modern threat of HNDL concrete and historically traceable.

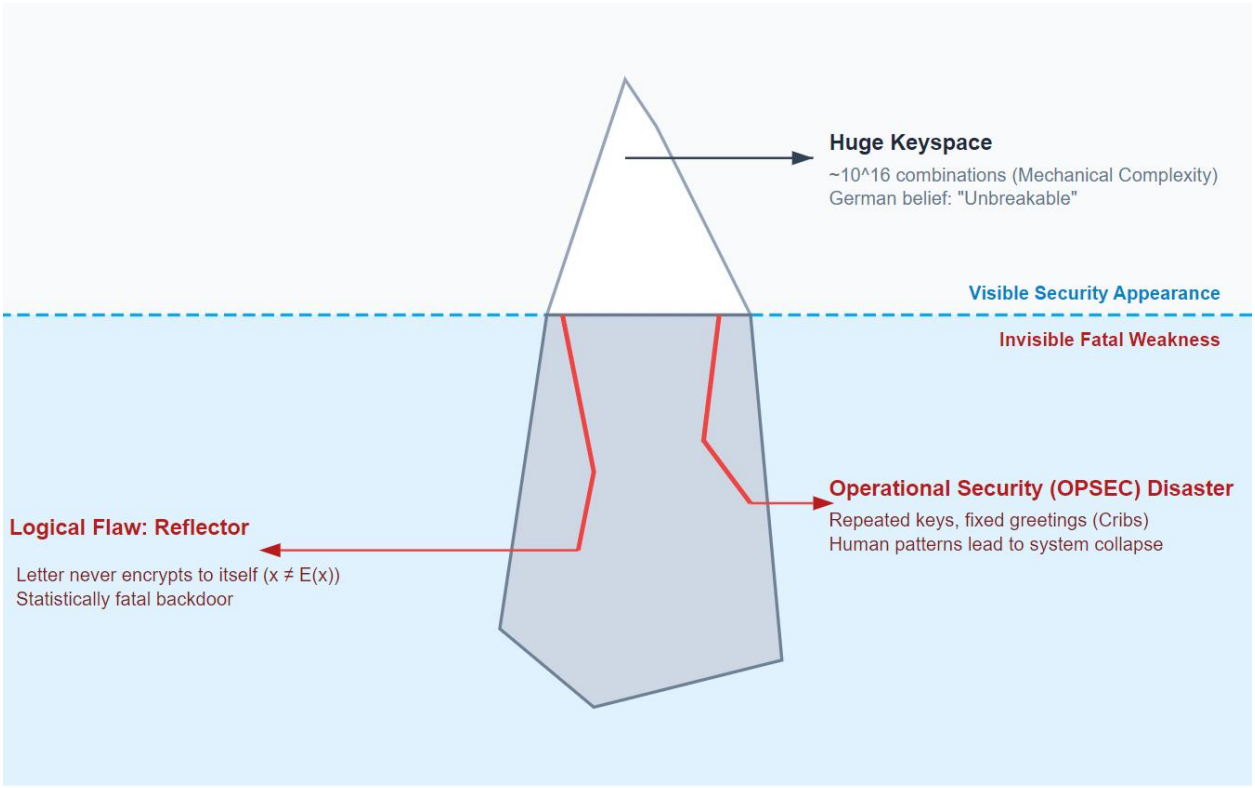
The Enigma story is not an isolated incident. A more recent, and even more chilling, example is the secret weaponization of cryptographic trust at the state level. During the 1982 Falklands War (or Malvinas War) [3-5], the Argentine military relied on advanced encryption devices purchased from the reputable, neutral Swiss company Crypto AG to protect its military communications. They believed the equipment was secure. However, the reality was that the company had been secretly acquired by the U.S. Central Intelligence Agency (CIA) and the West German Federal Intelligence Service (BND) since 1970. These intelligence agencies planted "backdoors" in the encryption machines sold globally (including to Argentina), allowing them to easily decrypt their customers' confidential communications. During the war, the U.S. used this secret advantage to read Argentina's encrypted military dispatches and shared critical intelligence with the United Kingdom, significantly influencing the course of the war. More ironically, after the war, when Argentina suspected its cryptosystems were compromised, a representative from Crypto AG successfully convinced them that their primary equipment remained "unbreakable," leading Argentina to continue using the compromised systems. This real-world case provides a more direct warning than Enigma:

If a nation or organization possesses the "master key" to break mainstream cryptography, they absolutely will not make it public; instead, they will secretly use it as the highest classified and most powerful strategic weapon. This makes the threat of "crossing the quantum divide" no longer a theoretical conjecture. The moment a nation becomes the first to build a quantum computer capable of breaking current public-key cryptography, the world will not hear any press release. Instead, the encrypted data of governments, businesses, and individuals globally could be silently decrypted without detection. This is the fundamental reason why post-quantum migration is so urgent—we must complete our defensive upgrade before the adversary's secret weapon reaches operational readiness.

Table 1.1: Vulnerabilities of the Enigma Era vs. Modern PQC Challenges

Vulnerabilities of the Enigma Era	Similar Challenges in Modern PQC	Strategic Mitigation Measures (Engine Modules)
Design Flaws (No Self-Encryption)	Potential, undiscovered algorithmic weaknesses in PQC candidate algorithms	Algorithmic Diversity (Technology Stack)
Operational Security Failures (Key	Insecure API usage, hard-coded keys,	AI-driven code analysis, High-fidelity verification

Repetition, "Cribs")	implementation layer vulnerabilities	(Simulation & Verification Engine)
Organizational Complacency (Belief in impregnability)	The misguided mindset of "One-time Migration," ignoring continuous risks	Continuous Risk Intelligence & Governance (Strategic Foresight, Governance Cycle)
Intercept First, Decrypt Later	"Harvest Now, Decrypt Later" (HNDL) attacks	Migration prioritization based on data secrecy lifespan (Strategic Foresight)



Historical Strategic Insight: Just as Enigma's collapse stemmed from weaknesses "beyond mathematics," modern **PQC migration** faces the same **"dual threat"**:

- **Above Water:** Belief in the mathematical robustness of PQC algorithms (e.g., lattice-based cryptography).
- **Below Water:** Neglect of **engineering implementation vulnerabilities** (e.g., side-channel attacks) and **management inertia**, which are the weakest links in the defense system.

Figure 1.1: The Illusion of Complexity - Enigma's Systemic Collapse

1.2 The Public-Key Revolution: A Modern World Built on Mathematical Assumptions

The fundamental flaw exposed by Enigma's symmetric encryption system was the "key distribution problem". For secure communication, both parties must first exchange a shared key through a secure physical channel. This was acceptable for small-scale military communications, but completely unscalable for the burgeoning computer networks of the 1960s and 1970s, which connected countless unfamiliar nodes. This

method was costly, inefficient, and completely unscalable, becoming a major obstacle to the development of the digital world.

1.2.1 A Tale of Two Cities in Invention

It was against this background that the greatest revolution in the history of cryptography—Public-Key Cryptography (PKC)—emerged. Interestingly, this revolution unfolded independently and almost simultaneously in two places, one secret and one public.

The Secret Invention (GCHQ, UK): At the UK Government Communications Headquarters (GCHQ), James Ellis proposed the theoretical concept of "non-secret encryption" in 1970. Subsequently, his colleague Clifford Cocks designed an implementation closely resembling the RSA algorithm in 1973, and another mathematician, Malcolm J. Williamson, invented a Diffie-Hellman-like key exchange method in 1974. However, due to the classified nature of their work, these pioneering achievements were locked away in archives and only became known to the public decades later.

The Public Revolution (Stanford, USA): Across the ocean in the United States, Whitfield Diffie and Martin Hellman, inspired by the earlier ideas of Ralph Merkle, publicly published the landmark paper "New Directions in Cryptography" in 1976, formally proposing the concept of public-key key exchange. Shortly thereafter, Ronald Rivest, Adi Shamir, and Leonard Adleman of MIT proposed the famous RSA algorithm, which is based on the mathematical difficulty of factoring large integers and provides a complete and practical scheme for public-key encryption and digital signatures.

1.2.2 The Asymmetric Breakthrough

The core idea of public-key cryptography is "asymmetry." Each user possesses a mathematically related pair of keys: a Public Key that can be freely distributed and made public, and a Private Key that must be kept

strictly confidential. Information encrypted with the Public Key can only be decrypted by the corresponding Private Key. This design cleverly solved the key distribution problem: people can exchange Public Keys through any insecure channel (like the internet) without establishing a secure connection beforehand. The trust foundation of cryptographic systems underwent a fundamental shift: it no longer relies on the physical security of the key transmission channel but instead relies on a brand-new cornerstone—the computational infeasibility of deducing the Private Key from the Public Key.

1.2.3 Social Impact: The "One-Dimensional" Cornerstone of Digital Trust

The profound impact of this cryptographic revolution has shaped the entire digital world as we know it today.

Secure Communication: PKC (Public-Key Cryptography) is the core of secure internet communication. The "lock" icon in the address bar when we browse the web is due to the SSL/TLS protocol, which uses PKC to negotiate a session key, establishing an encrypted channel for applications such as e-commerce, online banking, and instant messaging.

Authentication and Digital Signatures: PKC bestows "identity" and "credibility" upon the digital world. The private key can "sign" data, and anyone can use the public key to verify the signature, thereby confirming the authenticity of the information's source (authentication) and that the content has not been tampered with (integrity). This function is crucial; it is used to ensure your Windows software update truly comes from Microsoft and not a hacker and is also used to sign legally binding electronic contracts and protect financial transactions.

Public Key Infrastructure (PKI): To solve the problem of "how to trust that a public key genuinely belongs to the entity it claims," a vast ecosystem—Public Key Infrastructure (PKI)—emerged. At its core are

Certification Authorities (CAs), which act like the digital world's "passport issuing agencies," demonstrating the binding relationship between the public key and its owner through the issuance of digital certificates.

The immense success of PKC also bred its own vulnerability. Over the past few decades, the traditional cryptography market has exhibited a marked "one-dimensional" characteristic: technology paths are highly concentrated on a few algorithms like RSA and ECC, and application scenarios are also highly concentrated in a few core areas like finance and communication. The entire security edifice of the digital world is almost completely built upon two core mathematical problems: large integer factorization (the basis of RSA) and the discrete logarithm problem (the basis of ECC and other algorithms). This "single point of failure" dependence means that the global digital trust system would instantly collapse once a computational method capable of efficiently solving these two problems emerges. It lacks algorithmic diversity, constituting a massive, systemic risk.

Therefore, the upcoming PQC migration is by no means a simple algorithm replacement. It is a fundamental upgrade to the global trust infrastructure. The birth of PKC spurred PKI, and the entire PKI ecosystem (including CAs, the X.509 certificate standard, verification protocols, etc.) was constructed around the characteristics of RSA/ECC algorithms (such as smaller key sizes). As the following text will indicate, PQC algorithms generally have larger key and signature sizes, which poses a huge engineering challenge to traditional PKI systems. Consequently, the migration effort requires a redesign of the core mechanisms we rely on to issue and verify global digital identities.

Table 1.2: Comparison of Cryptographic Eras

Cryptographic Era	Core Problem	Foundational Solution	Basis of Trust	Ultimate Vulnerability
Symmetric Era (Pre-1970s)	Key Distribution	Shared Key (e.g., Enigma)	Physical security of the channel used for key exchange	Physical capture of Keys/Codebooks; Operational errors
Public Key Era (1970s - 2030s?)	Establishing trust in open networks	Asymmetric Key Pairs (RSA/ECC)	Computational complexity of mathematical problems (Factorization/Discrete Logarithms)	New computational methods capable of solving these mathematical problems

1.3 The Quantum Storm: When New Physics Annihilates Old Mathematics

If the global digital security system today—Public-Key Cryptography

(PKC)—is built upon a sturdy fortress called "mathematical difficulty," then the emergence of quantum computing is like a dimensional strike that can directly dismantle the fortress's foundation. This storm does not originate from the traditional computing field but from a paradigm shift in physics.

1.3.1 The Dawn of Theory: Feynman's Vision

The theoretical dawn of quantum computers can be traced back to a profound insight proposed by the physics giant Richard Feynman in 1981. Feynman pointed out that nature fundamentally operates according to the laws of quantum mechanics and simulating it with our classical computers based on 0s and 1s is extremely inefficient, with the computational effort increasing exponentially—it is practically unrealistic[6].

He thus proposed a subversive idea:

Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical.

This definition is crucial as it fundamentally draws a boundary: a quantum computer is not a classical computer that "runs faster"; it is not even designed to solve all problems that classical computers address. It is an entirely new computing paradigm, operating according to the bizarre rules of quantum superposition and entanglement, specifically designed to solve certain hard problems unreachable by classical computers.

1.3.2 Shor's Algorithm: The Fatal "Killer App"

For more than a decade after Feynman proposed his idea, quantum computing remained largely a concept in the minds of physicists and theorists. It was not until 1994, when the Bell Labs mathematician Peter Shor[7] published his quantum algorithm, that this physical concept was officially transformed into a concrete and fatal threat to the entire digital

world.

Shor's algorithm[7] acts like a precision-guided key, perfectly opening the two core locks of the public-key cryptography fortress. It proved that a sufficiently powerful quantum computer could efficiently solve two specific mathematical problems at an unimaginable speed:

Integer Factorization

Discrete Logarithm Problem

This is not a coincidence; it is a "precision strike." These two problems are precisely the security cornerstones upon which the two most widely used public-key cryptography systems—RSA and Elliptic Curve Cryptography (ECC)—rely for their security. The advent of Shor's algorithm[7] signals that the foundation supporting the global internet trust system has begun to loosen.

1.3.3 From Theory to Reality: The $15 Million "3 x 5"

If Shor's[7] paper was a "theoretical declaration of war" against classical cryptography, then a physical experiment in 2001 truly fired the first shot, bringing this threat from paper into the real world.

At the time, at the IBM Almaden Research Center, a research team led by Isaac Chuang of MIT, in collaboration with Stanford University and the University of Calgary, successfully ran Shor's algorithm[7] in its entirety on a 7-qubit Nuclear Magnetic Resonance (NMR) quantum computer. Although this prototype machine reportedly cost $15 million to develop, it successfully completed a seemingly trivial task: factoring the number 15 correctly into 3 and 5.

1.3.3.1 The Profound Significance of this Achievement

Factoring 15 into 3 and 5 is effortless for any school student or ordinary calculator, but for the development of quantum computing, it was a watershed moment whose significance far exceeds the result itself:

First Physical Verification of the Principle (Proof of Principle): This

was the first time in human history that Shor's algorithm[7] was fully and scalably implemented in a physical system. It eloquently proved that Shor's algorithm[7] is not merely a mathematician's theoretical deduction but a program that can run and produce correct results in the real physical world. It eliminated fundamental doubts about the feasibility of quantum algorithms.

Strong Evidence of Quantum Computing Feasibility: The experiment successfully manipulated 7 qubits, achieving a series of complex quantum mechanical phenomena such as superposition, entanglement, and interference, culminating in a definite classical answer. This injected great confidence into the entire field of quantum computing, indicating that building a practical quantum computer, though extremely difficult, is not a fantasy.

Substantial Warning to the Cryptography Community: Although factoring 15 posed no cryptographic threat, it was like a thunderclap that forced the cryptography and information security industries to no longer ignore quantum computing. It transformed the "quantum threat" from a distant, theoretical possibility into a clear and visible future determined by technological development. It spurred governments, standards organizations, and research institutions worldwide to begin seriously investing resources in developing Post-Quantum Cryptography (PQC) capable of resisting quantum computer attacks.

Therefore, the experiment by Chuang's team, despite its "simple" result, marked the crucial step from purely theoretical exploration to experimental science in quantum computing, serving as the first concrete epitome of Shor's algorithm[7] moving from an abstract concept to a real threat. It inaugurated a new era of strategic rivalry between quantum and classical information security systems.

1.3.3.2 Algorithm Revealed: Not Brute Force, But a "Dimensionality Reduction Strike"

The power of Shor's algorithm[7] does not lie in trying every possible key faster than a classical computer (brute force), but in utilizing the principles of quantum mechanics to directly "see through" the overall structure of the mathematical maze. We can understand this process through an acoustic analogy:

Quantum Parallelism (The Omniscient View): A classical computer looking for a password is like holding a flashlight in a dark room, illuminating corners one by one. A quantum computer utilizes "Superposition," as if instantly lighting up the entire room, sensing all possibilities simultaneously.

Quantum Interference (Filtering Noise): This is the soul of the algorithm. Through an operation called the "Quantum Fourier Transform" (QFT), Shor's algorithm acts as "noise-canceling headphones" or a "lens." In this process, all wrong answers cancel each other out like chaotic sound waves (Destructive Interference) and return to silence; while the correct answers (the "period" required to crack the code) reinforce each other like resonance (Constructive Interference), becoming clearly visible.

Measurement (Capturing the Result): Finally, when observed through this "lens," the correct key is revealed with extremely high probability.

Conclusion: This "dimensionality reduction strike" on the computational paradigm means that a computer with sufficient qubits can break the RSA-2048 problem—which would take a traditional supercomputer hundreds of millions of years to solve—in just a few hours.

1.3.4 "Harvest Now, Decrypt Later" (HNDL): The Future Threat That Is Already Here

The physical realization of quantum computers still faces enormous challenges, but this does not mean we can rest easy. This future threat has already spawned an immediate real-world crisis—"Harvest Now,

Decrypt Later" (HNDL). Adversaries worldwide, especially powerful state-level actors, are actively intercepting and massively storing the immense volume of data currently encrypted with RSA/ECC. Like squirrels hoarding food for the winter, they are saving this unbreakable ciphertext in huge server clusters, waiting for the advent of future quantum computers.

They are making a huge gamble, betting that future quantum computers will be able to decrypt this treasure trove of information that is currently locked away. This vault of data may include:

National Security Secrets

Core Corporate Intellectual Property

Financial Transaction Records

Personal Biometric and Genetic Data

Control Protocols for Critical Infrastructure

This threat has shifted from theoretical discussion in the intelligence community to an official concern for governments and businesses worldwide. Authoritative agencies, including the US Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA), have jointly issued public warnings, urging organizations to immediately begin preparing for PQC migration to address the HNDL threat to national critical infrastructure and sensitive information.

The awareness of this threat has permeated corporate decision-making layers. A 2025 Thales Data Threat Report shows that 58% [2] of organizations already view "the future decryption of today's data, including 'Harvest Now, Decrypt Later'," as a major quantum computing security threat. A concurrent study from Capgemini Consulting also found that 65% [1] of organizations are concerned about the rise of HNDL attacks. This series of evidence indicates that HNDL has successfully evolved from a forward-looking technical problem into a mainstream, quantifiable business risk, and is profoundly influencing corporate strategic planning and budget allocation.

This means that for any data requiring long-term confidentiality (e.g., more than 5-10 years), the security vulnerability already exists.

The migration to Post-Quantum Cryptography (PQC) is thus no longer a forward-looking investment to protect future data, but a remedial measure that must be taken immediately to mitigate the risk of data leakage from the present and past. This risk model fundamentally changes the time frame in which decision-makers assess risk.

Traditionally, risk assessment is based on the "here and now" threat. The HNDL model, however, requires decision-makers to engage in a "race against time" calculation:

If Expected Time of Quantum Computer Availability < Expected Confidentiality Lifespan of Data, then your data is already at risk.

This transforms PQC migration from a distant IT technical issue into an urgent business continuity and risk management priority concerning the organization's long-term survival.

1.4 Global Response: Forging a Quantum-Resistant Future

Facing the disruptive threat posed by Shor's algorithm[7], global academia, industry, and government agencies have not stood idly by, but have swiftly mobilized to launch a collaborative defense aimed at reshaping the future of digital security.

1.4.1 The Rise of a New Field: Post-Quantum Cryptography

Following the advent of Shor's algorithm[7], a new field of cryptographic research—Post-Quantum Cryptography (PQC)—emerged. Its core goal is to develop new public-key cryptographic algorithms whose security is based on mathematical problems believed to be equally difficult for both classical and quantum computers, thus enabling resistance to attacks from both dimensions. After years of exploration, researchers have gradually focused on several key candidate technology

routes, including Lattice-based Cryptography, Multivariate Cryptography, Hash-based Cryptography, Code-based Cryptography [15], and Isogeny-based Cryptography.

1.4.2 NIST Standardization: An Open, Collaborative Global Race

In this race, the PQC standardization project launched by the U.S. National Institute of Standards and Technology (NIST) presents a picture dramatically different from the clear-cut adversaries and secret operations of the Enigma era. This open, transparent, and collaborative model is not an "original invention" of the PQC project, but a "golden rule" that NIST began to explore since the call for DES and matured through the AES and SHA-3 standardization processes. The PQC project inherits this tried-and-tested mechanism, calling upon the world's top cryptographers to subject candidate algorithms to years of the most rigorous scrutiny and attack in a public environment, thereby "finding and eliminating the weak before deployment," to maximize confidence in the eventual winning algorithms.

Phase One: Global Call and Initial Screening (2016 - 2017)

December 2016: The Call for Proposals NIST formally released the global Call for Proposals for PQC algorithms. The announcement detailed expectations for the future PQC standard, including clear security level requirements (corresponding to the difficulty of breaking AES-128, 192, 256), performance metrics (key size, signature size, computation speed), and implementation flexibility. This effectively set clear rules and a playing field for the competition.

November 2017: Initial Acceptance By the deadline, NIST had received 82 proposals from 25 countries worldwide. This was an unprecedented turnout, demonstrating the global cryptography community's high enthusiasm for the challenge. NIST conducted a preliminary review of these proposals, eliminating those that were incomplete or clearly did not meet the basic requirements, ultimately

accepting 69 algorithms as official candidates for the first round.

Phase Two: First Round Review (2018 - 2019) Focusing on Security Fundamentals

Goal: Eliminate algorithms with obvious security flaws.

Process: Over the next 14 months, the complete design documents for these 69 algorithms were made public. NIST held its first PQC standardization conference, and cryptographers, hackers, and academics globally dedicated themselves to analyzing these algorithms. During this period, a large number of academic papers were published, pointing out theoretical vulnerabilities, implementation flaws, and even direct attack methods against many algorithms. This was a "find-the-flaw" competition, where any minor defect could be fatal.

January 2019: First Round Advancement Announcement NIST released its evaluation report for the first round. Based on feedback from the global community, many algorithms were proven insecure. NIST drastically cut the candidate list to 26. Most of the eliminated algorithms were due to the discovery of "shortcuts" in the mathematical problems they relied upon, or their parameter settings being insufficiently secure.

Phase Three: Second Round Review (2019 - 2020) Balancing Performance and Implementation

Goal: While ensuring security, begin to focus on evaluating the performance and practical deployment feasibility of the algorithms.

Process: The competition intensified. The remaining 26 algorithms were all "survivors" from the first round, with relatively better security assurance. The focus of this round shifted to: How efficiently do they run on real hardware (from servers to small IoT devices)? Are the key and signature sizes practical? Is the implementation code error-prone? Global researchers conducted extensive benchmarking and side-channel attack analysis (i.e., attempting to steal keys through physical information such as power consumption or electromagnetic radiation) on these algorithms.

July 2020: The Finalists Emerge After another round of rigorous evaluation, NIST announced the candidates for the third round, the final round. This list was divided into two groups:

Finalists: These were the algorithms considered the most mature and promising to become the final standards. Among them, lattice-based cryptography schemes dominated due to their excellent balance of security and performance.

Alternate Candidates: These algorithms also held potential but were slightly less mature or performed less well in certain aspects. NIST kept them as a "Plan B" in case unexpected problems arose with the finalists, and to encourage "algorithmic diversity."

Phase Four: Third Round Review and Final Selection (2020 - 2024)

Goal: Conduct the final, most in-depth review of the finalists and draft the standard.

Process: This was the final sprint. NIST and the global community subjected the 7 finalist algorithms to the most meticulous "interrogation." Discussions refined the focus to the selection of every parameter, optimization techniques on different platforms, and how to write secure code resistant to side-channel attacks. Concurrently, NIST began working closely with the submitters of these algorithms to draft the standardization technical documents.

July 2022: First Winners Announced NIST made a historic announcement, declaring the first four algorithms to be standardized, ending years of speculation:

Universal Encryption/Key Encapsulation Mechanism (KEM): CRYSTALS-Kyber [12]

Universal Digital Signature: CRYSTALS-Dilithium [13], Falcon

High Assurance Digital Signature: SPHINCS+ [14]

2023 - August 2024: Standardization and Finalization NIST released the draft standards (FIPS 203, 204, 205) based on Kyber [12] (ML-KEM), Dilithium [13] (ML-DSA), and SPHINCS+ [14] (SLH-DSA), and sought final

public feedback. After resolving all technical details and feedback, on August 13, 2024, NIST formally published the final versions of these three standards. This marked a watershed achievement in the nearly eight-year global cryptography race, providing a solid technical cornerstone for global PQC migration.

1.4.2.1 First PQC Standards: Balancing Performance and Robustness

The first batch of algorithms ultimately selected and standardized by NIST reflects a deliberate balance between performance, efficiency, and security:

Universal Key Encapsulation Mechanism (KEM): ML-KEM [12] (based on the CRYSTALS-Kyber algorithm) was selected and formally designated as the FIPS 203 standard. It is based on lattice cryptography, showing excellent performance and relatively compact size across various platforms, and is considered the preferred choice for universal encryption scenarios (such as TLS key exchange).

Universal Digital Signature: ML-DSA [13] (based on the CRYSTALS-Dilithium algorithm), also based on lattice cryptography, was chosen as the universal digital signature standard, FIPS 204, due to its good performance and security.

High Assurance Digital Signature: SLH-DSA [14] (based on the SPHINCS+ algorithm) was also standardized as FIPS 205. It is a stateless hash-based signature scheme. Although its signature size is larger and its speed is slower, its security relies only on the strength of the underlying hash function (such as SHA-256). Since hash functions are considered quantum-resistant, this makes SLH-DSA an extremely conservative and reliable choice, suitable for scenarios requiring the highest level of security, such as code signing and root certificate issuance.

1.4.2.2 Algorithmic Diversity: Strategic Foresight from Historical Lessons

NIST's strategic foresight was not limited to selecting the first batch of standards in 2022. They profoundly recognized that staking all hopes on a single type of mathematical difficulty (i.e., lattice cryptography) is itself a risk. History has repeatedly proven that a mathematical fortress that seems impregnable today might be breached by a new attack method tomorrow.

To address this challenge and further enrich the post-quantum cryptography toolbox, NIST initiated a fourth round of additional standardization process ("On-Ramp"), aimed at seeking more promising candidate algorithms. This move attracted continued participation from the world's top cryptographers, one landmark event being the submission of a new candidate standard by the team of Professor Jintai Ding from the University of Cincinnati.

Professor Jintai Ding's participation is of landmark significance. As a core creator of the global PQC standard CRYSTALS-Kyber [12], his continued involvement in the new round of standardization profoundly reflects the industry's strategic consensus—that beyond the existing lattice-based cryptography, it is imperative to explore heterogeneous mathematical foundations to build diverse technical backups for the future.

It is precisely based on this institutionalized adherence to the principle of "algorithmic diversity" that NIST is seeking a backup for lattice cryptography. Thus, on March 11, 2025, NIST announced the selection of an algorithm based on a completely different mathematical problem—the code-based HQC[15]—as another KEM standard. HQC is based on Hamming Quasi-Cyclic codes and has a mature mathematical theoretical foundation. Although its ciphertext size is slightly larger than ML-KEM, as an algorithm based on a different mathematical principle, it

provides critical "security redundancy" for post-quantum migration, serving as a long-term robust alternative should a vulnerability be discovered in lattice algorithms.

The significance of this series of decisions is profound. It institutionalizes the principle of "algorithmic diversity," preparing multiple Plan Bs for the "black swan" event where lattice cryptography might be broken in the future. This fundamentally sends a clear signal to all organizations planning migration: the future security architecture should not be rigid, but must be "Crypto-Agile [23]," meaning it must have the capability to flexibly switch to different cryptographic algorithms when necessary. This is the core foundation of the "Strategic Engine" framework in this white paper.

1.4.3 NIST National Cybersecurity Center of Excellence (NCCoE): The Bridge from Standard to Practice

Merely publishing technical standards is insufficient to solve the complex migration problem. To translate the standards into deployable solutions, NIST established the National Cybersecurity Center of Excellence (NCCoE), whose core mission is to convene experts from industry, government, and academia to collaboratively develop practical, interoperable cybersecurity solutions that address real-world needs.

In response to the major challenge of PQC migration, the NCCoE's work was launched almost simultaneously with the NIST PQC standardization group, with preparations starting as early as 2018. They formally initiated the "Migration to Post-Quantum Cryptography" project. The project aims to facilitate the migration efforts of various organizations by publishing white papers, playbooks, and proof-of-concept implementations.

The immense practical value and industry credibility of this project are reflected in its broad cooperation base. Project participants include not only tech giants like AWS, Microsoft, Cisco, Intel, IBM, and

international companies like Samsung SDS, but also financial institutions such as HSBC and JPMorgan, and government partners including the US National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA) of the US Department of Homeland Security.

1.4.3.1 Strategic Validation: NCCoE Practice Validates the "Migration Engine" Framework

The organizational structure and workflow of this project provide strong real-world validation for the "Strategic Engine" framework proposed in this white paper. The NCCoE project is primarily advanced through two core workflows, whose content highly aligns with the strategic modules of this white paper:

Cryptographic Discovery Workflow

This workflow focuses on using automated tools to help organizations inventory their cryptographic assets, i.e., understand where and how cryptography is used to protect data and systems. Its goal is to establish a detailed Cryptographic Bill of Materials (CBOM), and based on this, to conduct risk management and migration prioritization (e.g., applying the "Mosca Theorem"[8]). Strategic Correspondence: This is entirely consistent with the goal of the "Gaining Initial Momentum: Strategic Foresight and Risk Intelligence" stage of the "Strategic Engine" in this white paper.

Interoperability and Performance Workflow

This workflow aims to explore and answer a key question: how will the newly published NIST PQC standard algorithms perform in real-world communication protocols (such as TLS, SSH) and hardware security modules (HSM). It verifies the performance impact and system compatibility of PQC solutions by testing them in near-real environments. Strategic Correspondence: This is precisely the practical manifestation of the "Building Momentum: Post-Quantum Cryptography

Technology Stack" and "Accelerating the Engine: Simulation and Verification Module" stages in the "Engine" framework of this white paper.

1.4.3.2 Integrating NIST CSF 2.0: A Closed Loop from Technology to Governance

The NCCoE's practice not only validated the technical pathways but also deeply integrated them into the NIST Cybersecurity Framework 2.0 (CSF 2.0). The NCCoE mapped the complex PQC migration process to the six core functions of CSF 2.0—Govern, Identify, Protect, Detect, Respond, and Recover. This mapping provides organizations with a standardized management language, ensuring that PQC migration is not just a technical upgrade but part of the organization's overall cybersecurity governance.

1.4.3.3 Strategic Direction and Compliance Rigidity

The "Technology + Management" framework established by the NCCoE is, in effect, the official blueprint for addressing global compliance pressure. This aligns closely with the top-level strategy of the US Federal Government: according to the National Security Memorandum (NSM-10[20]) and related executive orders, the US has drawn a red line, requiring the complete replacement of product chains based on quantum-resistant algorithms (such as TLS upgrades) for National Security Systems (NSS) and critical infrastructure before 2035.

Therefore, the NCCoE project results not only prove the feasibility of the "Strategic Engine" framework but also reveal to the global industry: following the CSF 2.0 framework for orderly migration is the only correct path to meet the 2035 compliance deadline.

1.4.4 Publication of IETF RFC 9xxx (Mid-2025)

Following the release of the foundational algorithm standards by NIST, the IETF formally published the RFC standard document supporting

Hybrid Key Exchange in TLS 1.3. This signifies that PQC is no longer just a mathematical algorithm but has officially become a core component of internet communication protocols.

The core value of this RFC lies in establishing a dual-assurance mechanism of "Traditional Algorithm + Post-Quantum Algorithm" (e.g., the X25519 + ML-KEM combination)[16]. This hybrid mode has immense strategic significance:

Defense in Depth: It simultaneously utilizes the mature security of traditional Elliptic Curve Cryptography (ECC) and the quantum resistance of PQC. Even if a theoretical flaw is discovered in the PQC algorithm in the future, the traditional ECC can still hold the security baseline, eliminating industry concerns about relying on a single new technology path.

Countering "Harvest Now, Decrypt Later": By introducing the PQC element, the protocol immediately grants the data stream the ability to resist decryption by future quantum computers, solving the storage security problem for long-lived data.

This global common standard at the internet communication protocol layer completely clears the final protocol hurdles for cloud providers (like AWS, Azure) and CDN providers (like Cloudflare, Akamai) to implement large-scale infrastructure-level switching, enabling PQC to transition from an "experimental option" to a "default enabled configuration."

1.4.5 Global Policy Convergence: Closing the Window of Hesitation

Following the establishment of the technical foundation and the clarification of the threat, major global economies have successively introduced policies that transform PQC migration from an option into a mandatory task. Although these policies differ in specific implementation mechanisms, they demonstrate striking consistency in goals and timelines, collectively forming an irreversible global migration wave.

CBOM Compliance Baseline (2025): The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the European Union, in their 2025 software supply chain security guidance, for the first time explicitly require critical infrastructure vendors, when submitting an SBOM (Software Bill of Materials), to also include a CBOM (Cryptography Bill of Materials) that clearly labels the cryptographic algorithms used and their source. This move directly transfers the pressure for PQC migration to the very upstream of the entire software supply chain.

1.4.5.1 The United States: A Multi-layered Engine of Enforcement

The U.S. PQC policy framework is a complex and precise system, composed of strategic directives from the White House, legislation from Congress, implementation guidance from executive departments, and mandatory standards from national security agencies, progressing layer by layer and interlinking seamlessly.

Strategic Direction:

White House National Security Memorandum 10 (NSM-10)[20]: On May 4, 2022, the Biden administration issued National Security Memorandum 10 (NSM-10)[20], setting the highest level of strategic direction for PQC migration in the United States. The memorandum clearly states that the U.S. goal is to "mitigate quantum risk as much as possible before 2035," and instructs all federal agencies to launch a multi-year process for migrating to PQC. NSM-10[20] itself does not set specific algorithm deprecation dates but serves as the "starting gun" for the entire national effort, providing legitimacy and strategic basis for all subsequent specific policies.

Trump Administration Executive Order on Strengthening National Security and Technological Leadership in the Post-Quantum Era (June 2025): Following NSM-10[20]'s foundational work, President Trump signed a new Executive Order in June 2025, aimed at transforming

"strategic planning" into "decisive execution." The order emphasizes an "America First" quantum-safe supply chain and explicitly introduces a "Federal Procurement Circuit Breaker"—requiring that beginning in Fiscal Year 2026, all critical IT products procured by the federal government must possess post-quantum capability (or have a clear upgrade path), otherwise they will face a procurement ban. This measure greatly accelerates the compliance pace for the private sector (especially defense contractors and critical infrastructure vendors), forcing them to produce concrete migration roadmaps in the short term.

Legislative Solidification:

To ensure policy continuity, the U.S. Congress passed the Quantum Computing Cybersecurity Preparedness Act at the end of 2022, which was signed into law by the President on December 21, 2022. This act legally solidifies the core requirements of NSM-10 [20], requiring the Office of Management and Budget (OMB) to regularly report migration progress to Congress, thereby establishing a long-term mechanism to ensure executive branch execution and accountability.

Implementation Guidance:

OMB M-23-02 [30] Memorandum: To translate the strategic goals of NSM-10 [20] into concrete action, OMB issued Memorandum M-23-02 on November 18, 2022. This document requires all Federal Civilian Executive Branch (FCEB) agencies to complete an inventory of cryptographic systems within their information systems and submit cost estimates for migrating to PQC within a specified time frame. This is the first concrete execution step for PQC migration—"taking inventory."

Mandatory Enforcement Engine:

NSA's CNSA 2.0 [21] and NIST's Deprecation Timetable: The most

forceful part of the U.S. policy framework comes from the specific technical standards and timelines issued by the National Security Agency (NSA) and NIST. These documents translate high-level goals into binding, hard requirements for technology vendors and government agencies.

For National Security Systems (NSS): In September 2022, the NSA released the Commercial National Security Algorithm Suite 2.0 (CNSA 2.0 [21]), setting a highly aggressive and clear migration timetable for the NSS and its suppliers (including the vast Defense Industrial Base). For example, it requires that: by 2025, systems used for software and firmware signing, web browsers/servers, and cloud services must support and prioritize the PQC algorithms specified in CNSA 2.0. By 2030, traditional network equipment (such as VPNs, routers) and systems used for software/firmware signing must exclusively use PQC algorithms, with non-PQC-supporting equipment being phased out.

For Federal Systems: In November 2024, NIST released its draft technical report IR 8547 [22], providing an algorithm deprecation timetable for broader federal systems. The report explicitly states that traditional public-key algorithms with security levels below 128 bits (such as RSA-2048) are expected to be "deprecated" after 2030 and "disallowed" after 2035. This perfectly aligns with the overall 2035 goal of NSM-10 [20] and provides specific technical deadlines.

The sophistication of this multi-layered policy system lies in the fact that, while the mandatory timetable of CNSA 2.0 [21] is nominally only applicable to National Security Systems, it effectively serves to set the "de facto standard" for the entire U.S. and global technology market. Large technology vendors, such as cloud computing giants, operating system developers, and network equipment manufacturers, must make their commercial products comply with the stringent requirements of CNSA 2.0 in order to sell to the vast market of the U.S. Department of Defense and the intelligence community. This results in them integrating the CNSA 2.0 timeline into the R&D roadmap of their mainstream

products. Consequently, even an ordinary commercial company with no government business, when procuring new software, hardware, and cloud services, will find that these products have already achieved PQC compatibility according to the CNSA 2.0 rhythm. This market ripple effect, driven by federal procurement, greatly accelerates the adoption of PQC in the private sector, with its impact far exceeding the direct jurisdiction of government directives.

1.4.5.2 The European Union: Building a Coordinated European Continental Defense Line

In contrast to the U.S. top-down model, the evolution of the EU's PQC policy reflects a collaborative process from member states acting independently to forming a unified strategy, with its ultimate enforcement relying more on its robust regulatory framework.

Pioneers: Germany and France

Before a unified policy was formed at the EU level, Germany and France, as technological leaders, had already begun forward-looking planning.

German Federal Office for Information Security (BSI): Since 2020, the BSI has published its PQC migration recommendations and continuously updates its technical guidance (TR-02102-1). BSI not only closely follows NIST's pace but also recommends algorithms like FrodoKEM, which it considers to have higher security redundancy, and consistently emphasizes the importance of "Cryptographic Agility" and "Hybrid Mode."

French National Cybersecurity Agency (ANSSI): ANSSI released its PQC migration position paper in January 2022, clearly proposing a phased transition roadmap and strongly recommending the adoption of a hybrid mode to ensure that the defense capability against classical attacks is not reduced when introducing PQC. Furthermore, France has jointly released a position paper on Quantum Key Distribution (QKD) with

countries including Germany, the Netherlands, and Sweden, demonstrating its willingness to seek transnational coordination early on.

Unification Process: 2024 Commission Recommendation and 2025 Roadmap

The turning point for EU PQC policy came on April 11, 2024, when the European Commission issued a formal recommendation urging member states to develop a coordinated PQC implementation roadmap through the Network and Information Systems Security Cooperation Group (NIS Cooperation Group). This process culminated on June 23, 2025, with the European Commission and member states jointly releasing the Coordinated Implementation Roadmap for PQC Migration [24]. This document is the EU's current core PQC policy guideline, setting clear milestones:

By the end of 2026: All member states should launch national PQC migration strategies and begin taking "first step" actions, such as risk assessment and inventory of cryptographic assets.

By the end of 2030: PQC migration for high-risk use cases, especially critical infrastructure [24] (energy, finance, transport, health, etc.), must be completed.

By the end of 2035: Migration for medium- and low-risk systems should be substantially completed.

Unlike the U.S., where federal procurement is the main driver, the enforcement of the EU PQC roadmap will be realized through its powerful regulatory system. Although the roadmap [24] itself is a "recommendation," EU cybersecurity regulations, such as the Network and Information Systems Security Directive (NIS2) and the Cyber Resilience Act (CRA), require relevant entities to adopt "state-of-the-art" security measures. As PQC standards are finalized and related products are commercialized, PQC will quickly be defined as a "state-of-the-art"

security practice. At that point, regulatory bodies in EU member states, when enforcing regulations like NIS2, will consider the failure to plan and implement PQC migration as non-compliance, particularly in the critical infrastructure sectors facing the 2030 deadline. This compliance-driven model will strongly push PQC migration in the entire EU private sector through the threat of potential massive fines and legal liabilities.

1.4.5.3 The United Kingdom: A Pragmatic and Structured National Roadmap

Post-Brexit, the UK, under the leadership of its National Cyber Security Centre (NCSC), has adopted a pragmatic path that is both aligned with allies and uniquely characterized.

In November 2023, the NCSC released its PQC Migration White Paper[26], sending a clear signal to start preparations immediately. Subsequently, in March 2025, the NCSC published a more detailed PQC Migration Timetable guide, setting a clear three-phase national roadmap for the UK:

Phase One (by 2028): Organizations should complete comprehensive cryptographic asset discovery and assessment, define migration goals, and formulate preliminary migration plans.

Phase Two (by 2031): Complete early, highest-priority PQC migration activities and refine the detailed migration roadmap based on technological and market developments.

Phase Three (by 2035): Complete PQC migration for all systems, services, and products, keeping pace with the final goals of the U.S. and the EU.

The NCSC guidance is notable for its extreme emphasis on preparation, deliberately reserving 2-3 years for early activities such as discovery, assessment, and planning. This reflects a deep understanding and pragmatic attitude towards the complexity of migration for large organizations.

The UK's strategy can be seen as a "pragmatic bridge" connecting the U.S. "procurement-driven" model and the EU's "regulation-driven" model. On the one hand, the NCSC sets clear government timetables[26], providing clear targets for the industry. On the other hand, it also strongly emphasizes driving the process through market mechanisms, for example, encouraging organizations to issue "Statements of Migration Intent" to their suppliers to stimulate the market supply of PQC products and services. Additionally, the NCSC plans to launch a certification program for PQC migration consulting firms, aiming to cultivate a credible domestic professional service market rather than relying solely on top-down regulation. This hybrid model allows the UK to flexibly adjust its implementation strategy according to its national economic structure while maintaining strategic coordination with the Five Eyes alliance (especially the U.S.) and the EU, achieving policy goals by guiding the market.

1.4.5.4 International Organization for Standardization (ISO/IEC): Another Piece of the Global Consensus Puzzle

In addition to the NIST standards, the International Organization for Standardization is also actively advancing PQC standardization. ISO/IEC JTC 1/SC 27 has proceeded with relevant amendments in 2024 to include algorithms such as Kyber and Dilithium into the ISO/IEC 18033-2 (asymmetric encryption) and ISO/IEC 14888-3 (digital signature) standard systems[18-19]. For many multinational enterprises outside the U.S. and EU, ISO standards are often an important basis for procurement compliance, which further strengthens the global coverage network of PQC standards.

1.4.5.5 China's "Dual-Track Strategy": Cryptographic Autonomy and Standard Leadership

The most distinctive feature of China's PQC strategy is its firm

commitment to the "independent and controllable" path. The fundamental driving force for this choice stems from deep-seated concerns over potential "backdoors" in foreign-dominated technologies, as well as the national grand strategy of achieving technological self-reliance. This strategic stance dictates that China will not simply adopt or follow the U.S. NIST standards, but is committed to establishing an independent, China-led cryptographic ecosystem.

To achieve this goal, China has taken systemic actions through its official standardization bodies. In February 2025, the China Cryptography Standardization Technical Committee (CSTC) and the Institute of Commercial Cryptography Standards (ICCS) jointly launched a global solicitation for next-generation commercial cryptographic algorithms[27].

This action quickly achieved substantial progress. On October 9, 2025, the ICCS officially released the Announcement on Candidate Algorithms for Next-Generation Commercial Cryptography. This landmark document not only published the list of algorithms that passed the preliminary review but also clarified China's PQC standardization "timetable" and "roadmap." The announcement shows that the shortlisted algorithms cover multiple technical approaches such as lattice-based cryptography, code-based cryptography, and multivariate cryptography, and explicitly requires the core standards to be drafted before 2027.

This series of actions embodies a highly mature strategy: it leverages global top intellectual resources (such as the competition accumulation organized by CACR since 2018) to elevate the technical level of its national standards, while fully ensuring that the final outcomes comply with its core principle of "independent and controllable." This is essentially a "Chinese-style open innovation" aimed at creating a PQC standard system that is both globally influential and firmly controlled by China itself.

Meanwhile, China has adopted a "dual-track" strategy, pursuing PQC in parallel with Quantum Key Distribution (QKD). China has invested heavily in hardware QKD, which is based on physical principles, building the world's largest QKD backbone network.

However, we must be soberly aware of the objective limitations of the QKD technical route. QKD network construction costs are extremely high, and it relies heavily on dedicated physical fiber optic links, making it difficult to flexibly deploy in software form over large-scale, untrusted public computer networks (such as the Internet). More crucially, QKD only solves the key distribution problem and cannot provide the essential "identity authentication" function vital to the digital economy. Therefore, QKD will primarily be confined to specific secure communication private network scenarios, such as government, military, and financial backbone networks, both now and for a long time in the future.

1.4.5.6 The Post-Quantum Evolution of SM9—From Identity-Based Cryptography to Post-Quantum Identity-Based Cryptography

In 2025, the China National Data Administration, in advancing the construction of the "National Integrated Data Market," explicitly proposed to carry out pilot applications of anti-quantum encryption technology in the cross-regional, cross-entity data circulation (especially the "East Data, West Computing" project). This marks the expansion of China's PQC driving force from mere "security compliance" to the infrastructure construction level of "data element assetization."

To understand the uniqueness and complexity of China's PQC migration, there is no better case than analyzing the post-quantum evolution path of the SM9 algorithm within its commercial cryptography (SM) system. This process is not just an upgrade of a single algorithm but a comprehensive stress test and capability demonstration of China's entire autonomous cryptography strategy.

SM9 Status Quo: Functional Advantages and Quantum Vulnerability

SM9 is one of the core pillars of China's commercial cryptography system, an Identity-Based Cryptography (IBC) algorithm. Its entire family of algorithms, including digital signature, key encapsulation, and key exchange protocols, is not only widely used domestically but has also successfully gained recognition under ISO/IEC international standards[18-19], demonstrating its technical maturity and international influence.

The core innovation of SM9 is that it allows the use of a user's unique identity identifier (such as email address, phone number, or device ID) directly as their public key, thereby completely eliminating the complex digital certificate issuance, distribution, and management chain of traditional Public Key Infrastructure (PKI). The user's private key is generated and securely distributed by a trusted authority—the Key Generation Center (PKG)—using the system's master key. This "certificate-less" model greatly simplifies key management in large-scale network environments, particularly suitable for scenarios with massive nodes like the Internet of Things and Industrial Internet.

However, SM9's powerful functionality is built upon a fragile mathematical foundation. Its security relies on bilinear pairing operations on elliptic curves. Unfortunately, this mathematical problem is one of the targets that Peter Shor's quantum algorithm[7] can solve efficiently. This means that once a practical quantum computer emerges, the security of the entire current SM9 cryptographic system will instantly collapse. Therefore, upgrading SM9 to be post-quantum is not an option for its ecosystem but an inevitable requirement concerning its very survival.

Technical Path for SM9 Post-Quantum Evolution: Judgment Based on Industry Trends

The evolution of China's commercial cryptography system often follows rigorous scientific logic and national strategic needs. Although specific official migration details are still being formulated, combining the national cryptography strategy, public consultation drafts, and academic consensus, we can construct a forward-looking evolution reference framework from the perspectives of technical logic and industry demand.

Algorithm Kernel Replacement through Sovereign Standardization

The core of the migration is a fundamental replacement of SM9's mathematical engine. The global PQC algorithm solicitation launched by CSTC/ICCS in 2025 provides a standardized selection platform for finding an anti-quantum "heart" for SM9. To fully retain SM9's core advantage as an identity-based cryptosystem, simply adopting a NIST-standardized general Key Encapsulation Mechanism (such as ML-KEM [12]) is far from sufficient. Its replacement must be a Post-Quantum Identity-Based Encryption (PQC-IBE) scheme[28].

Currently, the most promising and deeply researched PQC-IBE construction path recognized by academia and industry is based on Lattice-Based Cryptography[28]. This is highly consistent with China's national strategy. The research guidelines for cryptography technology during the "14th Five-Year Plan" period, issued by the National Cryptography Administration, explicitly designate the security analysis of lattice-based cryptography (including LWE, SVP, and other problems) as a key supported direction, even setting assessment indicators like "breaking relevant international challenge records". This indicates that China is pooling national resources to fully master the core mathematical

tools required to build the next-generation PQC-IBE, laying a solid theoretical foundation for the SM9 upgrade[28].

Building a Pragmatic Transition Bridge with Hybrid Implementation Mode

For a large-scale cryptographic system already deeply integrated into various applications, an aggressive "rip-and-replace" style substitution is unfeasible. The consensus in the global cryptographic community, including IETF drafts and guidance from agencies like NIST and NCSC, points to the Hybrid Mode[17] as the smoothest and lowest-risk transition strategy. The hybrid mode combines a mature traditional algorithm (like the existing SM9) with a new PQC algorithm (like the future PQC-SM9); as long as at least one of them is secure, the overall security is guaranteed.

China's migration plan explicitly supports this path. The aforementioned national scientific research guidelines explicitly established the research topic of "Fusion Method Research for Existing Cryptographic Protocols and Post-Quantum Public-Key Cryptography Algorithms". This provides official policy and funding support for SM9 to adopt the hybrid mode. In practice, a hybrid SM9-PQC scheme's key encapsulation process might simultaneously execute one classic pairing-based operation and one brand-new lattice-based operation, combining the two results to generate the final session key. This design achieves two critical goals simultaneously:

Backward Compatibility: Un-upgraded systems can ignore the PQC portion and continue to communicate using the classic portion, ensuring business continuity.

Forward Security: The presence of the PQC portion can effectively defend against the "Harvest Now, Decrypt Later" (HNDL) attack, because even if an adversary possesses a quantum computer in the future, they will not be able to break the portion of the key protected by PQC.

Undertaking Systemic Infrastructure and Ecosystem Restructuring: The Generational Shift of Trust Anchors

The migration of SM9 faces challenges far more severe than traditional PKI—specifically, the resetting of Trust Anchors. In the SM9 architecture, a user's private key is derived by the Private Key Generator (PKG) using a Master Key.

Reconstructing the Root of Trust: Migrating to post-quantum algorithms (such as Lattice-based PQC-IBE) means the PKG must replace its mathematical "heart"—the Master Key. This is not merely a software upgrade; it mandates that all users must re-register with the new PKG to obtain new private keys.

The Burden of Legacy Data: The old PKG cannot be taken offline immediately, otherwise historical data will become indecipherable; the new PKG must be brought online in parallel. This long-term coexistence and eventual switch-over of "Dual Trust Sources" represents the greatest engineering risk point in the SM9 migration.

Conclusion: This reality dictates that the SM9 migration cannot be an incremental patch, but must be a carefully orchestrated "Holistic Lattice Transition" (a play on words implying a comprehensive system-wide switch to Lattice cryptography).

Therefore, the migration of SM9 is by no means a simple algorithm replacement; it requires a thorough, systemic restructuring of the existing identity-based cryptography ecosystem. China's planners have a clear understanding of this. The national scientific research guidelines require the undertaking units to develop the "Overall Technical Architecture for Post-Quantum Migration of Cryptographic Infrastructure and Cryptographic Devices," including "adaptation indicators for underlying anti-quantum cryptographic algorithms and digital certificates".

This clearly indicates that the migration plan is a full-stack

engineering effort, with a scope covering:

Core Infrastructure: Upgrading the software and hardware of the Key Generation Center (PKG) to enable it to manage and distribute lattice-based PQC-IBE private keys.

Application Development: Providing application developers with brand-new Software Development Kits (SDKs) that support both hybrid and pure PQC modes.

Cryptographic Hardware: Researching and deploying Hardware Security Modules (HSM), encryption cards, and security chips that support the new PQC-IBE algorithms, such as the "Liang-Kai" series products already released by China Electronics Corporation (CEC), to provide hardware acceleration for high-performance scenarios.

Protocols and Standards: Defining new protocol flows and data formats to accommodate the larger public/private key sizes and signature volumes brought about by PQC-IBE algorithms.

The successful migration of SM9 will be the ultimate proof that China can independently and autonomously complete a complex intergenerational shift in its next-generation cryptography system, serving as the flagship project and best example of China's "independent and controllable" PQC strategy. At the same time, this decision also reveals its strategic priority: to retain the significant convenience of identity-based cryptography in key management, China is willing to undertake the corresponding migration complexity—a strategic foresight focused on long-term operational efficiency rather than short-term migration ease.

The table below summarizes the evolution framework of SM9 from its current state to its future post-quantum state.

Table 1.3: SM9 Migration Framework: From Current State to Post-Quantum

Future

Feature	Current SM9 (Based on GM/T 0044 Standards)	Future Quantum-Resistant SM9 (Proposed)
Cryptographic Basis	Pairing-Based Cryptography (Bilinear Pairs)	Lattice-Based Cryptography (e.g., LWE/Ring-LWE problems)
Security Posture	Resists classical computer attacks; vulnerable to Shor's quantum algorithm	Resists all known classical and quantum attacks
Key Management Model	Identity-Based Cryptography (No PKI certificates), relies on centralized Key Generation Center (PKG)	Maintains Identity-Based model, relies on PQC-upgraded PKG

Standardization Carrier	GM/T 0044-2016, ISO/IEC 11770-3, etc.	New National Standards generated through the 2025 CSTC/ICCS Post-Quantum Cryptography Algorithm Solicitation[27]
Transition Strategy	N/A	Hybrid Mode: Parallel operation of classical SM9 and new PQC-IBE to ensure backward compatibility and forward security
Ecosystem Components	Pairing-based PKG, SDK, Hardware, and Applications	Upgraded PKG, Brand new PQC-IBE SDK, New Hardware Cryptographic Modules, and Adapted Applications
Trust Anchor Migration Difficulty	N/A (System Established)	Extremely High (Requires rebuilding root keys, all users must re-acquire private keys, and faces complex O&M for "dual-root

coexistence")

Strategic Impact and Outlook: Commercial Cryptography's Complete Renewal Reshapes the Industry Landscape

China's PQC migration strategy centered on commercial cryptography is not merely a defensive security upgrade; it is a strategic offensive aimed at reshaping the global cryptography landscape and competing for future technological standard dominance. This process will trigger a major shift in the entire cybersecurity industry and generate profound strategic impacts.

Firstly, the complete intergenerational replacement of the commercial cryptography system will spur massive industry restructuring opportunities. This is not just a replacement of a single algorithm but a full-stack update, from the underlying cryptographic chips and operating systems to the upper-layer application software and gateway devices. As China establishes an independent and autonomous PQC standard system (covering the full suite of PQC-SM2/3/4/9, etc.), all multinational companies operating in China will face significant "Compliance Friction." Companies must develop and maintain systems with a high degree of "cryptographic agility," enabling them to flexibly switch between NIST-based standards and China's commercial cryptography standards according to geographic location and regulatory requirements. This will force the cybersecurity industry to shift from simple "compliance sales"

to providing "dual-stack compatible" high-tech solutions, thereby greatly increasing the complexity and value threshold of R&D, testing, and supply chain management.

Secondly, on a more macro level, this may accelerate the trend of the global digital infrastructure moving towards "technological bipolarization" or "cryptographic divergence." The future may see two parallel, mutually incompatible cryptographic ecosystems: one centered on the U.S./NIST standards, and the other centered on the China/CSTC standards. This situation will pose long-term and profound challenges to global Internet interoperability, the smooth flow of international data, and the integrity of the global technology supply chain.

1.4.5.7 Japan: Active R&D and Strategic Alignment

Japan's PQC efforts are led by the National Institute of Information and Communications Technology (NICT) and the Cryptography Research and Evaluation Committee (CRYPTREC). Japan's strategy is a "two-pronged approach": on one hand, actively investing in independent R&D and security assessment, even submitting its own candidate algorithms to NIST, aiming to build a domestic expertise system rather than passively accepting external standards. On the other hand, its publicly released guidelines and industry practices show a high degree of alignment with the NIST process, ensuring interoperability with Western partners. Japan also has significant research in the QKD domain, but its overall strategy appears more integrated into the Western technology ecosystem.

1.4.5.8 South Korea: Comprehensive National Master Plan

The South Korean government has demonstrated strong top-level design capabilities, releasing a clearly structured Post-Quantum Cryptography Transition Master Plan, aiming for national migration completion by 2035. This plan is strongly supported by a national

strategic technology development program, committing to invest trillions of Korean Won (billions of US dollars) to develop core technologies, including kilobit-scale quantum computers, and to cultivate a massive talent pool in quantum technology. The plan is subdivided into six major directions, such as technology acquisition, legal revision, and industrial base construction, showcasing an ambitious blueprint for comprehensively building a "quantum economy."

However, the international influence of South Korean standards is relatively small. The main reason is that its international PQC standard solicitation activity stipulates that the lead proponent of all proposals must be South Korean. This exclusivity clause has, to some extent, limited the depth of participation by top global academics, making its standards more inclined towards domestic use rather than international universality.

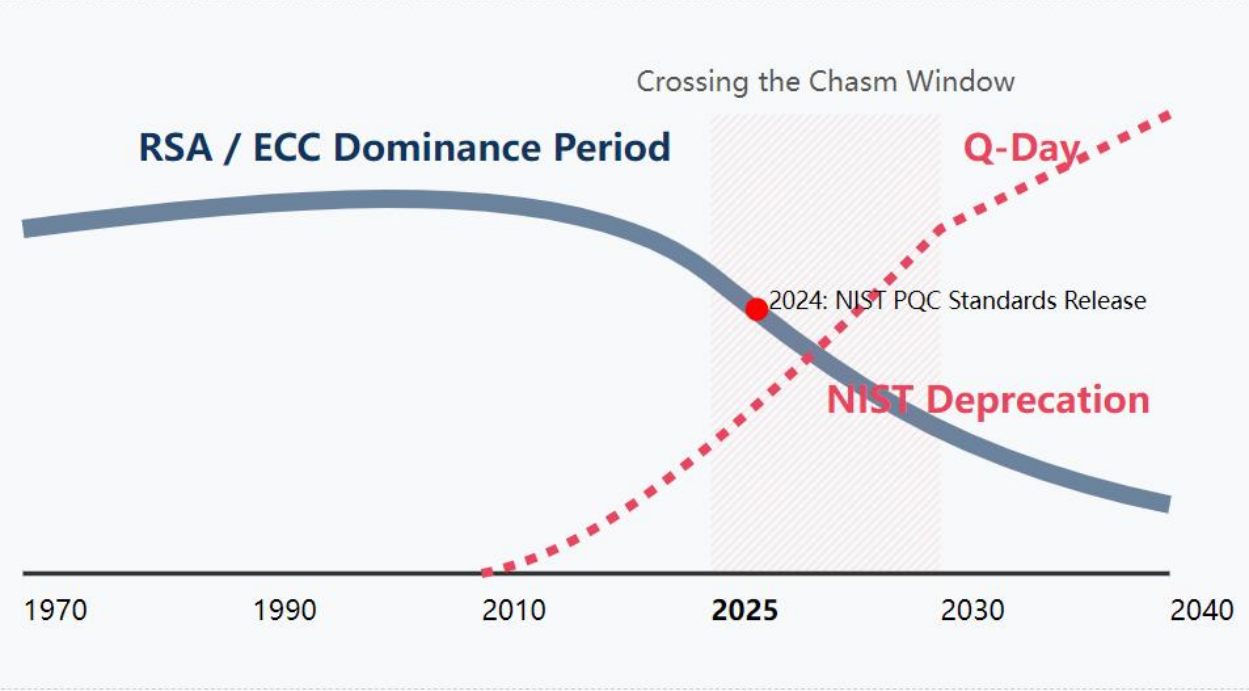
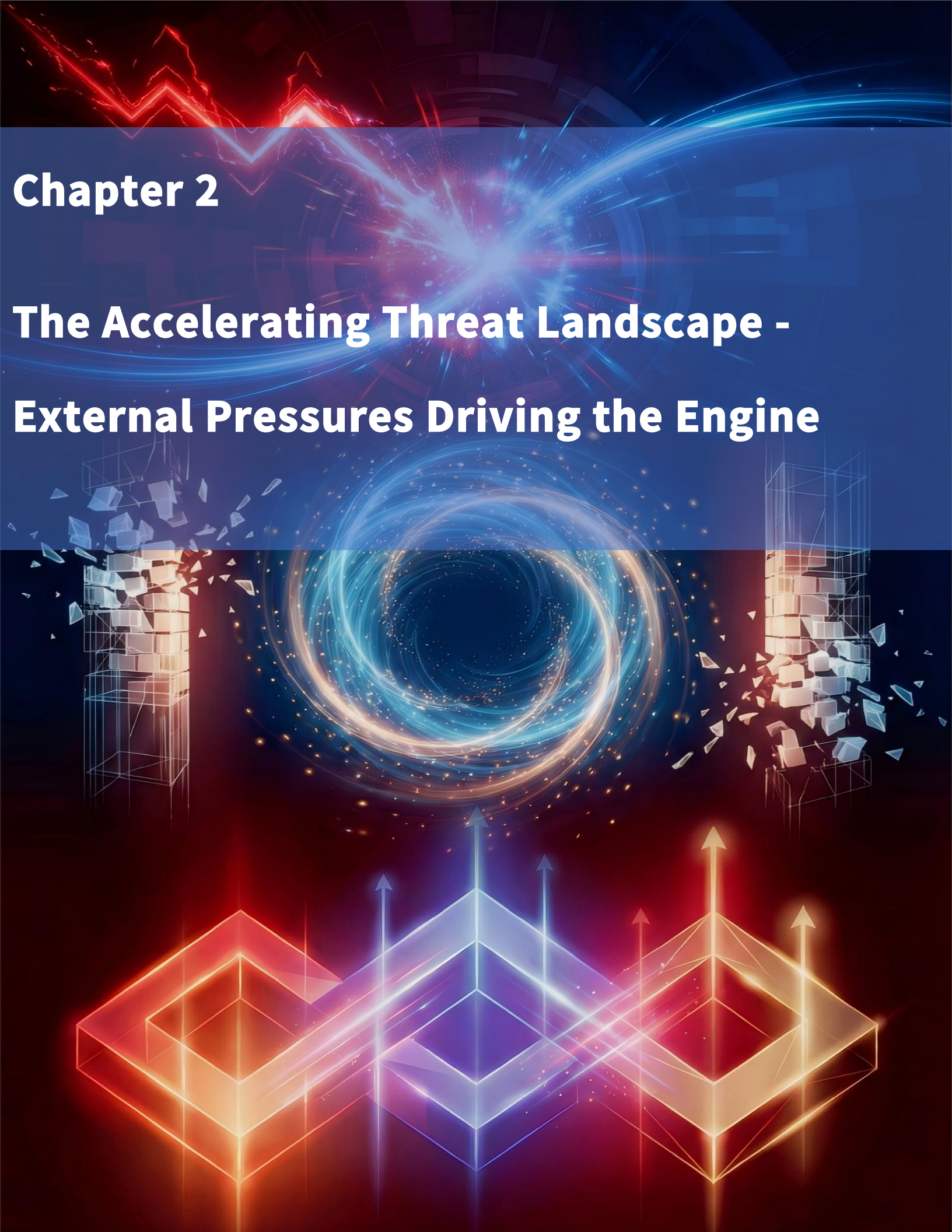


Figure 1.2: Timeline of Digital Trust Paradigm Shifts (1970-2040)

Chapter 2

The Accelerating Threat Landscape - External Pressures Driving the Engine



Chapter 2: The Accelerating Threat Landscape - External Pressures Driving the Engine

This section aims to clarify "why act"—the powerful, unignorable external pressures that are forcing global organizations to launch a vigorous migration engine.

2.1 The Shrinking Timeline: Why the Quantum Threat is Imminent

With the continuous development of quantum computing technology, its potential threat to existing cryptographic algorithms (such as RSA and ECC) has attracted widespread attention. The introduction of Shor's algorithm[7] theoretically demonstrates the ability of a quantum computer to break these classical cryptographic algorithms. To quantify this accelerating trend, we can adopt a research-based quantitative analysis model to evaluate the quantum resources and expected time required to break different cryptographic algorithms.

The HNDL attack has fundamentally altered the time logic of cybersecurity defense, introducing an extremely dangerous "asymmetric urgency." The defender must complete the cryptographic migration before the data loses its confidential value, while the attacker has a relatively ample amount of waiting time. Professor Michele Mosca of the University of Waterloo, Canada, proposed Mosca's Theorem[8], which brilliantly quantifies this crisis and provides us with a clear decision-making model:

$$X + Y > Z$$

Where:

X represents the number of years the data needs to remain

confidential (e.g., a mortgage contract might be 30 years, a state secret might be 50 years).

$\mathbf{Y}$ represents the time required for the entire financial system to migrate to post-quantum cryptography (including standard setting, hardware and software upgrades, interoperability testing, etc.).

$\mathbf{Z}$ represents the time until a cryptographically relevant quantum computer (CRQC) is realized and has the capability to break the encryption.

The theorem states that if $\mathbf{X} + \mathbf{Y} > \mathbf{Z}$, the system is already in a state of substantial insecurity, because the quantum computer will be able to decrypt the data still within its confidentiality period before the migration is complete.

This inequality is extremely alarming for any industry that relies on long-term sensitive data. The confidentiality period for a large amount of core high-value data (such as trade secrets, intellectual property, personal privacy files, medical records, or critical infrastructure blueprints) often lasts for 20 to 50 years.

Considering the massive scale of modern information systems, the complexity of legacy architectures, and the deep reliance on the supply chain, a conservative estimate for achieving full-system secure migration is 5 to 10 years, or even longer. Given that industry experts generally predict that a CRQC may emerge within the next 10 to 15 years (the $\mathbf{Z}$ value), the inequality $\mathbf{X} + \mathbf{Y} > \mathbf{Z}$ is highly likely to hold true today.

This means that for data with long-term value, the safe "deadline" has effectively passed, and we are in an "overtime" period in a race against time. This urgency compels all sectors to immediately initiate large-scale post-quantum migration preparations today, even before quantum computers are fully mature. Any delay is equivalent to handing over future information assets to an adversary.

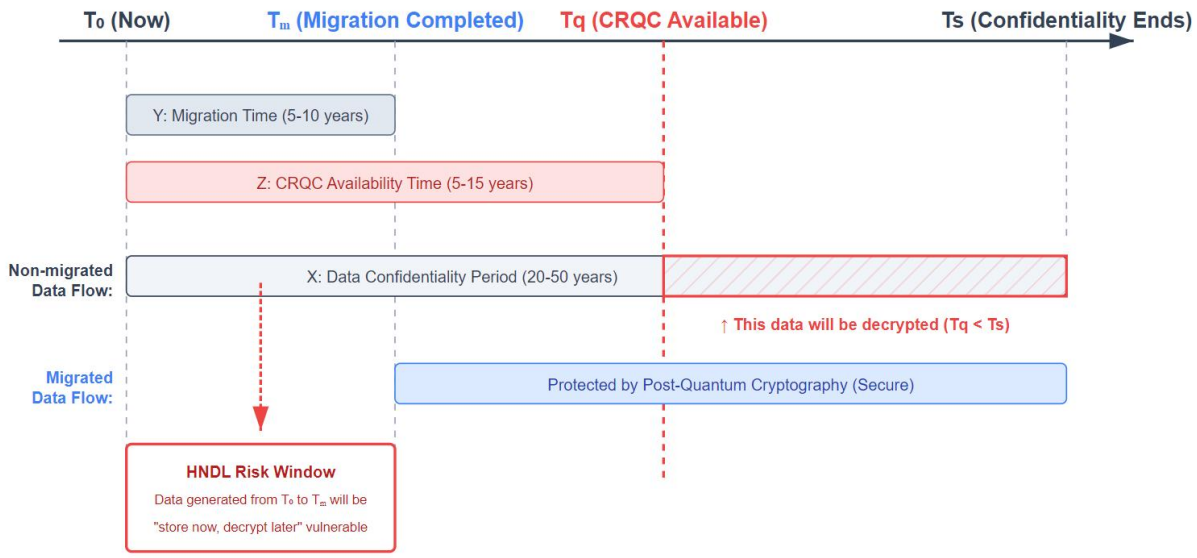


Figure 2.1: Mosca's Theorem Timeline Analysis and HNDL Risk Window

This figure illustrates the data security time window under the "Harvest Now, Decrypt Later" (HNDL) threat. Since the data confidentiality period (X, 20-50 years) is often much longer than the time until the quantum computer is available (Z, 5-15 years), i.e., $T_q < T_s$, traditional encrypted data created at the current moment (**Now**) faces the certainty of future decryption risk.

(Note: It is currently unknown whether T_m or T_q will occur first; data generated at T_0 is only safe if $T_q > T_s$)

Furthermore, this figure intuitively shows how a "Security Deficit" is formed. Consider the following typical scenario:

Real-world Case (2025): A bank signs a 30-year residential mortgage contract today or stores a national infrastructure blueprint with a 50-year secrecy period (X = 30 ~ 50).

Quantum Node (2035): The industry predicts that quantum computers with cracking capabilities will emerge in 10 years (Z = 10).

Conclusion: Even if we ignore the time required for migration (Y), the inequality $X > Z$ already holds. This means that this data generated today will be in a "naked" (fully exposed) state for the future 20-40 years of its secrecy period. For long-term assets, the risk window is not opening in the future but is already wide open right now.

2.1.1 Quantitative Analysis: Quantum Bit Requirements and Timeline for Breaking RSA and ECC

According to Shor's algorithm[7] and the latest data disclosed in the ETSI/QSC 2024 (Singapore) annual meeting report, the logical quantum bit requirements for breaking RSA and ECC encryption algorithms vary with key length. The following table is based on the research from the aforementioned cutting-edge conference, showing specific resource requirements and time predictions based on current development trends.

Table 2.1: Logical Quantum Bits Required to Break RSA/ECC

Encryption Algorithm	Key Length	Logical Qubits Required to Break	Physical Qubits Required to Break (Est.)	Projected Timeline (Fault Tolerant)
RSA	1024-bit	2000-2500	~2 million	2030
RSA	2048-bit	4000-5000	~4 million	2040
ECC	160-bit	1500	~1.5 million	2028
ECC	256-bit	4000	~4 million	2035

Logical Qubits vs. Physical Qubits: The "logical qubits" in the table are the idealized, error-free computational units required to execute the

algorithm. However, real-world quantum bits ("physical qubits") are extremely susceptible to environmental noise and errors. To construct a reliable logical qubit, a large number of physical qubits must be used to form an error correction code for protection.

It is alarming that this conversion ratio (overhead) is undergoing disruptive breakthroughs. Traditional views suggested this ratio was as high as 1000:1 or even higher, but according to international public literature in 2024 and the ETSI/QSC 2024 Singapore annual meeting report, thanks to the leap in quantum error correction coding technology, the physical-to-logical qubit conversion ratio has been significantly optimized to approximately 7.8:1. This critical data update means that the engineering difficulty and hardware scale required to build a cryptographically relevant quantum computer (CRQC) have dropped by two orders of magnitude compared to previous expectations, and the threat is approaching much faster than anticipated.

2.1.2 Strategic Implications: The Future of RSA and ECC

RSA Encryption Algorithm: Breaking a 1024-bit RSA key requires approximately 2000 to 2500 logical qubits and is expected to be achieved in 2030. The currently widely used 2048-bit RSA key requires 4,000 to 5,000 logical qubits and is expected to be broken in 2040. Recent research has further refined these estimates, for example, some studies suggest that RSA-2048 can be challenged using about 372 physical qubits and a circuit depth of several thousands.

ECC Encryption Algorithm: Breaking a 160-bit ECC key (equivalent to 1024-bit RSA) requires approximately 1500 logical qubits and is expected to be achieved in 2028. Breaking a 256-bit ECC key (equivalent to 2048-bit RSA) requires approximately 4000 logical qubits and is expected to be achieved in 2035. A detailed resource estimation for binary elliptic curves suggests that breaking ECC with n=233 (close to 256-bit security level) requires about 3035 logical qubits and a run time of about 7.9 minutes on

a superconducting quantum computer with a 11μs clock cycle.

2.1.3 Technological Synergy: Catalysts Further Compressing the Timeline

According to the latest strategic report released by ATIS (Alliance for Telecommunications Industry Solutions)[11] in 2025, and the groundbreaking research by Gouzien (2023) and Gidney (2025), the resource threshold required to break mainstream public-key cryptography is being significantly lowered. The following table shows the resource requirements and time predictions based on these latest hardware architecture innovations.

Table 2.2: Threat Acceleration Under Technological Breakthroughs (Cat Qubits)

Encryption Algorithm	Key Length	Traditional Estimated Physical Qubits	Physical Qubits in Latest Architecture (Based on Cat Qubits)	Projected Timeline (Aggressive/Hybrid Attack)
RSA	2048-bit	~20 million	< 1 million (Based on surface code optimization)	Early 2030s
ECC	256-bit	~10 million - 30 million	~126,000 (Based on cat qubits)	Late 2020s (Hybrid Attack)

Traditional estimates typically suggest that millions or even tens of millions of physical qubits are needed to build a fault-tolerant quantum

computer (CRQC) with breaking capability. However, the ATIS report[11] points out that this barrier is collapsing through the introduction of "Cat Qubits" and advanced "Surface Codes" technology.

Extreme Speed Breaking of ECC: According to the latest analysis by Elie Gouzien et al., a fault-tolerant architecture based on Cat Qubits only requires approximately 126,000 physical qubits to break 256-bit ECC encryption in 9 hours. This represents an order-of-magnitude reduction compared to the millions of qubits required by traditional architectures.

Lowering the RSA Threshold: C. Gidney's (2025) research indicates that by optimizing surface codes[10], the resources required to break 2048-bit RSA integers may drop below 1 million noisy physical qubits.

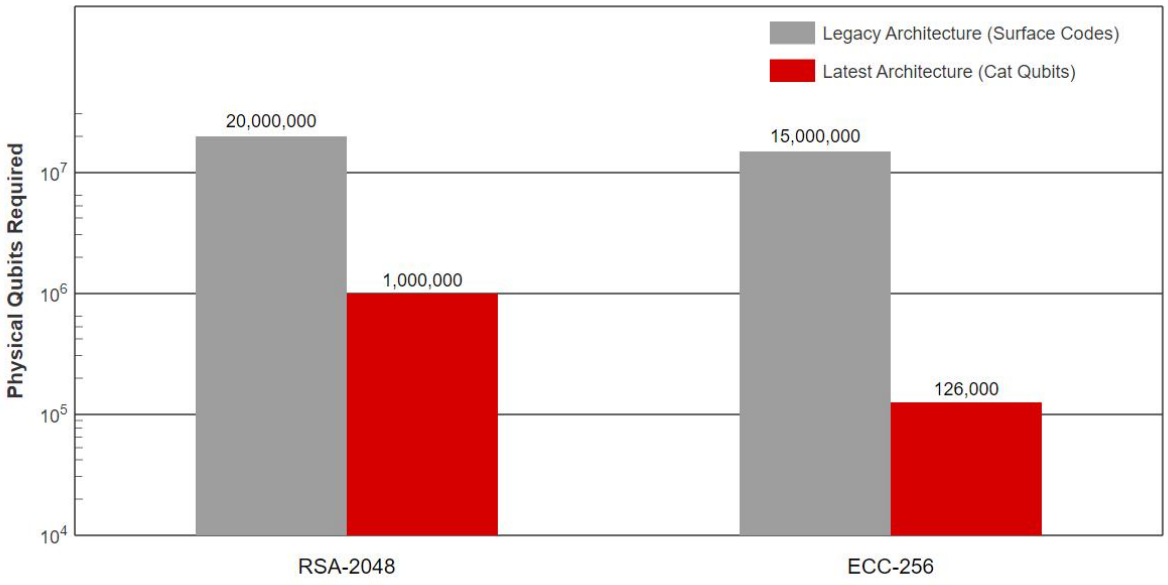


Figure 2.2: Threat Acceleration via Technical Breakthroughs – Comparison of Cracking Resources

This means that with improved hardware fidelity and the

combination of these new error correction architectures, the timeline for the quantum threat could be compressed by 5-10 years. While conservative estimates still point to 2035, an aggressive yet reasonable prediction is: hybrid attacks targeting some encryption systems may emerge in the late 2020s, and full breaking capability could be available in the early 2030s.

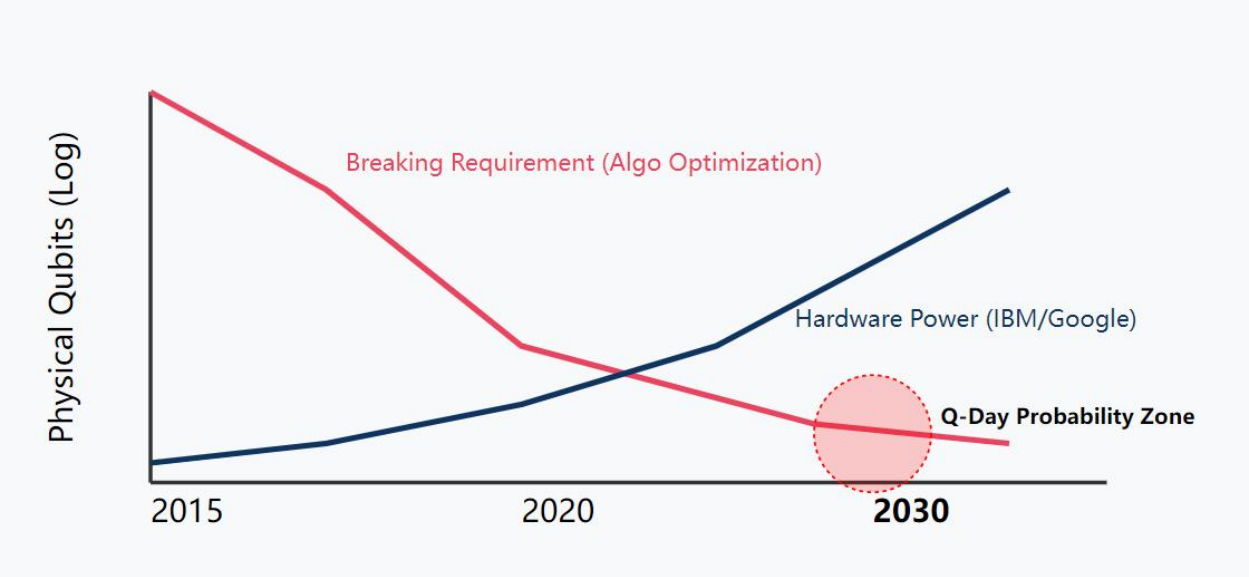


Figure 2.3: The Collapse of the Cracking Threshold — Evolution Trends in Quantum Computing Power Demand

2.2 The Evolving Threat Landscape: Beyond Shor's Algorithm

In addressing the challenges of post-quantum migration, organizations are facing a "two-front war." We are not confronting a single threat, but a dual-threat environment comprising future quantum risk and current classical risk.

The well-known "quantum threat," namely the disruption of existing public-key cryptography (RSA/ECC) by Shor's algorithm[7], is a long-term,

strategic risk. However, an equally powerful and more direct "classical threat" is continuously evolving, utilizing modern computational techniques, particularly AI-driven analysis tools, to shift the attack target from the mathematical foundation of algorithms to the concrete engineering implementation of cryptography. Symbolic AI tools like CodeQL and machine learning tools like CryptoGuard can automate and scale the discovery of subtle flaws in cryptographic implementations, such as hardcoded keys or insecure API misuse. These flaws are sufficient to completely bypass all mathematical security guarantees provided by the algorithm.

The "Harvest Now, Decrypt Later" (HNDL) attack model is the bridge connecting these two threats. Attackers can now use existing technology to massively intercept and store encrypted data, waiting for the advent of future quantum computers for decryption. This model fundamentally changes the nature of migration. For any data requiring long-term confidentiality—such as mortgage contracts that need to be saved for decades, core corporate intellectual property, or personal health records—the security vulnerability essentially already exists. PQC migration is therefore no longer a forward-looking investment to protect future data, but an immediate measure to remedy the risk of past and present data breaches.

The recent success of the XJTLU PQC-X Lab team in breaking the 200-dimensional Darmstadt Shortest Vector Problem (SVP) challenge[35] and solving the Kyber-208 instance from the Bochum Challenges is a clear example of the continuous escalation of classical threats. This achievement was led by Professor Jintai Ding of the PQC-X Lab at Xi'an Jiaotong-Liverpool University, a core member of this alliance. The security of the most promising family of PQC algorithms—lattice-based cryptography—is built on the assumed difficulty of solving problems like the high-dimensional SVP. This accomplishment not only provides a crucial real-world benchmark for the security of PQC systems but is also

powerful evidence of the "iterative" nature of the PQC threat. Along with the team's research revealing weaknesses in some NIST candidate schemes (such as GeMSS and LUOV), it collectively warns us to be wary of the notion that PQC migration is a "once and for all" solution. Even the PQC algorithms themselves, which form the core of the defense, are becoming targets for continuously evolving classical attack methods. This iterative threat dictates that our defense system cannot be a one-time replacement but must be a dynamic process capable of continuous learning, adaptation, and evolution—this is the core philosophy of the migration engine.

2.3 Global Response: Policy and Standard Convergence

Post-quantum migration is not driven by a single technology, but is a collaborative transformation globally propelled by government policies, international standards, and industry consensus. This global convergence sets a clear direction and an unignorable timeline for PQC migration, elevating it from a technical issue to a global strategic task and providing a strong external thrust to the running engine.

The PQC standardization project initiated by the U.S. National Institute of Standards and Technology (NIST) since 2016 has become the "North Star" for global PQC technology development. In August 2024, NIST formally released the first batch of PQC standards, including ML-KEM [12] (Kyber) as the general key encapsulation mechanism and ML-DSA [13] (Dilithium) and SLH-DSA [14] (SPHINCS+) as the general digital signature standards. Of greater strategic significance is NIST's choice of the code-based HQC as a backup standard for ML-KEM. The purpose of this is to provide "algorithmic diversity"[15] to counter the potential risk of future lattice-based mathematical problems being broken. This action profoundly demonstrates a well-thought-out strategy for cryptographic security and fundamentally requires enterprises to

possess cryptographic agility in their architectural design[23].

Following closely in NIST's footsteps, governments in major global economies have rapidly elevated PQC migration to the level of national strategy and policy directives.

United States: The White House's National Security Memorandum 10 [20] (NSM-10) and related Executive Orders set a clear timeline for the federal government: traditional public-key algorithms such as RSA-2048 will be "deprecated" by 2030 and completely "prohibited" by 2035.

European Union: The Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography [24] requires critical infrastructure to complete the migration to PQC by the end of 2030.

China: The National Cryptography Industry Standardization Technical Committee (CSTC) and the Commercial Cryptography Standardization Research Institute (ICCS) have launched a global PQC algorithm solicitation event, aiming to accelerate the promotion and construction of an independent PQC standard system.

This policy-driven certainty is profoundly affecting the technological strategies and investment decisions of global enterprises. Concurrently, industry organizations like the Post-Quantum Cryptography Alliance (PQCA) and open-source projects such as Open Quantum Safe (OQS) are actively building an ecosystem to support the migration and collectively lower the implementation threshold[36]. The convergence of global policies, the clarity of government directives, and the synergy of the industry ecosystem collectively form a powerful force, driving the wave of PQC migration. It is no longer a question of whether migration is necessary, but how to complete it in the most strategic and cost-effective manner within the established time frame.

Table 2.3: Global PQC Policy and Standardization Milestones

Region /Institution	Key Documents/Events	Date	Key Milestones/Requirements	Implications for Global Organizations
USA (NIST)	Release of First Batch of PQC Standards (FIPS 203, 204, 205)	August 2024	Formally established ML-KEM, ML-DSA, and SLH-DSA.	Provided stable, vetted algorithms for product development.
USA (NIST)	HQC Selected as KEM Backup	March 2025	Provided algorithmic diversity[15] to address potential risks of breaking lattice-based cryptography.	Reinforced the requirement for cryptographic agility.
USA (Government)	NIST IR 8547 / Executive Order Revision[22]	Nov. 2024 / June 2025	Set deadlines to deprecate RSA/ECC by 2030 and	Established a non-negotiable hard timeline for migration.

			disallow them by 2035.	
European Union (EU)	Coordinated Implementation Roadmap	June 2025	Member states to launch migration by 2026; critical infrastructure to complete by 2030[24].	Created a unified European market demand and compliance environment.
China (ICCS/ CSTC)	Global PQC Algorithm Solicitation	February 2025	Initiated an independent national standardization process[27].	Provides an alternative security option distinct from the West with independent intellectual property, contributing "Chinese wisdom" to global digital security governance.

Chapter 3

Quantum-Safe Migration Strategic Engine - A Strategic Framework

Chapter 3: Quantum-Safe Migration Strategic Engine - A Strategic Framework

This section will detail the "Quantum-Safe Migration Strategic Engine." This is not a static flowchart but a dynamic, cyclically accelerating kinetic system. Imagine a precision turbo engine: "Crypto-Agility"[23] is its solid foundation, supporting all operations; "Strategic Foresight" is the igniter, starting the first wave of energy; "Technology Stack" is the power train, ensuring continuous output; "Simulation and Validation" is the turbocharger, multiplying efficiency; and "Governance Evolution" is the ECU (Engine Control Unit), ensuring the engine runs smoothly under the complex road conditions of dual threats.

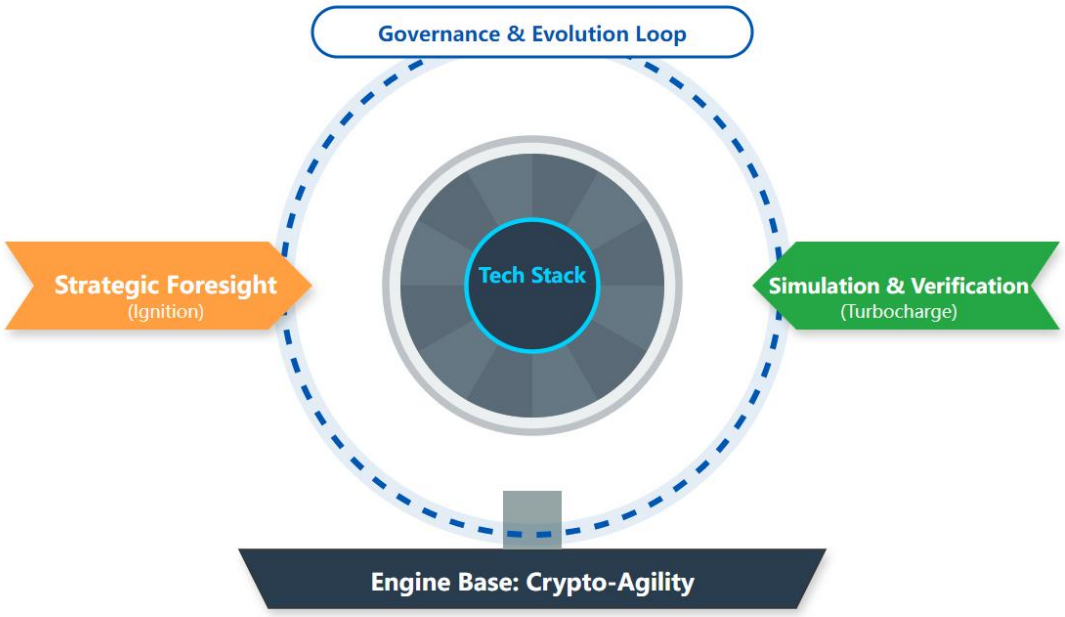


Figure 3.1: Quantum-Safe Migration Strategic Engine Framework

Figure 3.1 illustrates the Quantum-Safe Migration Strategic Engine, a dynamic, self-reinforcing lifecycle model that establishes Crypto-Agility as its unwavering foundation. Driven by Strategic Foresight for initial ignition and powered by a comprehensive Post-Quantum Cryptography Technology Stack, the engine utilizes Simulation and Verification as a turbocharger to multiply implementation efficiency, all while operating within a continuous Governance and Evolution Loop to ensure long-term organizational resilience against shifting quantum and classical threats.

3.1 Engine Foundation: Core Principles of Crypto-Agility (Heterogeneous Integration and Dynamic Restructuring)

If the migration engine needs continuous operation, then Crypto-Agility [23] is the unwavering foundation supporting its operation. It is not a simple technical feature but a strategic architectural assurance for dealing with future uncertainty. The strategic importance of this principle has been authoritatively recognized by the National Institute of Standards and Technology (NIST) of the United States [23]. In its pioneering white paper NIST CSWP 39, "Considerations for Achieving Cryptographic Agility: Strategies and Practices," the team of experts, including Lily Chen and Dustin Moody, laid the official groundwork for this concept.

According to NIST's formal definition, "Crypto-agility [23] is the capability required to replace and adjust cryptographic algorithms in protocols, applications, software, hardware, and infrastructure to achieve resilience without disrupting the operation of running systems." This means that information systems must be able to flexibly and efficiently switch or update the cryptographic algorithms, protocols, and related parameters they use, without major redesigns or service interruptions.

However, achieving crypto-agility [23] is not easy. NIST explicitly points out several severe challenges in its white paper, such as: the

performance overhead caused by the generally larger key and signature sizes of PQC algorithms, the potential for downgrade attacks during algorithm negotiation, hard-coded algorithms in difficult-to-update legacy systems and long-lifecycle devices, and the difficulty of phasing out old algorithms while maintaining interoperability.

Successful migration must, at the engineering level, embed crypto-agility [23] in the system's protocol construction and architectural design, and the technical solutions proposed in this white paper are a direct response to the challenges identified by NIST.

Table 3.1: Achieving Crypto-Agility: NIST Challenges and Responses

Key Cryptographic Agility Challenges Identified in NIST CSWP 39	Mitigation Strategies in the Engine Framework	Specific Technical Implementation
Downgrade attacks during algorithm negotiation	Core Principle: Crypto-Agile Design	Adopt algorithm negotiation protocols protected by strong integrity to prevent attackers from forcing the system to use weak algorithms.
Performance overhead of PQC (Large	Tech Stack: Software-Hardware Co-design	Deploy PQC hardware accelerator cards to handle high-throughput scenarios;

keys/signatures)		provide lightweight software libraries for resource-constrained devices.
Interoperability in heterogeneous environments	Core Principle: Crypto-Agile Design	Design and deploy heterogeneous Authenticated Key Exchange (AKE) protocols, allowing systems with different cryptographic capabilities to communicate securely.
Hard-coded algorithms in legacy systems	Execution Engine: Phased Evolution; Core Principle: Crypto-Agile Design	For systems that cannot be retrofitted, provide "encapsulation" protection through PQC-enabled security gateways; use cryptographic APIs instead of direct implementation.
Complexity of PKI migration	Core Principle: Crypto-Agile Design	Adopt Hybrid X.509 certificates, enabling a single certificate to be verified by both new and legacy systems, achieving a

smooth transition.

Successful migration must, at the engineering level, embed crypto-agility [23] in the system's protocol construction and architectural design. This requires a series of advanced technical implementations as support, transforming abstract agility principles into specific, operable engineering practices:

3.1.1 Protocol Interoperability Engineering in Heterogeneous Environments

In the vast and complex ecosystem of an enterprise, PQC migration progress will inevitably differ across institutions and systems, leading to a long-term "heterogeneous environment" with inconsistent cryptographic infrastructure. To resolve this critical pain point, heterogeneous Authenticated Key Exchange (AKE) protocols must be designed and deployed. The core goal of this protocol is to allow entities holding different types of long-term keys. for example, one party has migrated to Kyber [12] based on Key Encapsulation Mechanism KEM, while the counterparty is still using Dilithium [13] based on Digital Signature to complete secure identity authentication and key negotiation. This allows organizations to migrate in phases and batches without mandating synchronous upgrades for all counterparties, making it a key protocol layer innovation for achieving crypto-agility [23].

3.1.2 Hybrid Implementation Mode as a Transition Bridge

Before fully transitioning to a purely PQC environment, the Hybrid Cryptography Mode is a widely recommended pragmatic strategy. It combines a fully validated classic algorithm (such as ECC) with a new PQC algorithm (such as Kyber [12]), the security of which is based on the premise that the entire connection is secure as long as at least one of the

two algorithms is secure. This includes two main technical paths:

Separable Hybrid Mode: Classic and PQC cryptographic computations run independently and in parallel. For example, simultaneously executing one ECDHE and one ML-KEM [12] key exchange during a TLS handshake. This mode is relatively simple to implement and allows for flexible enabling of the PQC portion based on policy.

Inseparable Hybrid Mode: Classic and PQC cryptography are deeply integrated. For example, through a nested encryption mechanism, the client first encrypts with a classic algorithm, and then uses a PQC algorithm for secondary encryption of the intermediate ciphertext. Although this mode is more complex to implement, it can effectively reduce communication overhead.

To support these complex hybrid modes, the protocol itself also needs deep optimization. For instance, an optimized TLS handshake process can be designed where the server first sends its PQC public key, thereby reducing one round-trip interaction and significantly improving protocol efficiency. The "LK Quantum Shield" developed by the LK Quantum team is a post-quantum agile framework supporting hybrid digital signatures, key encapsulation, and key exchange, representing a typical practice for smooth transition to the hybrid mode.

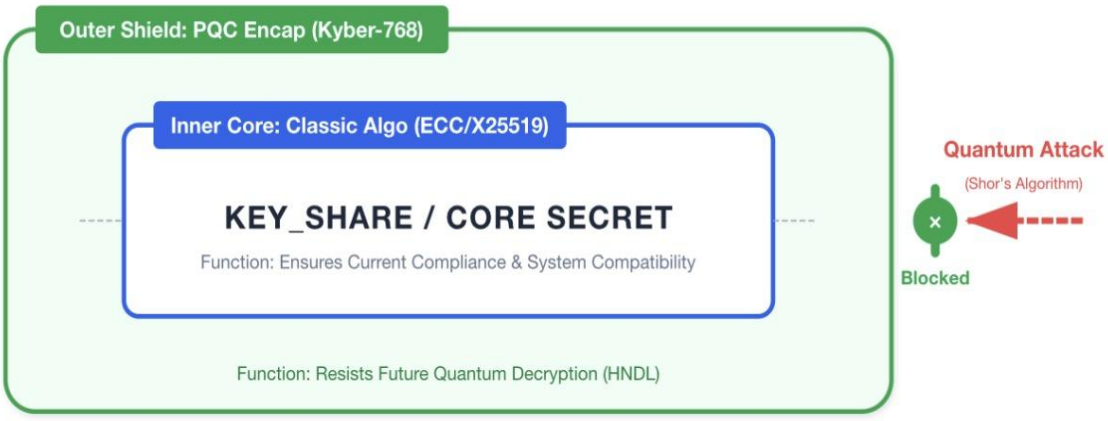


Figure 3.2: Hybrid Protocol Stack Architecture — Double Safe Design

3.1.3 Agile Public Key Infrastructure (PKI) Management

PQC poses significant challenges to existing Public Key Infrastructure (PKI), the most prominent of which is that PQC public keys and signature sizes are much larger than traditional algorithms, leading to a significant increase in digital certificate volume. For a smooth transition, an effective technical solution is to design Hybrid X.509 Certificates. This scheme stores the PQC public key and corresponding signature value in the certificate's extension fields. In this way, upgraded systems can extract information from the extension fields for PQC verification, while traditional systems can ignore the extension fields and continue to use classic algorithms for verification. This design enables a single certificate system to simultaneously meet the verification needs of both new and old systems, making it a key technology for agile PKI migration.

Crypto-agility [23] is the foundation for the stable ignition of the entire engine. An agile architecture ensures that subsequent technology selection, deployment verification, and long-term governance are all flexible, thereby reducing friction and costs arising from future changes in standards or threats.

3.2 Gaining Initial Momentum: Strategic Foresight and Risk Intelligence

Completing the ignition and startup of the organization's 'Quantum-Safe Migration Strategic Engine.' This power comes from intelligence-based strategic foresight and a precise grasp of the risk landscape. It is worth emphasizing that many core activities in this phase can be considered "no-regret moves." This strategic concept, originating

from PQC migration manuals[25] released by organizations like TNO, refers to actions that bring significant security value to an organization regardless of when—or even if—the quantum threat arrives.

It is a crucial strategic perspective to view PQC migration as an opportunity to enhance the organization's overall "Cryptographic Maturity," rather than just a simple technical upgrade. Cryptographic maturity means the organization has a comprehensive understanding of its cryptographic usage, the ability to assess related risks, and has formulated strategies consistent with regulations and business objectives. From this perspective, the initial steps of launching the migration are themselves a comprehensive upgrade of security governance.

Under this strategic framework, China's National Key R&D Program "Top-Level Design for Quantum-Resistant Migration Architecture" (Project No.: 2023YFC3305501, or "Project 055") proposed a migration reference architecture specifically for key information infrastructure such as the banking sector. This architecture profoundly recognizes the stringent requirements of the financial industry for high trustworthiness, high stability, and interoperability. It not only maintains strategic consistency with the latest "Cybersecurity Framework 2.0" (CSF 2.0) released by the US NIST in its top-level design but also innovatively introduces the "Science of Crypto-Agility." The project team explicitly proposes that migration in the banking sector should not stop at algorithm replacement but must build a comprehensive governance system encompassing "Implementation Agility, Compliance Agility, and Platform Agility." By establishing a precise inventory of cryptographic assets, formulating phased migration plans, and implementing strict interoperability testing, Project 055 aims to provide a risk-controllable evolutionary path for complex financial legacy systems, ensuring the continuity and stability of existing financial operations while addressing future quantum threats. This is the best example of translating "Strategic Foresight" into

"Engineering Practice."

3.2.1 From Inventory to Intelligence: Data-Driven Crypto Asset Discovery

Before action, the organization's current encryption status must first be fully understood. This is the most crucial "no-regret move" in PQC migration—Cryptographic Asset Management. Establishing a comprehensive inventory of cryptographic assets is not only a prerequisite for PQC migration but also the foundation of modern cyber risk management. It helps organizations respond quickly to any cryptographic vulnerability (whether quantum-related or not), thereby enhancing overall security resilience.

A data-driven agile migration framework provides core guidance for this, going beyond simple asset counting to emphasize a full-spectrum analysis centered on "data":

Data Flow as the Main Thread: Track the complete lifecycle of sensitive data within the system, mapping out a dynamic encryption map closely associated with the business.

Data Type as the Criterion: Classify data based on its Confidentiality Lifespan. Long-term contracts that need to be preserved for decades face a fundamentally different level of "Harvest Now, Decrypt Later" (HNDL) risk than session data that only requires short-term confidentiality. This classification method directly provides decision support for prioritizing migration work.

Data Compatibility as the Yardstick: Evaluate the compatibility of new PQC solutions with existing data processing paths, measuring the "agility" of different migration schemes.

Through this data-driven approach, organizations can build a far more profound and insightful view of crypto assets than a static inventory, laying a solid intelligence foundation for subsequent risk assessment and strategic planning. This process has also spurred the consulting, risk

assessment, and cryptographic asset inventory management service markets, with market research institutions widely predicting explosive growth, with the Compound Annual Growth Rate (CAGR) expected to be in the high range of 37% to 47% by 2034.

3.2.2 Comprehensive Risk Assessment: Visualizing Systemic Risk

After grasping the internal crypto asset situation, it is necessary to combine a comprehensive analysis of external threats to build a complete risk landscape. This requires a theoretical framework covering the entire chain of "Risk Identification - Assessment and Early Warning - Migration Supervision."

Firstly, at the risk identification level, systematically sort out the quantum vulnerabilities faced by information systems at the algorithm, protocol, and business layers, and draw up a detailed Risk Point Inventory.

Secondly, at the risk assessment level, use a Risk Matrix to rate different risks by combining the two dimensions of risk probability and impact.

More crucially, the risk transmission mechanism must be modeled. The impact of a quantum attack is not isolated; it can trigger a chain of failures through the inherent connections between systems. By drawing a Risk Contagion Map, the transmission path of risk can be visually demonstrated. For example, an attack against an external website might not only lead to data leakage in that system but also spread the risk to the entire enterprise ecosystem due to data interaction. This map is a key tool for transforming and understanding the HNDL threat, converting a potential, delayed threat into a currently visible and analyzable systemic risk, thereby greatly enhancing decision-makers' awareness of the migration urgency. This also means that the system's migration priority depends not only on the confidentiality lifespan of the data it carries but

also on its "connectivity" in the Risk Contagion Map.

This preliminary assessment provides the ignition energy for the engine, and it will be continuously optimized as the engine runs/accelerates through real-world data collected in the subsequent "Execution and Validation" phase.

3.3 Building Momentum: Post-Quantum Cryptography Technology Stack

Key Point:

An organization needs a diverse portfolio of PQC tools, not a single solution. This chapter explains how investing in the right mix of hardware and software will ensure the organization's business maintains excellent performance while staying secure.

To enable the engine to output continuously strong power, a solid, efficient, and comprehensive technology stack must be built. This technology stack gives the engine its "core power train," ensuring that the migration process is both secure and reliable, and can run smoothly under the stringent performance requirements of core business operations. This is the embodiment of the "Technological Diversity Fission" dimension in the market's three-dimensional restructuring.

3.3.1 Algorithm Portfolio: A Cryptographic Toolbox Customized for General Scenarios

No single PQC algorithm is a "one-size-fits-all" solution. The best choice always depends on the specific application environment and security requirements. Organizations need a carefully screened and optimized Algorithm Portfolio to cope with their diverse business scenarios. PQC development has shown a "blooming of a hundred flowers" situation, with algorithms based on various mathematical problems such as lattices, codes, hashes, multivariate, and isogenies

coexisting and developing.

Lattice-Based Cryptography: Represented by NIST-standardized ML-KEM [12] (Kyber) and ML-DSA [13] (Dilithium), this is the most mature and performance-balanced technical route currently, dominating the first batch of NIST standards, and is suitable for general core scenarios such as establishing secure communication channels.

Hash-Based Signatures: Represented by NIST-standardized SLH-DSA [14] (SPHINCS+), its security relies solely on the strength of the underlying hash function, making it an extremely conservative and reliable choice. It is suitable for scenarios with the highest security requirements and where performance overhead can be tolerated, such as issuing certificates for Root Certificate Authorities (Root CA) or signing firmware updates.

Multivariate Cryptography: Represented by UOV, its outstanding advantage is extremely fast signature and verification speeds, making it particularly suitable for scenarios requiring the processing of massive signature verifications, such as large-scale IoT device authentication or high-frequency business systems.

Code-Based Cryptography: Represented by HQC, it serves as a backup to lattice cryptography, providing algorithmic diversity, and is suitable for scenarios where encryption speed is crucial.

Table 3.2: PQC Algorithm Portfolio Strategy for Enterprise Scenarios

Algorithm Family	Standardized Examples	Relative Key / Signature Size	Relative Performance	Security Basis	Main Application Scenarios

Lattice-based Cryptography	ML-KEM (Kyber), ML-DSA (Dilithium)	Moderate	Good / Excellent	Hardness of solving problems like the Shortest Vector Problem (SVP) in high-dimensional lattices.	General Core Scenarios: Establishment of TLS/IPsec secure channels, encryption and signing of business data, and cloud service data protection.
Hash-based Signatures	SLH-DSA (SPHINCS+)	Very Large (Signature)	Slow (Signing)	Security of the underlying cryptographic hash functions (e.g.,	High-Assurance & Long-Lifecycle Scenarios: Root CA certificate issuance, system firmware/softw

				SHA-256).	are update signing, and archival signing of long-term contracts and legal documents.
Multivariate Cryptography	UOV	Large Public Key, Small/Medium Signature	Extremely Fast Verification	Hardness of solving systems of multivariate quadratic polynomial equations.	High-Frequency Verification Scenarios: Identity authentication for large-scale devices (e.g., POS terminals), signature verification in high-frequency business systems, and

					internal risk control systems.
Code-based Cryptography	HQC	Large (Public Key)	Fast (Encryption)	Hardness of decoding general linear codes.	KEM Backup & Algorithm Diversity: As a backup to lattice-based schemes, suitable for scenarios where encryption speed is critical.

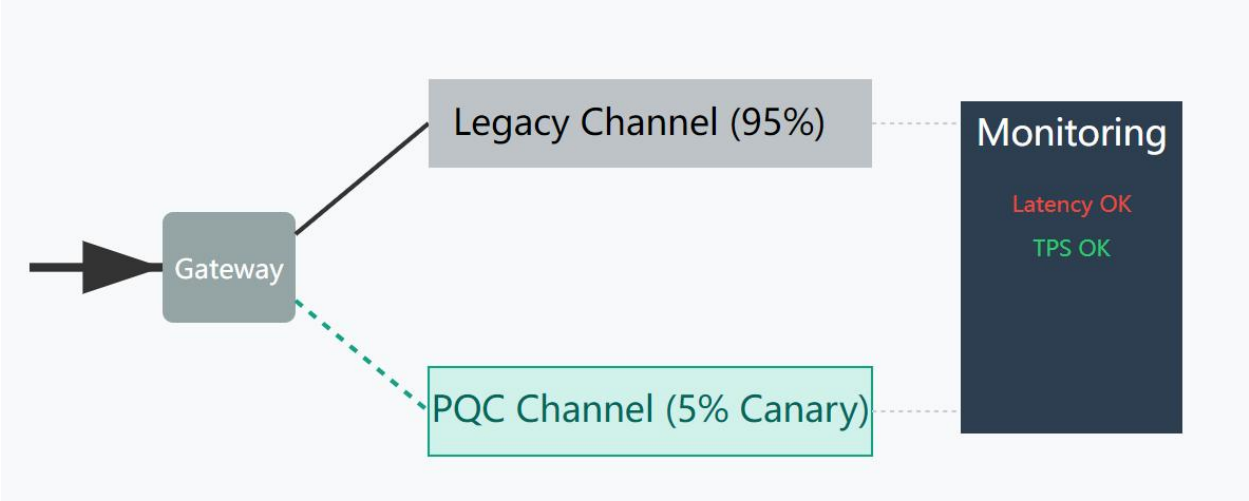


Figure 3.3: Risk-Controlled Gray Release Mechanism

3.3.2 Implementation Engine: Software/Hardware Co-design

Given the general performance overhead of PQC algorithms (greater computation, larger key and signature sizes), algorithm theory alone is far from enough. A powerful implementation engine must be built through software/hardware co-design to ensure PQC can run efficiently under the system's high load. This implementation strategy must be differentiated.

Hardware Acceleration Layer: For backend core business systems and other scenarios requiring the handling of massive concurrent requests, hardware acceleration is the essential path. This has spurred targeted hardware innovations such as quantum-resistant chips, coprocessors, and optimized implementations on ASIC/FPGA. This includes Quantum-Resistant Server HSMs (Hardware Security Modules) tailored for data centers.

Optimized Software Layer: For general computing environments on the server side and resource-constrained environments on the client side,

highly optimized software implementations must be provided.

CPU Platform Software Module: For mainstream X86 server platforms, through technologies like cache optimization and automatic vectorization (utilization of SIMD instruction sets), superior performance is achieved at the pure software level.

Mobile SDK: For mobile devices with limited computing and memory resources, dedicated lightweight SDKs must be developed. By deeply optimizing core computing modules using NEON assembly instructions, PQC SDKs suitable for Android and iOS platforms can be successfully developed, providing critical technical support for the secure migration of mobile applications.

A solid technology stack forms the strategic engine's core 'power train,' ensuring continuous power output and system stability. These technological choices will be tested in the 'Execution and Validation' phase, and their performance data will be fed back to provide a basis for future engine performance tuning.

3.4 Accelerating Engine: Simulation and Validation Module

Key Point:

Any strategic plan must be tested in the real world. The validation platform and toolset described in this chapter are crucial for ensuring the smooth implementation of the PQC migration plan, avoiding business interruptions, and controlling implementation risks.

Having strategic foresight and a solid technology stack, the next step is to put the migration engine into practice, building and accelerating its momentum in a real business environment. The core of this phase is "Simulation and Validation," which, through a high-fidelity validation environment and a complete toolset, transforms theoretical planning into measurable, controllable, and iterative deployment actions, directly addressing the most severe real-world challenges during migration.

3.4.1 Quantum-Ready Toolkit

To execute migration efficiently and securely, a complete "Quantum-Ready Toolkit" needs to be developed, providing organizations with comprehensive support from algorithm libraries, protocol libraries to evaluation software. This toolset is the "arsenal" for the execution phase, ensuring that every link of the migration has precise tools available, including fully validated and performance-optimized quantum-resistant cryptographic adaptation algorithm libraries and protocol libraries, certificate management tools capable of issuing Hybrid X.509 certificates, and evaluation software for compliance and security checks.

3.4.2 High-Fidelity Validation Environment: Migration Test Platform

Theory and lab tests are far from sufficient to cope with business complexity. PQC solutions must undergo rigorous validation under conditions as close to the real environment as possible before being put into production. To this end, a core validation facility needs to be built—the Quantum-Resistant Cryptography Migration Test Platform. This platform is not just a test field but a "high-fidelity simulator" for rehearsing and optimizing migration strategies and accumulating practical experience.

The platform's core capabilities are manifested in two aspects:

Engineering Validation: The platform can simulate typical industry business scenarios (such as mobile applications, Web platforms), inject real business messages, and complete end-to-end full-link testing. In this way, the actual impact of PQC solutions on business performance (such as latency, throughput) can be accurately and quantitatively evaluated, and potential performance bottlenecks and compatibility issues can be

identified.

Gray-Scale Evolution: The platform has a built-in powerful policy orchestration and version governance engine. Through policy scheduling, the platform can flexibly combine traditional cryptography and PQC algorithms, enabling dual-track parallel operation, and directing different proportions of traffic to the new solution as needed. The version governance mechanism supports phased A/B testing and Canary Releases of algorithms and protocols, and has Risk Rollback capabilities that are automatically triggered upon anomaly detection. This transforms the migration process from a high-risk "rip-and-replace" switch to a dynamic evolution closed loop where risk is controllable, the process is observable, and the result is measurable.

Table 3.3: Migration Challenges and Engine Framework Response Strategy Matrix

Key Migration Challenge	Challenge Description	Response Component/Strategy in Engine Framework	Specific Technical Examples
Performance Overhead & Resource Constraints	The computational complexity and larger key/signature	Technology Stack: Implementation Engine	Hardware Acceleration: Deploying post-quantum Server HSMs (Hardware Security Modules) achieving encryption

	sizes of PQC algorithms put pressure on system performance and resource-constrained devices.		performance of 210,000 ops/sec. Software Optimization: Providing lightweight SDKs with NEON assembly optimization for mobile applications.
Supply Chain Complexity & Dependency Risks	Enterprise IT systems consist of numerous third-party software and hardware; any component lacking PQC support can become a migration bottleneck.	Core Principle: Crypto-Agility Design	Protocol Agility: Adopting heterogeneous authenticated key exchange protocols to allow secure communication with third-party systems that have not yet been upgraded. Architectural Agility: Plug-in based algorithm integration frameworks supporting

			rapid replacement of cryptographic libraries.
Legacy System Integration	Massive amounts of "Shadow Cryptography" are deeply embedded in legacy systems that cannot be directly upgraded, making discovery and remediation extremely difficult.	Execution Engine: Phased EvolutionCore Principle: Crypto-Agility Design	Risk Isolation: For systems that cannot be remediated, using PQC-enabled security gateways for "encapsulated" protection. Compatibility Design: Using hybrid X.509 certificates to ensure certificates issued by new systems can still be verified by legacy systems.

Implementation Risks & Migration Failures	Improper PQC implementation may introduce new security vulnerabilities, potentially reducing rather than enhancing security.	Execution Engine: High-Fidelity Verification	Full-Link Testing: Injecting real business traffic into the migration pilot platform for end-to-end functional, performance, and security verification. Automated Rollback: Leveraging the platform's phased evolution capabilities to automatically roll back to stable traditional cryptographic schemes upon detecting anomalies.

Crucially, the migration test platform is not just the endpoint of execution and validation; it is the key to the engine achieving 'intelligent supercharging.' All data generated during the validation process—performance indicators, compatibility reports, failure logs—is extremely valuable new intelligence. This intelligence is fed back in real-time to the "Strategic Foresight" phase of the engine for dynamic

correction of risk assessments, adjustment of migration priorities, and optimization of technical solutions. It is this closed loop formed by "Execution-Validation-Feedback" that transforms a linear migration process into a spiraling cycle of continuous learning and optimization. With each completed cycle, the engine accumulates more experience and data, making subsequent power output more efficient.

3.5 Sustaining Momentum: Governance and Dynamic Evolution

Once the Quantum-Safe Migration Strategic Engine is started, its goal is not to reach a static "completion" state but to enter a virtuous cycle of continuous operation, adaptation, and evolution. To sustain the engine's power and ensure its long-term effectiveness, a robust governance framework must be established. This governance loop is the engine's ECU (Electronic Control Unit), ensuring that the engine's operation remains synchronized with organizational strategy, the external environment, and emerging threats.

3.5.1 Establishing a Normalized Governance Structure

The long-term nature of PQC migration requires it to be transformed from a temporary project into a normalized component of enterprise risk management and technology governance. This necessitates the establishment of a clear, multi-level governance structure to ensure continuous oversight, decision-making, and resource investment. A model for reference includes a Steering Committee composed of senior management, an Expert Committee composed of internal and external experts, and a Project Working Group responsible for daily execution. Importantly, this governance model is designed to seamlessly interface and integrate with the enterprise's existing Enterprise Risk Management (ERM) framework (such as ISO 31000 or COSO), incorporating PQC risk

into the overall enterprise risk management view, thus communicating using the language and structure already understood and trusted by high-level leadership.

3.5.2 Creating a Continuous Intelligence and Feedback Loop

The core of the governance cycle is the establishment of a formal, continuous intelligence feedback mechanism to ensure the engine can dynamically adjust based on the latest internal and external information.

Internal Feedback: Monitoring data collected from the migration test platform and the production environment must be institutionalized and fed back to the "Strategic Foresight" team. This first-hand data is the most valuable input for correcting risk models and optimizing technical solutions.

External Intelligence: A dedicated team or role must be designated to establish a quantum threat intelligence and monitoring network, responsible for continuously tracking global PQC development dynamics, including the latest progress from international standards organizations such as NIST, IETF, and China CSTC, as well as new cryptanalysis results. This continuous intelligence is crucial for managing interoperability risks, as the coexistence of NIST standards and China's national PQC standards may lead to the divergence of technical routes.

3.5.3 Investing in the "Human Firewall"

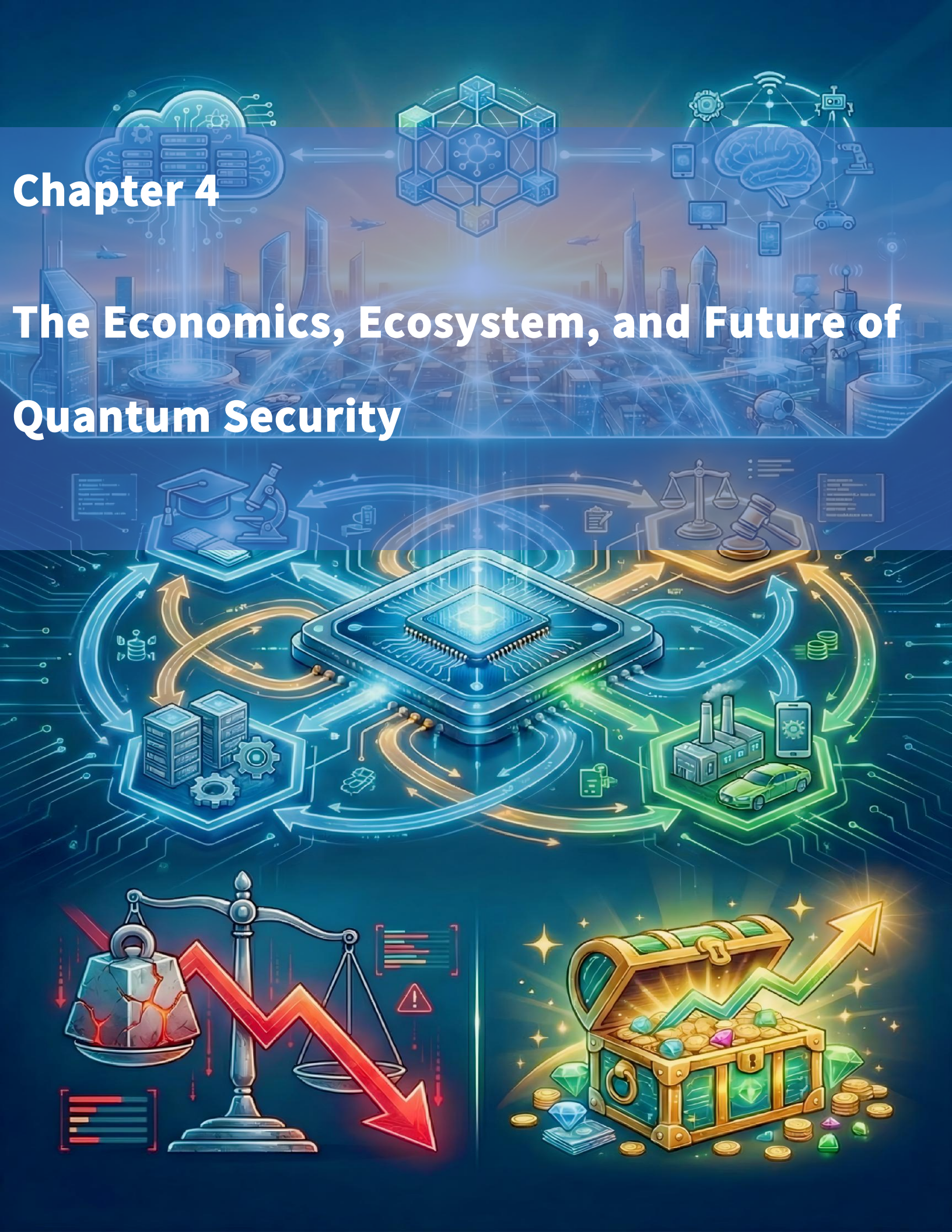
Technology and processes ultimately need to be executed by people. Advanced algorithms and platforms will still fail in PQC migration if they lack professionals with the corresponding knowledge and skills to plan, implement, and maintain them. Currently, professional talent proficient in PQC algorithms, migration implementation, and security assessment is relatively scarce, constituting a human resource bottleneck. Therefore, investment in talent is the most fundamental guarantee for sustaining the engine's power. Successful PQC experts need to possess interdisciplinary

composite capabilities, including deep cryptographic theory, excellent software engineering skills, system architecture and hardware knowledge, and risk management and strategic planning capabilities. Organizations should establish internal training programs and systematically build talent pipelines through methods such as establishing joint laboratories with universities and research institutions, to bridge the talent gap.

A strong governance cycle ensures the engine does not stall when the project ends. By providing stable energy and the correct direction for the engine's long-term operation, it acts as a dynamic living body, continuously drawing nourishment from the "Execution and Validation" phase, and providing more precise input for the next round of "Strategic Foresight."

Chapter 4

The Economics, Ecosystem, and Future of Quantum Security



Chapter 4: The Economics, Ecosystem, and Future of Quantum Security

This section will explore the broader context and profound impact of successfully implementing the migration engine, analyzing its economic rationale, showcasing the powerful ecosystem that drives the engine, and looking ahead to its application prospects in the next wave of technological innovation.

4.1 The Economics of Crossing the Quantum Chasm: Investment, Risk, and Opportunity

Elevating PQC migration from a technical issue to a strategic decision requires a clear understanding of its economic principles. Investing in PQC is not merely a hedge; it is an investment in the "shield" of the digital economy. Compared to the high-risk "spear" of quantum computing hardware, PQC offers a deterministic market growth logic driven by global compliance. This is not just a security expense but a strategic investment in a company's future resilience and market competitiveness.

4.1.1 The Cost of Inaction: Quantifying the "Quantum Security Debt"

Delaying PQC migration is not a zero-cost decision; it is, in fact, the accumulation of "Quantum Security Debt." The core of this debt is the risk posed by the "Harvest Now, Decrypt Later" (HNDL) attack. The potential financial impact is enormous, including the permanent loss of intellectual property, massive regulatory fines, and the collapse of brand reputation.

4.1.2 Return on Investment (ROI) for Migration: Investing in Digital Trust

The Total Cost of Ownership (TCO) for PQC migration is substantial. While the U.S. federal government's early planning budget estimate was about $7.1 billion, this is widely regarded by the industry as an extremely conservative floor. Considering the enormous cost of legacy system discovery, complex supply chain dependencies, and the long-cycle requirement for "dual-track" operation, the actual total industry migration expenditure is expected to be several times this amount, potentially reaching tens of billions of U.S. dollars.

However, the return on this investment is multi-dimensional. The most direct return is the discharge of "Quantum Security Debt," avoiding catastrophic financial losses. More importantly, in a market increasingly focused on data security, companies that are first to complete PQC migration can use it as a powerful competitive advantage. The ability to demonstrate to customers and partners that their data possesses long-term security will be key to winning high-end contracts and customer loyalty. As large enterprises and government agencies adopt PQC compliance as a mandatory standard for supplier selection, early movers in migration will gain preferential access and stronger negotiating power in the supply chain.

4.1.3 Market Opportunity: PQC-Driven Exponential Leap

The global PQC market is undergoing explosive growth. Driven by the dual forces of replacing existing market share and increasing emerging market volume, the PQC market size is expected to achieve exponential growth. We can understand its potential using a simplified three-layer penetration model:

$$V_{PQC} = (S_{legacy} \times \alpha) + (S_{emerging} \times \beta) + V_{services}$$

Where:

V_{PQC} is the total size of the post-quantum cryptography market.

S_{legacy} represents the existing market size of traditional cryptographic applications that require PQC upgrades.

α is the PQC replacement rate in the existing market.

$S_{emerging}$ represents the market size of emerging applications directly adopting PQC, catalyzed by digital transformation.

β is the PQC penetration rate in emerging markets.

$V_{services}$ represents the market size of consulting, integration, operation, monitoring, and other services accompanying PQC deployment.

According to forecasts from multiple market research institutions, the global PQC market size is projected to grow from approximately $400 million to $1.6 billion in 2025 to nearly $7 billion to $10 billion by 2034, with a Compound Annual Growth Rate (CAGR) exceeding 37%. The capital market is increasingly viewing "cryptographic agility platforms" as core digital infrastructure assets, whose value lies in providing companies with a long-term compliance moat, a key element for unifying long-term social value and economic returns.

4.2 The Quantum-Ready Alliance and Practice Pioneers

Post-quantum migration is no longer a theoretical discussion. Global technology leaders have begun deploying PQC in actual products serving hundreds of millions of users, setting a benchmark for the entire industry and proving the feasibility of large-scale PQC deployment.

Google: Has experimented with and deployed a hybrid key exchange mechanism based on ML-KEM [12] in its Chrome[32] browser to secure TLS connections, and has added support for PQC digital signatures in its cloud key management service.

Apple: Released a groundbreaking post-quantum encryption protocol called PQ3 for its iMessage [31]. Its most significant innovation

is the achievement of continuous post-quantum key updates (rekeying), establishing a new security paradigm for end-to-end encrypted communication. The rollout of PQ3 will begin with versions like iOS 17.4 and macOS 14.4.

Microsoft: Is committed to deep integration of PQC capabilities into its Windows and Linux operating systems. By adding support for ML-KEM [12] and ML-DSA [13] to the Cryptography API: Next Generation (CNG) in Windows Insiders versions, it significantly lowers the barrier for enterprises to adopt PQC in their existing IT environments.

Meta: Has adopted a hybrid key exchange mechanism based on Kyber [12] in its internal TLS traffic as a defense-in-depth strategy during the transition period.

Signal: As the "gold standard" in secure communication, Signal launched the PQXDH (Post-Quantum Extended Diffie-Hellman) protocol[30] in September 2023. This is the world's first PQC hybrid key negotiation protocol implemented in a large-scale consumer application, proving that PQC can be deployed without sacrificing user experience such as call latency, and directly spurring subsequent applications like WhatsApp to follow suit.

Zoom: In May 2024, Zoom announced support for post-quantum upgrades for End-to-End Encryption (E2EE) in products like Zoom Workplace, becoming the first enterprise video conferencing platform to deploy PQC at scale. This move fills a gap in the migration of enterprise collaboration tools and validates the feasibility of PQC in high-bandwidth, low-latency scenarios such as real-time audio and video streaming[33].

Linux Foundation (PQCA): The Cornerstone of the Open Source Ecosystem. Furthermore, special attention must be paid to the Post-Quantum Cryptography Alliance (PQCA) led by the Linux Foundation, established in February 2024. The alliance unites tech giants such as AWS, IBM, Google, NVIDIA, and top research institutions like the University of Waterloo, aiming to provide production-ready, open-source PQC software

implementations globally. By integrating the well-known Open Quantum Safe project and the newly launched PQ Code Package, the PQCA is committed to building a highly secure open-source algorithm library compliant with NSA CSNA 2.0 standards. This means PQC capabilities will be standardly injected into the underlying code of the open-source ecosystem, greatly lowering the barrier for global developers to acquire PQC capabilities and ensuring the cryptographic agility of the entire software supply chain in the face of future quantum threats.

4.2.1 The Alliance as an Integrated Engine: From Oligopoly to Pluralistic Coexistence

The rise of the PQC market disrupts the stable structure of the traditional cryptography market dominated by a few oligarchs, fostering a more complex, dynamic, and multi-layered "pluralistic coexistence" ecosystem. A strong ecosystem is key to the successful implementation of the migration engine. The publishing alliance of this white paper, with its organizational structure, is itself a physical embodiment of the strategic engine framework, designed to provide customers with an integrated, "out-of-the-box" capability that can drive all phases of the engine.

The ecosystem map visually demonstrates how the alliance powers every stroke of the engine, visually encapsulating the alliance's comprehensive value proposition in a single, intuitive panorama.

4.2.2 Strategic Foresight and Algorithm Engine

Xi'an Jiaotong-Liverpool University PQC-X Lab: Led by Professor Jintai Ding, one of the core designers of the NIST standard ML-KEM [12], it possesses the dual capability of "spear" (cryptanalysis) and "shield" (algorithm design), providing the most authoritative risk assessment and algorithm selection guidance for the "Strategic Foresight" phase of the engine. The lab is dedicated to the research and technology transfer of general key technologies for post-quantum cryptography, aiming to build

an open, international R&D and technology transfer center.

Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University) Ministry of Education (CPS-DSC): Relying on the profound influence of its steering committee expert, Professor Hong Xiang, in international standards organizations (such as ETSI), this lab focuses on the security governance and international standards coordination of Cyber-Physical-Social Systems (CPSS). As the alliance's "Strategic Radar," it is responsible for tracking the global evolution of PQC standards (especially NIST and ETSI dynamics), providing the alliance with macro-strategic intelligence that spans technological and social governance dimensions, ensuring the migration solution possesses international interoperability and compliance.

Technology Stack Engine (Hardware Cornerstone and Software Framework): The alliance achieves a closed-loop capability of "software-hardware synergy." At the hardware level, represented by the indigenously controlled PQC chip (such as AHC001) developed by C*Core Technology, the computing power foundation is established; at the software level, members like LK Quantum have built a complete agile framework and SDK. Through deep collaborative design, the two collectively form the powerful "Technology Stack" that drives the engine's operation.

Yunchao Financial Services (Beijing) Co., Ltd. (Yunchao Financial Services): As a national high-tech enterprise focused on the cutting edge of financial quantum security technology, Yunchao Financial Services was jointly founded by the National Engineering Research Center for Financial Security and System Equipment and a wholly-owned enterprise subordinate to the People's Bank of China. The company has established three major strategic cores—"Digital Engineering, Integration Engineering, and Innovation Engineering"—and is committed to building an autonomous and controllable financial security barrier. Within the alliance, Yunchao Financial Services leverages its technological

advantage as a core participant in the Ministry of Science and Technology's National Key R&D Program "Research on Post-Quantum Cryptography Migration Technology for Banking and its Critical Infrastructure Information Systems," focusing on promoting the deep application of Post-Quantum Cryptography (PQC) technology in financial infrastructure. Its key contributions include: building a digital currency security system, providing anti-quantum encryption for the entire process of issuance and circulation; implementing financial infrastructure upgrades, integrating PQC technology into regional cash processing centers, digitized smart vaults, and unstaffed banking systems; and providing quantum-secure credit and data services, ensuring the transmission security of sensitive financial information. Yunchao Financial Services is committed to becoming a leading financial digital security service provider and industry innovation leader in the quantum era.

This advantage is not merely an academic connection but a strategic intelligence capability that can deeply understand the evolution of the world's two major PQC standard systems. The white paper has explicitly pointed out that "global standard divergence and compliance friction" is one of the major policy challenges facing PQC migration. Through Professor Hong Xiang's deep involvement in international standards organizations (such as serving as the Chairman of the Post-Quantum Cryptography Working Group at the 2017 ETSI QCS Annual Meeting, and successfully lobbying for the first time hosting of top international conferences like ETSI and PQCrypto in China) and domestic standard setting, the alliance gains the core capability to directly confront this challenge. For clients with global operations, this means the alliance can not only provide technical migration solutions but also offer strategic consulting on how to navigate the complex situation of coexisting NIST and Chinese national cryptography standards, helping them design architectures with high cryptographic agility[23], thereby gaining a

decisive advantage in managing supply chain risks and ensuring future interoperability. This essentially elevates the alliance's role from a technical implementer to a geo-technology risk strategist in the PQC field.

4.2.3 Simulation and Verification Engine

LK Quantum provides the migration framework and toolset, while Shanghai Xuntian Qianhe (Aerospace) and specialized joint laboratories in the financial and energy sectors provide the most authentic industry proving grounds, collectively forming the engine's "Simulation and Verification Ecosystem."

4.2.4 Governance and Talent Development

The PQC-X Lab plans to cultivate 20-50 PQC experts within three years, directly fueling the "human firewall" in the "Governance Cycle" to ensure sustained momentum.

The inclusion of the Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University) Ministry of Education (CPS-DSC) bridges the gap between technology and social trust. The lab will focus on establishing social trust models and governance frameworks for PQC migration, researching how to build verifiable trust chains in complex Cyber-Physical Systems (CPS). Concurrently, leveraging its platform advantages as a Ministry of Education Key Laboratory, it will focus on cultivating standardization experts and security governance talents with a global perspective, providing high-end intellectual support to maintain the engine's momentum.

This design is not accidental, but a strategic community meticulously constructed to systematically solve the challenges of PQC migration. The alliance is not a loose partnership but a living, breathing, and readily deployable migration engine.

4.2.5 Capital and Market Engine

Capital and Market Engine (Industry Incubation and Resource Allocation): To cross the "Valley of Death" in the commercialization of scientific research achievements, the alliance introduces professional industrial capital power. Strategic investment partners focus on resolving the industrial integration proposition of "spear and shield." As the alliance's Strategic Investment and Industry Incubation Engine, they support the construction of infrastructure, such as PQC agility platforms through "patient capital," opening up the circulation of technology and capital, accelerating the commercialization and M&A integration of PQC technology, and providing continuous financial lifeblood and strategic navigation for the ecosystem.

Table 4.1: Quantum Readiness Alliance Partners and Capability Matrix

Partner Organization	Core Expertise	Alliance Role	Key Contributions & Technologies	Representative Experience/ Products
XJTLU PQC-X Lab	PQC Algorithm Design & Cryptanalysis	Algorithmic Engine	Independent PQC algorithm R&D; Core design of NIST standard (ML-KEM); Advanced	Ding Key Exchange; Design of Rainbow, UOV, TUOV signature algorithms

			cryptanalysis (Breaking GeMSS, LUOV); World record in SVP Challenge	
Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University) Ministry of Education (CPS-DSC)	Cyber-Physical-Social Systems (CPSS) Security; International Standard Governance	Governance & Strategic Engine	International standard coordination; Social trust model construction; High-end talent cultivation	Deep participation in international standard formulation (e.g., ETSI); Possesses theoretical achievements in trusted computing for complex systems

Suzhou Langkong Post-Quantum Technology Co., Ltd. (LK Quantum)	Full-stack PQC Engineering & Productization	Commercialization Engine	PQC Agile Framework; SDK; Cloud SaaS Platform; AI-Assisted Migration Model	"LK Quantum Shield" Framework; Successfully applied to AI Large Model (DeepSeek) security & Hyperledger Fabric post-quantum migration
C*Core Technology Co., Ltd.	Proprietary CPU Cores; Secure Chip Design & Mass Production	Hardware Cornerstone	R&D of high-performance, controllable PQC chips & cryptographic cards; Anti-Side-Chan	AHC001 Anti-Quantum Cryptographic Chip (28nm process, proprietary CPU core); CCUPHPQ01

			nel Attack (SCA) design	Anti-Quantum Cryptographic Card
Yunchao Financial Services (Beijing) Co., Ltd. (Yunchao Financial Services)	Financial Infrastructure Anti-Quantum Upgrade; Digital Currency Security; Core Participant in National Key R&D Program	Financial Infrastructure & Digital Currency Security Engine	R&D of next-gen financial security infrastructure resisting quantum attacks; Building a secure encryption system for the full process of digital currency issuance,	Core entity of the National Key R&D Program; Digital Currency Security System; Regional Cash Processing Center

			circulation, and storage; Anti-quantum transmission protection for financial credit data	
Shanghai Xuntian Qianhe Space Technology Co., Ltd.	Commercial Satellite Development & On-orbit Verification	Industry Proving Ground (Aerospace)	Providing satellite communication scenario adaptation and on-orbit/high-fidelity environment testing	Leading commercial satellite ODM manufacturer; Possesses a low-cost new technology on-orbit verification platform

Chapter 5

The Battlefield of Specific Industries: Tailoring Migration Strategies to Industry Realities

Chapter 5: The Battlefield of Specific Industries: Tailoring Migration Strategies to Industry Realities

Post-Quantum Cryptography (PQC) migration is not a one-size-fits-all process. The vast differences in business characteristics, regulatory environments, data sensitivity, and device lifecycles across various industries necessitate a customized migration strategy, requiring precise "tuning" of each industry's "migration engine." The urgency and priority of the migration strategy largely depend on two core factors typical of the industry: "Data Lifespan" (the time data needs to remain confidential) and "Device Lifespan" (the service life of equipment in the field and its upgradeability). This chapter demonstrates how to apply the abstract "migration engine" framework to the unique operational realities of different key sectors, moving from theory to practice, and providing a tailored action manual.

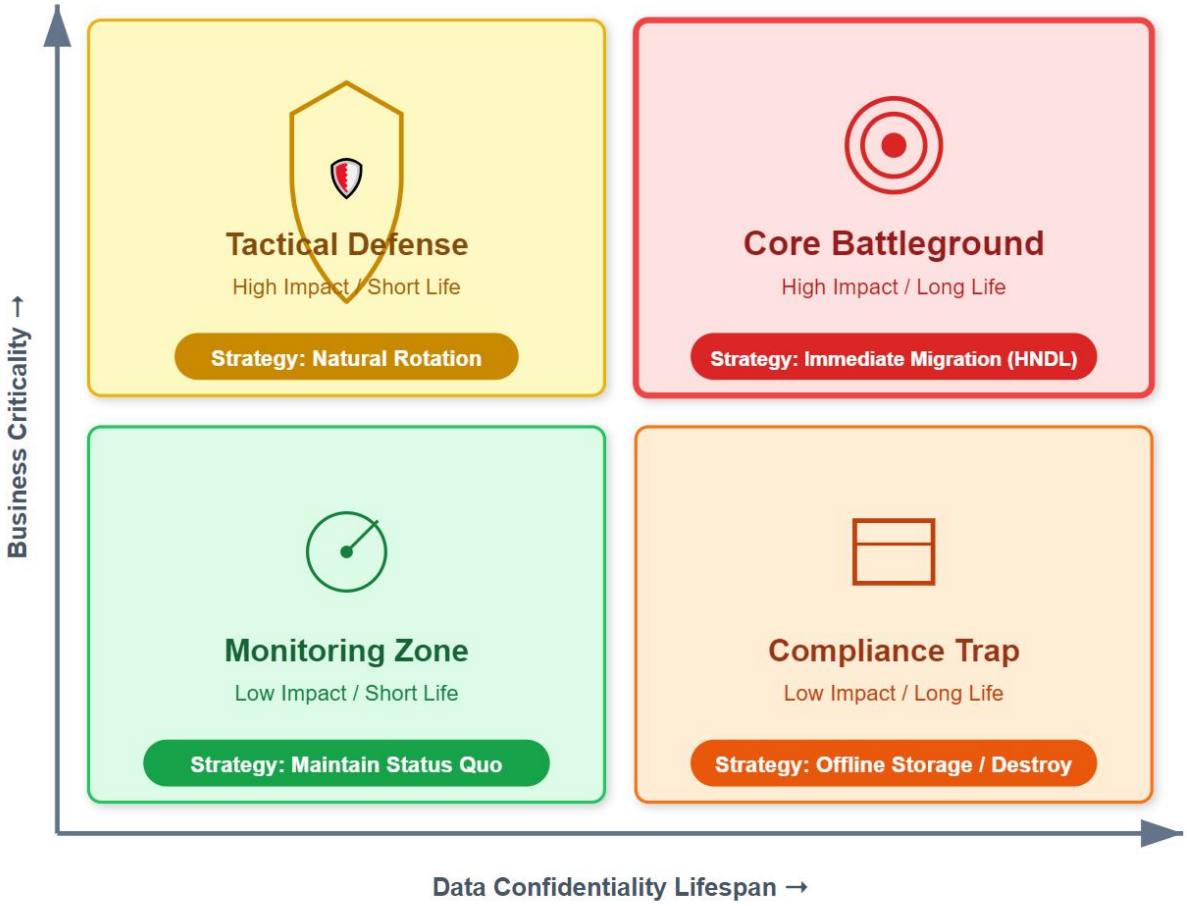


Figure 5.1: Strategic Triage — Migration Priority Decision Matrix

5.1 Industry-Specific Action Manual: Engine Adaptation

5.1.1 Critical Infrastructure (Finance + Energy + Power Grid)

5.1.1.1 Financial Services

Unique Challenge: The financial services industry faces a dual extreme challenge: on one hand, core transaction systems demand

extremely low latency and high throughput; on the other hand, vast amounts of financial data (such as mortgage contracts, insurance policies) have a confidentiality lifespan of decades, making them the highest value targets for "Harvest Now, Decrypt Later" (HNDL) attacks. As the "cornerstone" of the national financial system, PQC migration for the banking sector is crucial for preventing and defusing major economic and financial risks.

Engine Tuning:

Technology Stack: In terms of technology selection, priority must be given to deploying high-performance PQC Hardware Security Modules (HSM) and specialized cryptographic cards (such as the CCUPHPQ01 cryptographic card developed by alliance member C*Core Technology) to accelerate core transaction processing and meet stringent performance indicators such as a signature rate of no less than 4,000 times per second and a verification rate of no less than 8,000 times per second.

Execution and Validation Engine: Professional validation platforms must be utilized. For example, in collaboration with leading financial institutions, industry-leading financial security innovation platforms are utilized to conduct comprehensive functional, performance, and security verification of PQC solutions in a high-fidelity environment covering three core business scenarios: mobile banking, online banking, and interbank transactions, ensuring a smooth transition for customer terminals.

5.1.1.2 Energy and Utilities (Power Grid)

Unique Challenge: The biggest challenge in the energy and power grid sector is protecting its Industrial Control Systems (ICS) and Operational Technology (OT). These systems have extremely long lifecycles (often over 20 years) and are typically designed as "set and forget," making direct software or firmware updates difficult or even impossible. At the same time, the power system's requirements for high reliability and real-time performance allow for no compromise.

Engine Tuning:

Technology Stack: Technology choices must favor lightweight, low-power, and highly reliable PQC chips and cryptographic modules. This requires close cooperation with professional partners possessing core chip R&D capabilities for the State Grid, ensuring the solution meets industrial-grade standards.

Execution and Validation Engine: Since direct modification of legacy systems is not feasible, the core strategy is "encapsulation" protection. By deploying PQC-enabled secure access gateways (developed by professional equipment manufacturers with deep deployment experience in the energy sector), PQC security assurance can be provided for external communications without touching the existing OT system. All solutions must undergo comprehensive simulation verification and security attack testing in a professional laboratory environment that simulates power grid operations.

5.1.2 Long-Lifecycle Devices (Industrial IoT + Connected Vehicles + Satellites)

5.1.2.1 Industrial Internet of Things (IIoT/IoT)

Global Consensus in the Telecom Industry (2025): 3GPP officially accepted the PQC migration technical specifications for the 5G Core network and Subscriber Identity Module (SIM/eSIM) in its Release 19 standard freeze and Release 20 pre-study. The GSMA (Global System for Mobile Communications Association) subsequently released the Telecom Industry Post-Quantum Migration White Paper 2.0, warning global operators that infrastructure PQC upgrades[29] must be completed before 6G commercialization.

Unique Challenge: The Industrial IoT faces billions of resource-constrained devices with extremely limited computing power, memory, and power consumption. Furthermore, these devices are often

deployed in environments difficult to physically access, making large-scale Over-The-Air (OTA) firmware updates highly challenging. Their long lifecycle makes them ideal targets for HNDL attack.

Engine Tuning: The technology stack selection must prioritize lightweight PQC algorithms optimized for resource usage (such as Falcon and Kyber [12]) and adopt compact hardware designed specifically for IoT gateways (such as Mini-PCIe anti-quantum cryptographic cards). Crucially, PQC digital signatures must be used to secure the OTA update process itself, preventing the distribution of malicious firmware.

5.1.2.2 Intelligent Connected Vehicles (ICV)

Unique Challenge: The security of V2X (Vehicle-to-Everything) communication directly relates to the life safety of occupants and the public safety of road traffic. A vehicle's lifecycle often exceeds 15 years, meaning that cars manufactured today must have security systems capable of resisting cyber threats in 2040 and beyond. Therefore, PQC capability must be deeply integrated into the initial design phase of the entire vehicle's Electronic/Electrical Architecture (EEA).

Engine Tuning: The migration focus is on making PQC transformation a core component of the vehicle's EEA security investment, deploying compact PQC cryptographic cards suitable for the in-vehicle environment in On-Board Units (OBU) and Roadside Units (RSU) to protect the communication security and identity authentication of long-lifecycle vehicles.

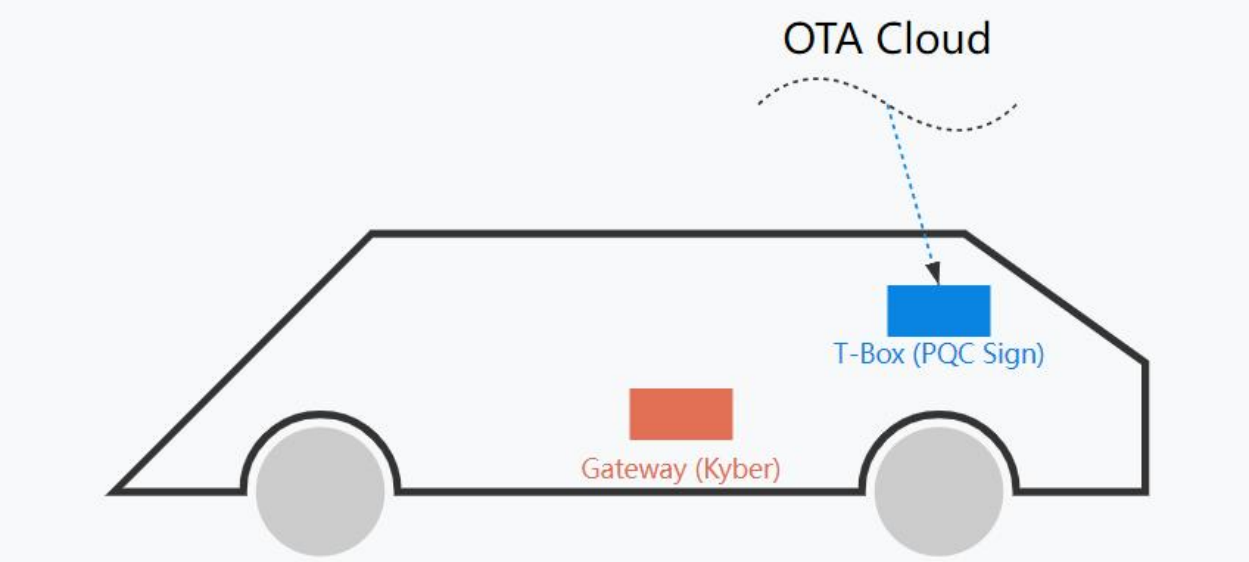


Figure 5.2: Quantum Immune System for Software-Defined Vehicles (ICV EEA)

5.1.2.3 Satellite Communication

Unique Challenge: The space environment is extremely harsh, resources on satellites (computing power, power consumption, storage) are highly limited, and communication links are characterized by high latency and limited bandwidth. Once launched into orbit, hardware upgrades are nearly impossible. In addition, anti-space radiation design must be considered.

Engine Tuning: It is necessary to collaborate with leading domestic commercial satellite ODM manufacturers like Shanghai Xuntian Qianhe and other professional partners to research the lightweight implementation of PQC algorithms and develop anti-radiation ARM encryption modules. In the execution and validation phase, their in-orbit verification platforms or high-fidelity space environment laboratories must be utilized to comprehensively test and evaluate innovative solutions such as "space-ground collaborative layered encryption,"

ensuring a space-to-ground code rate greater than 1kbps and a bit error rate below 10^{-4} under stringent conditions.

5.1.3 New Digital Ecosystems (AI + Blockchain + Web)

5.1.3.1 Artificial Intelligence and Advanced Robotic Systems

PQC is vital for protecting large-scale AI models, training data, and user interaction privacy. The technology framework of alliance member

LK Quantum has been successfully applied to protect the communication and database security of large AI models such as Qwen and DeepSeek. For embodied intelligent robots with long service cycles, PQC is a key defense strategy to ensure the security of their control instructions and data flow, preventing physical security risks.

5.1.3.2 Web3.0 and Blockchain

The security of emerging paradigms such as Dapps, digital identity, and DAO governance deeply relies on the robustness of the underlying cryptography. Project leader Professor Ding Jintai holds relevant patents for "anti-quantum blockchain," and the "LK Quantum Shield" framework by alliance member LK Quantum has also been successfully used for the post-quantum migration of the Hyperledger Fabric distributed operating system. In communities such as DAOs, planning and deploying protective measures against quantum attacks has become a developing trend.

5.1.3.3 Life Science and Healthcare

Genomic data, electronic medical records (PHI), and other highly sensitive information requiring long-term preservation make full-lifecycle security protection unprecedentedly important. This sector is one of the main demanders of PQC solutions. The focus of engine tuning is to adopt strong encryption methods capable of resisting future quantum attacks, utilizing PQC data archiving and destruction systems for long-term secure

storage and compliant destruction of medical records, thereby fostering a segmented market for quantum-safe data storage and processing.

These industry-specific action manuals reveal a core principle: the urgency and priority of PQC migration strategies largely depend on the industry's typical "Data Lifespan" and "Device Lifespan". The flexibility of the engine framework allows it to be effectively tuned to these different needs.

5.2 New Frontiers: The Application of Post-Quantum Cryptography in Artificial Intelligence and Physical Security

A successfully operating migration engine builds not only defensive capabilities but also an innovative capacity that can be applied to the next generation of security challenges. The application of PQC is rapidly moving beyond the traditional scope of communication encryption, entering new fields such as AI security and physical asset authentication.

5.2.1 Securing the Autonomous Future: Post-Quantum Cryptography Empowering AI Security

AI systems, particularly autonomous agents, have the core function of processing and creating high-value data with long-term confidentiality value (such as corporate strategic planning, R&D results), making them natural targets for HNDL attacks. An emerging multi-layered, in-depth defense architecture is providing end-to-end, future-proof protection for AI systems by combining PQC with Privacy-Preserving Computation (PPC) technologies.

Communication Security (Data in Transit): By integrating PQC algorithms (such as ML-KEM [12]) into protocols like TLS, all external communications of AI agents are ensured to be resistant to quantum decryption attacks.

Integrity Protection (Static Data and Code): PQC digital signature technology (such as ML-DSA [13]) is utilized to cryptographically sign AI models, training datasets, and software update packages, verifying their source and integrity, thereby defending against data poisoning and model tampering attacks.

Cognitive Protection (Data in Use): Advanced privacy-preserving computation technologies, such as Fully Homomorphic Encryption (FHE), are introduced to protect the confidentiality of data during AI inference and decision-making processes.

A profound strategic opportunity is embedded within this: the mathematical foundation of many state-of-the-art Fully Homomorphic Encryption (FHE) schemes is precisely the same as the core of the NIST PQC standards (such as Kyber [12] and Dilithium [13])—lattice-based cryptography. This means that the investment organizations are forced to make in PQC migration to counter future quantum threats is not purely a defensive cost. The technical capabilities established for PQC migration, including a deep understanding of lattice cryptography, specialized hardware acceleration capabilities (such as co-processors to speed up lattice operations), and optimized software libraries, can be directly reused for deploying next-generation privacy-preserving AI applications. Therefore, PQC migration transforms from a passive, compliance-driven cost center into a proactive, strategically enabling investment that provides enterprises with a competitive advantage in the future AI race. This provides a strong business case for accelerating PQC migration.

The following table summarizes the main threats faced by AI agents and corresponding cryptographic mitigation measures.

Table 5.1: AI Threats and Mitigation

Threat Vector	Threat	Primary	Technical

	Description	Cryptographic Mitigation	Mechanism
Communication Eavesdropping (HNDL)	Attackers intercept the agent's encrypted communications, waiting to decrypt them with future quantum computers.	PQC-Enhanced TLS 1.3 (using ML-KEM, etc.)	Using quantum-resistant algorithms to negotiate session keys ensures that intercepted ciphertexts cannot be broken even in the future.
Model/Software Tampering	Attackers tamper with the agent's software or model update packages during distribution.	PQC Digital Signatures (using ML-DSA, etc.)	All update packages carry the developer's PQC signature; the agent verifies the signature before installation to

			ensure authenticity and integrity.
Data/Model Poisoning	Attackers disrupt the agent's long-term decision-making capabilities by polluting training data or learning feedback.	PQC Digital Signatures + TEE	Signing trusted data sources with PQC; conducting model training/fine-tuning within a Trusted Execution Environment (TEE) to ensure the integrity of the training process is free from external interference.
User Data Privacy Leakage (In Use)	Service providers or attackers obtain sensitive user input data	Fully Homomorphic Encryption (FHE)	Users submit encrypted queries; the agent computes directly

	while the agent processes user queries.	on the encrypted data and returns encrypted results without decryption at any stage, achieving zero-knowledge processing.

5.2.2 The Rise of Quantum-Resistant Authentication: The Post-Quantum Anti-Counterfeiting Industry

PQC is transforming from a purely defensive technology into an enabling technology that gives rise to new business models. By applying PQC digital signature technology to physical goods, a permanent proof of authenticity can be created that is resistant to any known future computational attacks. Early market validation cases by LK Quantum in areas such as high-value collectibles, artwork, and fast-moving consumer goods clearly reveal the contours of this emerging industry. Its core value lies in the fact that the authentication provided by a PQC signature has its security rooted in mathematical problems, creating a new, eternal standard of trust for the "identity" of both physical goods and digital assets. This marks PQC's shift from being a risk mitigation tool to an engine for value creation and market expansion.

Table 5.2: Key Industry PQC Migration Drivers and Strategy Matrix

Industry Sector	Key Challenges (Data vs. Device Lifespan)	Key Migration Strategies	Relevant Alliance Partner Expertise
Financial Services	Extremely long data lifespan (decades), extremely high performance requirements for transaction systems	Hardware Acceleration (HSM/Crypto Cards); Full business validation in high-fidelity environments	C*Core Technology (Hardware)
Energy/Power Grid	Extremely long device lifespan (20 years), difficult to upgrade Operational Technology (OT) systems	"Encapsulated" Protection (PQC Secure Gateways); Industrial-grade chips & modules; Lab simulation	Industrial-grade chip partners (Environmental testing), Professional system integrators
Industrial IoT	Massive resource-constrained devices, difficult	Lightweight algorithms & hardware;	C*Core Technology (Chips), LK Quantum (Software

	firmware updates (OTA)	Protecting the OTA update process with PQC signatures	Framework)
Intelligent Connected Vehicles	Long vehicle lifecycle (15 years), safety directly impacts life	Deeply integrating PQC during the initial design phase of the Electronic Electrical Architecture (EEA)	C*Core Technology (Automotive-grade Chips/Crypto Cards)
Satellite Communications	Harsh space environment, highly resource-constrained, hardware cannot be upgraded after launch	Lightweight, Radiation-hardened implementation; On-orbit/High-fidelity environment verification	Shanghai Xuntian Qianhe (Satellite/ODM)
Artificial Intelligence	High value of AI models and training data, natural targets for HNDL attacks	Coordinated deployment of PQC & FHE to protect the entire process	LK Quantum (AI Large Model Security Application)

	of communication, data, and computation

*Reason: This matrix condenses the detailed discussion in Chapter 5 into a quick reference table, which is easy to read and helps readers quickly compare the strategic points of different industries and intuitively understand how alliance members match these needs.

Chapter 6

Comprehensive Overview of Global Post-Quantum Cryptography Migration Challenges

Chapter 6: Comprehensive Overview of Global Post-Quantum Cryptography Migration Challenges

The global migration to Post-Quantum Cryptography (PQC) is an unprecedented systemic engineering effort, with challenges spanning across technical, policy, economic, and organizational dimensions. Below is a comprehensive overview of these core challenges.

6.1 Technical Challenges: Navigating the Minefield of Engineering and Performance

Performance Overhead and Algorithm Selection: While bringing quantum security, NIST-standardized PQC algorithms (such as ML-KEM [12], ML-DSA [13]) also introduce significant performance overhead, primarily manifesting in much larger key and signature sizes than traditional algorithms, and higher computational complexity. This places immense pressure on environments with limited bandwidth and storage (such as the Internet of Things) and high-throughput systems (such as financial transactions), often requiring specialized hardware acceleration to compensate for performance loss.

Difficulty in Achieving Cryptographic Agility: Given the uncertainty of future threats, systems must possess "cryptographic agility"—the flexibility to switch encryption algorithms. However, the engineering complexity of retrofitting vast existing applications with hardcoded algorithms, designing protocol-layer negotiation mechanisms to thwart downgrade attacks, and managing diverse algorithms (such as HQC, the code-based backup scheme chosen by NIST for lattice cryptography) is extremely high.

Overhauling Legacy Systems and Public Key Infrastructure (PKI): One

of the greatest technical obstacles to migration is dealing with legacy systems and "shadow cryptography" deeply embedded in corporate operations. For those systems that cannot be directly modified, the only approach is "encapsulation" protection by deploying PQC security gateways. Simultaneously, the large key sizes of PQC necessitate a fundamental overhaul of the core of global PKI—the X.509 certificate standard—and the promotion of solutions like "Hybrid X.509 Certificates." This, however, requires upgrading the entire chain of certificate issuance and validation, which is a massive engineering undertaking.

The Evolving "Dual Threat": Organizations must not only defend against future Shor's algorithm[7] attacks on the mathematical foundations but also counter the "classical threats" of currently using AI tools to attack PQC engineering implementations. The severity of this challenge was highlighted by the recent event where the team led by Professor Ding Jintai from the PQC-X Lab at Xi'an Jiaotong-Liverpool University, a core member of this alliance, successfully cracked the 200-dimensional SVP challenge. This event powerfully demonstrates that even after migrating to next-generation cryptography considered 'quantum-resistant', classical attack capabilities against their mathematical foundations continue to evolve. This, coupled with the revelation of weaknesses in some NIST candidate schemes, collectively warns us that PQC migration is by no means "a once-and-for-all solution" but a dynamic process that requires continuous vigilance and iteration. Beyond the challenges to the mathematical foundation, attacks targeting engineering implementations have also become a reality. For instance, the "KyberSlash" side-channel vulnerability disclosed in late 2023 exploited timing differences in the division operation during the implementation of Kyber (the ML-KEM standard), allowing an attacker to recover the private key[34]. This case powerfully warns us that the theoretical security of an algorithm is not equivalent to the security of its engineering implementation, and high-fidelity validation environments

and anti-side-channel design are crucial in migration.

6.2 Policy and Governance Challenges: Managing Divergence and Internal Inertia

Global Standard Differences and High Demands for Dual Compliance: Global PQC policies are exhibiting a trend of 'great divergence'. The NIST standard camp led by the United States and China's independent standard route pursuing technological sovereignty coexist. This difference imposes higher-level security assurance requirements on multinational corporations, potentially forcing them to maintain incompatible product lines for different markets, increasing R&D costs and supply chain complexity, and even risking the fragmentation of the global internet's technical foundation.

Conflicting Global Timelines: Major economies like the United States, the European Union, and the United Kingdom are generally aligned but differ in migration milestones (e.g., 2030, 2035) and mandatory requirements. This compels global enterprises to align their planning with "most stringent requirements," conducting complex global risk assessments and resource prioritization to address the most pressing compliance pressures.

The Difficulty of Internal Governance: Internally, PQC migration faces two major governance challenges. The first is conducting a comprehensive "cryptographic asset discovery," which is extremely difficult due to the proliferation of "shadow cryptography," system heterogeneity, and a lack of automated tools. The second is establishing a permanent governance structure that transforms PQC migration from a one-time project into a perpetual risk management function, which requires overcoming managerial challenges such as the decline in top-level attention, cross-departmental collaboration difficulties, and organizational inertia.

6.3 Ecosystem and Economic Challenges: Bridging the Cost and Talent Gap

High Costs and the "Quantum Security Debt": The Total Cost of Ownership (TCO) for PQC migration is prohibitive, with the US Federal Government's estimate exceeding 7 billion USD. However, the cost of inaction is the accumulation of a "quantum security debt" composed of "Harvest Now, Decrypt Later" (HNDL) attack risks, the potential losses of which could far exceed the migration cost. Clearly justifying the necessity of this strategic investment to decision-makers is a major challenge.

The Critical Talent Bottleneck: The most fundamental constraint facing global PQC migration is the extreme scarcity of talent. Qualified PQC experts require a rare composite skillset spanning cryptography theory, software engineering, system architecture, and risk management. This talent shortage not only inflates project costs but may also cause the actual pace of migration to lag behind policy timelines, potentially even leading to flawed, rushed implementations done purely for compliance, which introduces new risks.

Nascent Ecosystem: The PQC ecosystem supporting large-scale migration remains immature in many aspects. The market lacks mature automated discovery and retrofitting tools, solutions are fragmented, and professional service providers with deep migration experience are still few. This necessitates a strategic community, such as the alliance that published this white paper, to integrate capabilities from industry, academia, research, and application to provide integrated solutions.

6.4 Industry-Specific Challenges: A Tailored Battlefield

PQC migration strategies must be "tuned" according to the realities of different industries, with each sector facing its unique combination of challenges:

Financial Services: Faces the dual pressure of long-term data

confidentiality needs and the requirement for extremely low latency and high throughput in transaction systems.

Energy and Critical Infrastructure: The biggest problem is protecting Industrial Control (OT) systems with lifecycles spanning decades that cannot be directly updated.

Internet of Things (IoT): Faces the challenges of extremely limited device resources (computing, memory, power consumption) and difficulties with large-scale firmware updates.

Intelligent Connected Vehicles: Security directly concerns human life, and the long vehicle lifecycle requires PQC to be deeply integrated into the initial design of the entire vehicle's Electronic/Electrical Architecture (EEA).

Chapter 7

Strategic Conclusion: Building a Resilient Migration Engine

Chapter 7: Strategic Conclusion: Building a Resilient Migration Engine

7.1 Recommendations for Enterprise Leaders (CISO, CIO, CEO)

7.1.1 Acknowledge Urgency, Elevate Strategic Positioning: Turn Risk into Opportunity

As enterprise leaders, you must view Post-Quantum Cryptography (PQC) migration as a current strategic risk concerning the company's survival and competitiveness, rather than a distant IT upgrade project that can be postponed. The urgency of this risk stems from the "Harvest Now, Decrypt Later (HNDL)" attack model, where adversaries are massively intercepting and storing today's encrypted data, waiting for the advent of future quantum computers to decrypt it. This means that for any data requiring long-term confidentiality—such as core intellectual property, long-term financial contracts, and personal health records—the security vulnerability effectively already exists.

Therefore, delaying PQC migration is not a zero-cost decision; it is, in fact, continuously accumulating an invisible yet extremely dangerous "quantum security debt." The potential "repayment" cost of this debt could be catastrophic, including permanent loss of intellectual property, massive fines for violating regulations like the Network and Information Systems Security Directive, Second Edition (NIS2), and devastating damage to brand reputation and customer trust. The historical lesson (such as the Crypto AG [3-5] incident) tells us that once an adversary masters the "master key" to break mainstream cryptography, they will never publicly disclose it but will secretly use it as a top-secret weapon. It

is imperative to complete the defense upgrade before the adversary's secret weapon achieves combat readiness.

The primary responsibility is to complete the ignition and start-up of the organization's 'Quantum Security Migration Strategy Engine'. Enterprises that complete the migration first can leverage it as a powerful competitive advantage, gaining an early lead in winning high-end contracts and customer loyalty, and receiving priority in increasingly strict supply chain access.

7.1.2 Immediately Launch "No-Regret Moves": Intelligence-Driven Decision

Any successful migration begins with a clear understanding. Therefore, immediate authorization and investment are required to initiate a comprehensive, enterprise-wide inventory of cryptographic assets and a quantum risk assessment. This initiative is widely considered a "No-Regret Move" because, regardless of when the quantum threat arrives, it significantly enhances the organization's security visibility and management capabilities, representing a pivotal opportunity to elevate overall "cryptographic maturity."

The goal of this work goes far beyond creating a static asset list; it is to build a dynamic, data-driven cryptographic intelligence view:

Map Cryptography: With data flow as the main thread, track the complete lifecycle of sensitive data within systems, understanding where, how, and why encryption is used.

Assess Risk Exposure: Classify data based on its confidentiality lifetime. Long-term contracts that need to be preserved for decades face a fundamentally different level of HNDL risk than session data that only requires short-term confidentiality. This classification method directly provides a decision basis for prioritizing migration efforts.

Visualize Systemic Risk: By mapping the risk contagion graph, understand how the vulnerability of a single system might spread to the

entire enterprise ecosystem through data interaction, thereby identifying systems that are critical nodes in the risk transmission path.

This task is challenging because "shadow cryptography" is ubiquitous, systems are highly complex and heterogeneous, and enterprises often lack automated inventory tools and standardized processes. However, this work provides a prerequisite for starting the migration engine and gaining initial ignition energy, transforming abstract risk into concrete, quantifiable actions. More importantly, it provides strong justification for obtaining high-level support. The PQC migration roadmap [24] published by the European Union explicitly states that "No-Regret Moves" like cryptographic asset management are part of compliance with regulations such as NIS2, and the management of relevant entities may be held accountable for failing to take "state-of-the-art" security measures[5]. This turns the initial steps of PQC migration from a forward-looking project to address a future threat into a necessary action to meet current legal compliance requirements, providing a solid legal basis for CISOs and CIOs to apply for resources from the board.

7.1.3 Invest in Agility, Not Specific Algorithms: Building a Future-Oriented Architecture

Establish cryptographic agility [23] as a core principle for all new technology architectures and procurement decisions. According to the authoritative definition by NIST, cryptographic agility is "the ability to replace and adjust... cryptographic algorithms for resiliency without interrupting running system processes." Future cryptographic standards and the threat environment are still subject to change, and only architectures that can flexibly switch encryption algorithms will remain resilient in the future. Investing in agility is crucial for the following reasons:

Respond to Standard Evolution: NIST's standardization process is far

from over. The launch of its fourth round of additional processes and the selection of code-based HQC as a backup for lattice-based cryptography both demonstrate an institutionalized adherence to "algorithmic diversity." Architectures must be able to adapt to new standards that may emerge in the future, rather than being locked into a single technology path.

Counter Iterative Threats: We face a "dual threat" environment. Even PQC algorithms themselves, which are the core of future defense, are becoming targets of constantly evolving classical attack methods, as evidenced by the recent successful break of the 200-dimensional SVP [35] challenge. An agile architecture allows you to respond quickly when new vulnerabilities are discovered, repairing the security line by switching algorithms instead of undergoing disruptive system reconstruction.

Navigate Global Divergence: With countries like China establishing independent PQC standard systems, global standards are showing a trend of "great divergence." For multinational companies, an agile architecture that can support and flexibly negotiate different cipher suites is the only realistic way to maintain compliance and interoperability in different regulatory environments.

Cryptographic agility [23] is the "foundation" of the entire migration engine, ensuring that the engine can run smoothly and continuously to adapt to any changes in the external environment. In practice, this means promoting technical teams to adopt abstract cryptographic APIs, supporting PKI with hybrid X.509 certificates, and modern communication protocols capable of securely negotiating algorithms at the protocol layer.

7.2 Recommendations for Policymakers and Regulatory Agencies

Post-quantum migration is a systemic project concerning national

security, economic stability, and technological sovereignty. The role of policymakers and regulatory agencies is to clear obstacles for all organizations' "migration engines" and provide a strong external "tailwind," ensuring the entire nation can smoothly and securely navigate this generational change in cryptography. To this end, we propose the following four core recommendations:

7.2.1 Refine Implementation Paths, Strengthen Strategic Execution

Given that our country has clearly defined the strategic direction and roadmap for post-quantum cryptography standards, the current focus should shift from "strategic planning" to "tactical execution." One of the biggest challenges facing PQC migration is organizational inertia. Therefore, the focus of policy formulation should be on transforming top-level design into concrete implementation levers, ensuring that the national strategy can penetrate all industries.

Issue Sector-Specific Implementation Details and Mandatory Timetables: Under the established national strategic framework, further non-negotiable hard deadlines for migration should be set for key infrastructure sectors such as finance, energy, and transportation (e.g., completing high-risk system migration before 2030). By breaking down macro goals into assessable phased tasks, a predictable and stable policy execution environment can be provided for the entire society.

Use Government and State-Owned Enterprise Procurement as Market Leverage: Drawing on the successful experience of the U.S. National Security Agency (NSA) CNSA 2.0 strategy, make compliance with PQC standards a mandatory requirement for government and key industry procurement. This will generate a powerful market ripple effect, incentivizing technology vendors to prioritize the integration of PQC capabilities into their commercial products, thereby greatly accelerating the popularization and application of PQC technology in the private

sector.

Provide Fiscal Incentives, Foster New Growth Points in the Digital Economy: PQC migration should be viewed as a crucial part of upgrading digital economy infrastructure. It is recommended to establish special funds or tax incentives, not only to reduce the compliance costs of small and medium-sized enterprises but also to drive the development of the high-end cryptography industry and the cybersecurity service industry through migration demand, building them into the secure foundation for data element circulation. This will not only solve security problems but also create economic increments.

7.2.2 Promote Standard Coordination, Reduce Global Compliance Friction

In the global digital economy, the fragmentation of standards will lead to huge economic costs and security risks. The key responsibility of policymakers is to act as a bridge and minimize technological barriers.

Actively Participate in and Promote International Standard Dialogue: Facing the trend of "great divergence" where the standard system represented by the U.S. NIST coexists with China's pursuit of an independent standard system, communication should be actively promoted among major standard-setting organizations such as NIST, the European Union Agency for Cybersecurity (ENISA), and the China Cryptography Standardization Technical Committee (CSTC) through diplomatic and technical exchange channels. Explore the establishment of mutual recognition of standards or cross-standard interoperability testing frameworks to reduce compliance costs and supply chain complexity for multinational companies.

Encourage and Invest in "Cryptographic Agility" Architecture: Given the uncertainty of future standards and the threat environment, "cryptographic agility" should be established as a core principle of the national cybersecurity architecture. Fund research and development of

technologies that can support heterogeneous cryptographic environments, such as security gateways and protocols that can simultaneously handle different national PQC standards, ensuring that the domestic system can maintain broad interoperability in the context of standard divergence.

7.2.3 Continuously Fund R&D Ecosystem, Bridge the Technology and Talent Gap

PQC migration is a long-term technological evolution that requires sustained innovation and knowledge reserves to maintain the "migration engine's" power.

Precise Funding for Next-Generation Fundamental Research: Funding support should not stop at currently standardized algorithms. Continuous investment should be made to support the ongoing security analysis of existing PQC standards (especially the mainstream lattice-based cryptography) to counter constantly evolving "classical threats" such as the successful break of the SVP challenge. At the same time, focus should be placed on funding backup algorithms with different mathematical foundations (such as code-based and isogeny-based cryptography) to ensure "algorithmic diversity" and prepare for potential "black swan" events in the future.

Vigorously Support Migration Tools and Platform Development: The complexity of PQC migration urgently requires mature tools for simplification. Special funds should be set up to encourage cooperation between academia and industry in developing open-source and commercial toolsets that can automate "cryptographic asset discovery," provide "high-fidelity validation," and achieve "grey evolution," thereby reducing the migration cost and implementation risk for the entire society.

Vigorously Support PQC Migration Validation System Construction: Establishing a sound PQC migration validation and

evaluation mechanism is key to ensuring migration security. Third-party testing institutions and industry laboratories should be authorized and supported to formulate scientific migration validation norms based on national standards. The focus should be on authoritative evaluations of PQC product compliance, migration scheme effectiveness, and system compatibility, providing credible quality certification and risk underwriting for migration work in various industries.

Establish a National Talent Training System: Recognizing the extreme scarcity of PQC professionals as the most fundamental constraint on migration, talent development should be elevated to a strategic height. Systematically build a cross-disciplinary talent pipeline that meets the needs of the next decade by supporting specialized university courses, establishing industry-academia joint training bases like the PQC-X laboratory, and providing subsidies for enterprises and individuals participating in PQC training.

7.2.4 Support Public-Private Partnerships (PPP), Accelerate Practical Implementation

The scale and complexity of PQC migration far exceed what any single entity can handle, necessitating the construction of a tight national-level cooperative network.

Promote the National Cybersecurity Center of Excellence (NCCoE) Model: NIST's NCCoE project is a public-private cooperation model that successfully unites technology giants, key industry users, and government agencies to jointly develop specific, actionable migration guidelines and practical solutions. This model should be replicated and promoted domestically, establishing specialized PQC migration innovation centers for key industries such as finance, energy, and healthcare, transforming standards into solutions that meet industry needs.

Fund Industry-Specific Pilot Projects and Validation Platforms: The

government should take the lead in investing and collaborating with industry-leading enterprises to jointly build industry-level "migration trial platforms." By verifying the performance and business compatibility of PQC solutions in real or high-fidelity simulation environments (such as the practice of Bank of Jiangsu in financial scenarios), valuable practical data can be accumulated, industry best practices can be formed, and shared industry-wide, thereby accelerating the migration process for the entire sector.

7.3 Recommendations for the Technical Community

The technical community is the ultimate implementer of global PQC migration and the core force for building and maintaining efficient and reliable components for the entire "migration engine." Facing this profound technological change, the actions of the technical community will directly determine the success, speed, and safety level of the migration. To this end, we propose the following three core recommendations:

7.3.1 Collaboration and Contribution: Jointly Building an Open, Robust PQC Ecosystem

The complexity of PQC migration is far beyond what any single organization can handle, and an open, collaborative, and battle-tested ecosystem is the cornerstone of success.

Deeply Participate in the Standardization Process: Actively participate in the work of international and national standard organizations such as NIST, IETF, and China CSTC. This means not only submitting new algorithm proposals but also investing in rigorous, public cryptanalysis of candidate algorithms, becoming the key force in "finding the weak before deployment." At the same time, contribute to the PQC adaptation of critical protocols such as TLS, IPsec, and X.509, solving

practical engineering problems caused by PQC algorithms, such as increased key/signature size and the need to support hybrid modes.

Strengthen Open Source Community Contributions: Actively participate in the Post-Quantum Cryptography Alliance (PQCA), established by the Linux Foundation in February 2024. PQCA integrates resources from tech giants including AWS, Google, and IBM, and formally takes over the governance of core open-source projects such as Open Quantum Safe (OQS). This signifies the transition of the PQC open-source ecosystem from a loosely community-driven model to industrial-grade joint governance. It is recommended to focus on the OQS project and contribute code, security reviews, and best practices to it.

High-Performance Implementation: Develop and optimize algorithm implementations for different platforms (such as x86, ARM) and instruction sets (such as AVX2, NEON), with a particular focus on the ability to resist side-channel attacks.

Language and Framework Integration: Create PQC library wrappers for popular programming languages (such as Go, Rust, Python, Java) and integrate them into mainstream cryptographic frameworks (such as OpenSSL) and applications, lowering the barrier to entry for developers.

Establish a Cryptanalysis Culture: Continuously conduct public academic attacks and security audits on standardized PQC algorithms, establish a responsible vulnerability disclosure mechanism, and promote the continuous improvement and security evolution of algorithms. The recent successful break of the 200-dimensional SVP [35] challenge is clear evidence of the value of community contribution.

7.3.2 Responsible Innovation: Simplify Security, Counter "Dual Threats"

The core responsibility of the technical community is to make the secure use of PQC simple, making "secure by default" the new normal, to counter the challenge of "dual threats."

Build "Misuse-Resistant" APIs and Libraries: Given that the most common risk in PQC migration stems from insecure engineering implementations (such as hardcoded keys, insecure API usage), the technical community should be committed to developing high-level, developer-friendly cryptographic libraries. These libraries should encapsulate complex underlying operations and provide concise, secure APIs that make it difficult for developers to make mistakes.

Develop Automated Security Tools: To counter automated attacks on engineering implementations driven by AI-driven cryptanalysis tools, the community should develop corresponding open-source defense tools. This includes:

Cryptographic Asset Discovery Tools: Develop tools capable of automating scans of code bases, binary files, and network traffic to help organizations establish their "Cryptography Bill of Materials (CBOM)" and discover "shadow cryptography."

Implementation Layer Vulnerability Scanners: Build tools that can statically or dynamically analyze code, specifically designed to find common vulnerabilities in PQC implementations.

Create Modular Migration and Validation Frameworks: Create open-source migration validation platforms and toolsets that support "grey evolution" strategies such as A/B testing, canary releases, and risk rollback, helping organizations conduct high-fidelity functional, performance, and security validation before putting PQC into production.

7.4 Focus on Forward-Looking Applications: Expanding the Value Frontier of PQC

PQC is not only a defensive technology but also an engine that empowers next-generation technological innovation. The technical community should move beyond traditional encryption scenarios and explore the value-added applications of PQC.

Empower Artificial Intelligence and Autonomous System Security: AI systems are natural targets for "Harvest Now, Decrypt Later" attacks. The technical community should develop dedicated frameworks to deeply integrate PQC into all layers of AI, including:

Using PQC to protect communication security between AI agents and between them and users.

Using PQC digital signatures to protect the integrity of AI models, training data, and software updates, countering data poisoning and model tampering.

Exploring the profound mathematical synergy between lattice-based cryptography in PQC and Fully Homomorphic Encryption (FHE) to lay the foundation for building next-generation privacy-preserving AI.

Foster New Business Models and Industries: Apply PQC technology to solve trust issues in the physical world. For example, utilizing the long-term security of PQC digital signatures to provide counterfeit protection for high-value goods, artworks, and legal documents that can resist any future computational attacks, thereby fostering the emerging industry of "post-quantum anti-counterfeiting."

Provide a Security Cornerstone for Emerging Digital Ecosystems: Provide deeply customized PQC solutions for emerging fields such as Web3.0, Blockchain, Industrial Internet of Things (IIoT), and Intelligent Connected Vehicles (ICV). For example, developing lightweight PQC firmware update mechanisms for resource-constrained IoT devices, or designing quantum-resistant digital signature schemes for blockchains.

7.5 Your First 90 Days: PQC Migration Quick Start Guide

For leaders who have been convinced by this white paper and wish to take immediate action, the most direct question is: "What is the immediate agenda for Monday morning?" This guide distills the core

ideas from the chapter on "Strategic Foresight and Risk Intelligence" into a goal-oriented, phased immediate action checklist. The core objective of these 90 days is to apply a powerful and precise ignition energy to the organization's "migration engine.

Phase 1: Days 1-30 — Establish Leadership Core, Unify Strategic Understanding

The goal of this phase is to lay the organizational foundation and elevate PQC migration from a technical issue to a strategic imperative with organization-wide consensus.

Week 1: Form a Cross-Functional PQC Working Group

Appoint a Project Lead: Appoint a senior executive (such as CISO, CIO, or CTO) as the project sponsor, empowering them with decision-making authority and resource mobilization capabilities.

Establish the Core Team: Team members must cross departmental boundaries, including representatives from IT, cybersecurity, application development, legal, compliance, risk management, and key business units. This ensures that migration decisions consider technical feasibility, compliance requirements, and business impact from the outset.

Weeks 2-4: Hold a Strategic Kick-off Meeting, Form High-Level Consensus

Clarify Urgency: Clearly communicate the nature of the quantum threat to the special team and core enterprise decision-makers (including CEO, CFO). Focus on explaining the "Harvest Now, Decrypt Later (HNDL)" attack model, emphasizing that for data requiring long-term confidentiality, the security risk already exists, and delaying action is accumulating "quantum security debt."

Establish a Strategic Perspective: Position PQC migration as a strategic opportunity to enhance the organization's overall "Cryptographic Maturity," rather than a simple technical upgrade. Emphasize that this is a business continuity imperative related to the

company's future survival and competitiveness, and it is a "No-Regret Move" that must be taken immediately.

Phase 2: Days 31-60 — Launch Asset Discovery, Complete Preliminary Assessment

The goal of this phase is to "get a clear picture," shifting from vague risk perception to data-driven, quantifiable risk understanding.

Weeks 5-7: Launch Cryptographic Discovery

Execute Scans: Utilize automated tools or engage professional service organizations to conduct comprehensive scans of networks, applications, databases, and code bases. The goal is to establish a preliminary "Cryptography Bill of Materials (CBOM)," understanding the use of cryptographic algorithms, protocols, keys, and certificates within the organization.

Identify "Shadow Cryptography": Pay special attention to undocumented cryptographic implementations deeply embedded in legacy systems or introduced by third-party components.

Weeks 8-9: Identify High-Value Data Assets and Classify Them

Map Data: Collaborate with business units to identify and list data assets with the longest confidentiality lifetime and highest business value, with data flow as the main thread. This includes core intellectual property, long-term customer contracts, personal biological and genetic records, financial transaction records, etc.

Sort by Lifetime: Classify data according to its expected confidentiality lifetime. This is the key basis for subsequent risk ranking and determining the priority of HNDL threats.

Phase 3: Days 61-90 — Quantify Core Risks, Determine Pilots, and Plan the Roadmap

The goal of this phase is to translate macro risks into specific action plans, preparing for the next stage of starting the engine.

Weeks 10-11: Host a Risk Assessment and Visualization Workshop

Quantify Risk: Combine the cryptographic asset inventory and the high-value data inventory and rank the risk of different systems based on the formula "Risk = Data Confidentiality Lifetime > Quantum Threat Appearance Time."

Build a Risk Matrix: Rate different risks by constructing a Risk Matrix, combining the two dimensions of the probability of risk occurrence and the magnitude of the impact caused.

Map the Risk Contagion Graph: Analyze the transmission mechanism of risk, draw a "Risk Contagion Map" and identifying systems that are at critical nodes and whose compromise could trigger a chain reaction.

Weeks 12-13: Determine Pilot Projects and Develop a Preliminary Roadmap

Select Pilots: Based on the risk assessment results, identify 3-5 of the most critical systems as the first batch of migration pilots. Ideal pilot projects should possess the characteristics of: highest risk, longest data confidentiality lifetime, being technically feasible (e.g., not highly coupled legacy systems), and capable of generating significant demonstration effects upon success.

Develop a Roadmap: Create a high-level migration roadmap for the pilot projects. The content should include:

Clear goals and scope.

Preliminary timeline and key milestones.

Preliminary estimates of required resources (human resources, budget, external experts).

Report to the PQC Working Group and decision-makers to obtain formal approval and budget support, preparing for the next stage of the engine: "Building Momentum: The Post-Quantum Cryptography Technology Stack."

Core Glossary

Abbreviation	Full Name	Definition / Context
AKE	Authenticated Key Exchange	A protocol allowing parties to verify identities and negotiate keys. The paper emphasizes deploying "Heterogeneous AKE" to address compatibility issues during the PQC migration.
ANSSI	National Cybersecurity Agency of France	The French authority for cybersecurity. It published a position paper on PQC migration, recommending a hybrid model for the transition.
BSI	Federal Office for Information Security	Germany's information security authority. It published the

	(Germany)	TR-02102-1 guideline, recommending algorithms like FrodoKEM as redundant backups.
CA	Certificate Authority	An authority responsible for issuing digital certificates. PQC migration requires CAs to upgrade to support hybrid X.509 certificates.
CAGR	Compound Annual Growth Rate	Used to describe PQC market growth. The paper predicts the PQC market CAGR will reach 37%-47% by 2034.
CBOM	Cryptography Bill of Materials	An inventory recording all cryptographic assets (algorithms, keys, libraries) in a system. The US and EU have designated it a mandatory compliance requirement for supply chains.
CDN	Content Delivery Network	Service providers such as

		Cloudflare. New IETF standards have cleared protocol obstacles for CDNs to perform large-scale PQC switchovers.
CISA	Cybersecurity and Infrastructure Security Agency	The US agency responsible for critical infrastructure security. It issued joint warnings with the NSA and drives CBOM compliance.
CISO	Chief Information Security Officer	The executive responsible for enterprise security. The paper suggests CISOs should lead PQC task forces and report risks to the board.
CNSA	Commercial National Security Algorithm Suite	The algorithm suite published by the NSA (Version 2.0), mandating that national security systems complete PQC migration between 2030 and 2035.

CRA	Cyber Resilience Act	An EU regulation requiring entities to adopt "state-of-the-art" security measures. Failure to implement PQC migration may be deemed non-compliant.
CRQC	Cryptographically Relevant Quantum Computer	A practical quantum computer with sufficient scale and error-correction capability to run Shor's algorithm and break RSA/ECC.
CSF	Cybersecurity Framework	The framework published by NIST (CSF 2.0). The NCCoE maps PQC migration to its core functions: Govern, Identify, Protect, etc.
CSTC	Cryptography Standardization Technical Committee	China's cryptography standard-setting body. Together with ICCS, it initiated a global PQC algorithm solicitation to build

		China's autonomous PQC standard system.
Crypto-Agility	Cryptographic Agility	A core strategic principle. The ability to flexibly switch cryptographic algorithms without disrupting business, serving as a foundation for handling future uncertainty.
DAO	Decentralized Autonomous Organization	An organizational form in Web 3.0. The paper notes that DAO communities are planning to deploy post-quantum protection measures.
ECC	Elliptic Curve Cryptography	Currently widely used public-key system. Relying on the discrete logarithm problem, it faces direct decryption threats from Shor's algorithm.

EEA	Electronic Electrical Architecture	The electronic system architecture of vehicles. Due to long vehicle lifespans, PQC capabilities must be deeply integrated during the EEA design phase.
ETSI	European Telecommunications Standards Institute	An international standards organization. The paper cites data on qubit requirements from its 2024 annual meeting in Singapore.
FHE	Fully Homomorphic Encryption	Technology allowing computation on ciphertext. Its mathematical basis (lattice cryptography) aligns with NIST PQC standards, offering strategic synergy.
HNDL	Harvest Now, Decrypt Later	A core threat model where attackers steal encrypted data now to decrypt it later with quantum computers. This makes long-term

		data risks a current reality.
HQC	Hamming Quasi-Cyclic	A code-based KEM algorithm. Selected by NIST as a backup standard for lattice cryptography to ensure algorithm diversity[15].
HSM	Hardware Security Module	A physical device for key management and crypto operations. High-performance scenarios like finance need to deploy quantum-resistant HSMs.
IBC	Identity-Based Cryptography	A system using identities (e.g., email) as public keys (e.g., SM9). The paper explores its evolutionary path toward PQC-IBE.
ICCS	Institute of Commercial Cryptography Standardization	A Chinese institution that published announcements and roadmaps for next-generation commercial cryptography (PQC)

		candidate algorithms.
ICS	Industrial Control Systems	Core systems in sectors like energy grids. Long lifecycles and update difficulties make them a challenging area for PQC migration.
ICV	Intelligent Connected Vehicles	Vehicle systems requiring PQC integration in V2X communications to guarantee long-term security.
IETF	Internet Engineering Task Force	The organization responsible for Internet standards. It published RFC standards supporting hybrid key exchange in TLS 1.3.
ISO/IEC	International Organization for Standardization	Has advanced amendments to incorporate Kyber and Dilithium into international standard systems like ISO/IEC 18033-2.
KEM	Key Encapsulation	A mechanism for negotiating

	Mechanism	shared keys. ML-KEM (Kyber) is the general-purpose KEM standard selected by NIST[12].
LWE	Learning With Errors	A core mathematical problem in lattice cryptography and a key research direction for China's next-generation anti-quantum identity cryptography.
ML-DSA	Module-Lattice-Based Digital Signature Standard	The general-purpose PQC digital signature standard published by NIST (FIPS 204), also known as Dilithium.
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism	The general-purpose PQC encryption standard published by NIST (FIPS 203), also known as Kyber.
NCCoE	National Cybersecurity Center of Excellence	A NIST subsidiary that translates PQC standards into practical

		guidelines through industry collaboration (e.g., migration projects).
NCSC	National Cyber Security Center	The UK security agency. It published a detailed three-stage roadmap for PQC migration (2028-2035).
NIS2	Network and Information Security Directive (2)	An EU directive mandating high-level security measures for critical infrastructure, driving PQC compliance requirements.
NIST	National Institute of Standards and Technology	The global frontrunner in PQC standardization, having selected the first batch of PQC algorithm standards through multiple rounds of competition.
NSA	National Security Agency	Issued the CNSA 2.0 algorithm suite, setting a mandatory PQC

		migration schedule for national security systems.
OQS	Open Quantum Safe	An open-source project providing PQC libraries (liboqs). It has now merged into the Linux Foundation's PQCA alliance.
OTA	Over-The-Air	Remote firmware update technology. PQC signatures must be used to protect the OTA process against malicious firmware injection.
OT	Operational Technology	Hardware/software used to monitor and control physical devices (e.g., grid control). Often hard to update, requiring "encapsulation" protection.
PKC	Public-Key Cryptography	The cornerstone of modern digital trust. The traditional PKC system

		faces reconstruction due to the emergence of Shor's algorithm.
PKG	Key Generation Center	The core component in identity-based cryptography (SM9) responsible for private key generation; requires post-quantum upgrades.
PKI	Public Key Infrastructure	The trust system based on digital certificates. PQC migration requires PKI to support larger key sizes and hybrid certificates.
PPC	Privacy-Preserving Computation	Technologies including MPC and homomorphic encryption. The paper notes combining PQC with PPC ensures security across the AI lifecycle.
PQC	Post-Quantum Cryptography	New-generation cryptographic algorithms capable of resisting

		quantum computer attacks; the core technology discussed in this white paper.
PQCA	Post-Quantum Cryptography Alliance	An alliance led by the Linux Foundation with AWS, IBM, etc., dedicated to providing production-ready open-source PQC software.
QaaS	Quantum Computing as a Service	Quantum computing power provided via cloud platforms. This makes it easier for attackers to access quantum capabilities, increasing security threats.
QFT	Quantum Fourier Transform	The core step of Shor's algorithm, capable of efficiently finding function periods to break mathematical problems like RSA.
QKD	Quantum Key Distribution	Key distribution technology based

		on physical principles. The paper notes it struggles with authentication and should complement PQC.
RFC	Request for Comments	Internet standard documents published by the IETF. RFC 9xxx established standards for hybrid key exchange in TLS 1.3.
ROI	Return on Investment	The ratio of investment to gain. The paper emphasizes PQC migration as a high-ROI investment for clearing "quantum security debt" and gaining competitive advantage.
RSA	Rivest-Shamir-Adleman	One of the most mainstream public-key encryption algorithms. Based on the large integer factorization problem, it will be

		broken by quantum computers.
SBOM	Software Bill of Materials	Software supply chain inventory. PQC compliance requires supplementing SBOMs with cryptographic information.
SDK	Software Development Kit	The paper mentions the need to develop lightweight PQC SDKs optimized for mobile endpoints.
SLH-DSA	Stateless Hash-Based Digital Signature Standard	A NIST standard (SPHINCS+). It offers high security but lower performance, suitable for scenarios like code signing.
SVP	Shortest Vector Problem	The security cornerstone of lattice cryptography. XJTLU's PQC-X Lab successfully challenged high-dimensional SVP, highlighting persistent classical threats.
TCO	Total Cost of Ownership	The total cost of PQC migration.

		The paper notes the actual cost could reach tens of billions of dollars.
TEE	Trusted Execution Environment	A secure area with hardware isolation. Used to protect the AI model training process from poisoning attacks.
TLS	Transport Layer Security	Protocol protecting Web traffic. A core scenario for PQC migration is upgrading the TLS handshake to support anti-quantum algorithms.
UOV	Unbalanced Oil and Vinegar	A multivariate digital signature scheme. Characterized by extremely fast verification, making it suitable for low-power terminals like IoT.
V2X	Vehicle-to-Everything	Vehicle communication technology. Requires PQC

		implementation during the design phase to resist future threats.
Web3.0	Web 3.0	The third-generation internet based on blockchain. The security of its digital identities and assets depends deeply on PQC upgrades.

Reference Documentation

[1]Capgemini Research Institute, "Future Encrypted: Why Post-Quantum Cryptography Tops the New Cybersecurity Agenda," Capgemini, 2025. [Online]. Available: https://www.capgemini.com/insights/research-library/post-quantum-crypto/

[2] Thales Group, "2025 ThalesData Threat Report: AI, Quantum and the Evolving Data Threatscape," Thales CPL Research, 2025. [Online]. Available:https://cpl.thalesgroup.com/ppc/data-threat-report?utm_source=google&utm_medium=cpc&utm_source=google&utm_medium=cpc

[3] G. Miller, "The Intelligence Coup of the Century," The Washington Post, 2020. [Online].
Available: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

[4]P. Oltermann, "CIA controlled global encryption company for decades, says report," The Guardian,
2020.[Online].Available: https://www.theguardian.com/us-news/2020/feb/11/crypto-ag-cia-bnd-germany-intelligence-report

[5]National Security Archive, "The CIA's 'Minerva' Secret," The George Washington University, 2020. [Online].
Available: https://nsarchive.gwu.edu/briefing-book/chile-cyber-vault-intelligence-southern-cone/2020-02-11/cias-minerva-secret

[6]R. P. Feynman, "Simulating Physics with Computers," International Journal of Theoretical Physics, vol. 21, 1982. [Online].
Available: https://link.springer.com/article/10.1007/BF02650179

[7]P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proc. 35th Annu. Symp. Found. Comput. Sci., 1994. [Online].
Available: https://ieeexplore.ieee.org/document/365700

[8]M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" IEEE Security & Privacy, vol. 16, no. 5, 2018. [Online].
Available: https://ieeexplore.ieee.org/document/8490169

[9]E. Gouzien et al., "Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126,133 Cat Qubits," Physical Review Letters, vol. 131, 2023. [Online].
Available: https://arxiv.org/abs/2302.06639

[10]C. Gidney, "How to factor 2048 bit RSA integers with less than a million noisy qubits," arXiv preprint arXiv:2505.15917, 2025. [Online].

Available: https://arxiv.org/abs/2505.15917

[11]Alliance for Telecommunications Industry Solutions (ATIS), "Quantum Technologies and the Cryptographic Threat Timeline: A Strategic Overview," 2025. [Online].
Available: https://atis.org/resources/quantum-technologies-and-the-cryptographic-threat-timeline-a-strategic-overview/

[12]NIST, "Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203)," 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/203/final

[13]NIST, "Module-Lattice-Based Digital Signature Standard (FIPS 204)," 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/204/final

[14]NIST, "Stateless Hash-Based Digital Signature Standard (FIPS 205)," 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/205/final

[15]NIST, "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption," NIST News Release, 2025. [Online].
Available: https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

[16]F. Driscoll et al., "Terminology for Post-Quantum Traditional Hybrid Schemes (RFC 9794)," IETF, 2025. [Online].

Available: https://www.rfc-editor.org/info/rfc9794

[17]D. Stebila et al., "Hybrid key exchange in TLS 1.3 (draft-ietf-tls-hybrid-design)," IETF Internet-Draft, 2025. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

[18]ISO/IEC, "ISO/IEC 11770-3:2021 Information security — Key management — Part 3: Mechanisms using asymmetric techniques," 2021. [Online]. Available: https://www.iso.org/standard/82709.html

[19]ISO/IEC, "ISO/IEC 14888-3:2018 Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms," 2018. [Online]. Available: https://www.iso.org/standard/76382.html

[20]The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10)," 2022. [Online]. Available: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[21]National Security Agency (NSA), "Announcing the Commercial National Security Algorithm Suite 2.0," 2022. [Online]. Available: https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

[22]NIST, "Transition to Post-Quantum Cryptography Standards (NIST IR 8547 Draft)," 2024. [Online]. Available: https://csrc.nist.gov/pubs/ir/8547/ipd

[23]NIST, "Considerations for Achieving Crypto Agility: Strategies and Practices (CSWP 39)," 2025. [Online]. Available: https://www.nist.gov/news-events/news/2025/12/nist-publishes-cswp-39-considerations-achieving-crypto-agility

[24]European Commission, "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography," 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[25]TNO, AIVD, & CWI, "The PQC Migration Handbook, Version 2," 2023. [Online]. Available: https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf

[26]National Cyber Security Centre (NCSC), "Timelines for migration to

post-quantum cryptography," 2025. [Online].

Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[27]Institute of Commercial Cryptography Standards (ICCS), "Announcement on Launching the Next-generation Commercial Cryptographic Algorithms Program (NGCC)," 2025. [Online]. Available: https://www.niccs.org.cn/en/

[28]State Cryptography Administration of China, "GM/T 0044-2016: SM9 Identity-based Cryptographic Algorithms," 2016. [Online].

Available: http://www.gmbz.org.cn/main/bzlb.html

[29]GSMA, "Post Quantum Cryptography Guidelines for Telecom Use Cases V2.0" 2024. [Online].

Available: https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/post-quantum-cryptography-guidelines-for-telecom-use-cases-pq-03-2/

[30] Signal Foundation, "PQXDH: The New Post-Quantum Agreement Protocol for Signal," 2023. [Online]. Available: https://signal.org/blog/pqxdh/

[31]Apple Security Engineering and Architecture, "iMessage with PQ3: The new state of the art in quantum-secure messaging," 2024. [Online].

Available: https://security.apple.com/blog/imessage-pq3/

[32] Google Chrome Team, "Advancing Our Amazing Bet on Asymmetric Cryptography," Chromium Blog, 2024. [Online]. Available: https://blog.chromium.org/2024/05/advancing-our-amazing-bet-on-asymmetric.html

[33]Zoom Video Communications, "Zoom bolsters security offering with the inclusion of post-quantum end-to-end encryption in Zoom Workplace," 2024. [Online]. Available: https://news.zoom.com/post-quantum-e2ee/

[34]D. J. Bernstein et al., "KyberSlash: Exploiting secret-dependent division timings in Kyber implementations," IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025. [Online]. Available: https://kyberslash.cr.yp.to/

[35] XJTLU PQC-X Lab, "XJTLU team sets code-breaking record for testing post-quantum online security," 2025. [Online]. Available: https://www.xjtlu.edu.cn/en/news/2025/03/xjtlu-team-sets-code-breaking-record-for-testing-post-quantum-online-security

[36]Linux Foundation, "Announcing the Post-Quantum Cryptography Alliance (PQCA)," 2024. [Online]. Available: https://pqca.org/