Article

Not peer-reviewed version

Accelerating the Deployment of China's National Standard and Industrialisation of Quantum Resistant Cryptography (PQC) Proposal for Building National Security "Double Insurance" in Quantum Era

Wei Meng *

Posted Date: 25 August 2025

doi: 10.20944/preprints202508.1741.v1

Keywords: PQC standardisation; QKD enhanced defence; national security governance; international influence

 doi:10.20944/preprints202508.1741.v1

Article

Accelerating the Deployment of China's National Standard and Industrialisation of Quantum Resistant Cryptography (PQC) Proposal for Building National Security "Double Insurance" in Quantum Era

Wei Meng

Dhurakij Pundit University, Thailand; weimeng4@acm.org

Abstract

Under the threat window of 'interception first, decryption later' in quantum computing, national security and industrial sovereignty face new systemic challenges. This paper proposes a dual-track approach of 'PQC baseline + QKD enhancement' to comprehensively compare the standard systems, governance models, and engineering progress of China and the United States in post-quantum cryptography (PQC) and quantum key distribution (QKD). The study employs a three-tier evidence integration framework of 'policy-standards-engineering,' combining authoritative documents from NIST, OMB, CISA, and other sources with China's national standard platform and industry announcements. It constructs an analysis model of 'standard hierarchy-migration ecosystem-international interoperability' and evaluates the feasibility of the scheme through gap-risk mapping, roadmap design, and KPI matrix assessment. The results show that the United States has established a closed-loop system of 'primary standards + redundancy' based on FIPS 203/204/205 and HQC backup algorithms, and has entered an auditable implementation phase driven by mandatory migration and toolchain initiatives from OMB and CISA; China maintains an advantage in QKD engineering and standardisation, but national standards for PQC have not yet been solidified, and the migration governance system lags behind, resulting in a structural shortfall of 'engineering leading the way while algorithm standards lag behind.' Based on this, this paper proposes a 'three-year-five-year-ten-year' national roadmap: establish a standardised baseline within three years, achieve large-scale migration and verification within five years, and complete consolidation and internationalisation within ten years. This will be supplemented by protocols, PKI/certificates, key lifecycle management, testing and certification, and algorithm switching mechanisms, in conjunction with a five-tier governance structure led by the State Cryptography Administration, with TC260/TC485 as the technical focal points, and the Ministry of Industry and Information Technology/ the Cyberspace Administration of China/People's Bank of China, operator and critical infrastructure implementation, and research institutes. The conclusion states that PQC must be established as the 'basic defence line' in the quantum era, while QKD should serve as the 'enhanced defence line' for critical links; China must complete the construction of PQC national standards and migration governance capabilities within a three-year standardisation, five-year consolidation, and ten-year internationalisation timeline, and achieve dual-track integration and international interoperability with the QKD standard suite, thereby safeguarding national security, consolidating industrial resilience, and enhancing international influence.

Keywords: PQC standardisation; QKD enhanced defence; national security governance; international influence

I. Introduction

 doi:10.20944/preprints202508.1741.v1

During the rapidly approaching window of "harvest-now-decrypt-later" risk of quantum computing, the U.S. has formally finalised and released three national standards for post-quantum cryptography (FIPS 203/204/205) in August 2024, and added HQC as a backup algorithm for key encapsulation mechanism (KEM) in March 2025 to form a "master standard + redundancy" security framework; and the White House OMB M-23-02 and CISA OMB M-23-02 and CISA OMB M-23-02 will be released to the public. In March 2025, HQC was added as the backup algorithm for key encapsulation mechanism (KEM), forming the security framework of "main standard + redundancy"; under the traction of the White House OMB M-23-02 and the CISA quantum-ready roadmap, the US has entered the stage of forced migration and systematic landing (NIST, 2024a; NIST CSRC, 2024; NIST, 2025; OMB, 2022; CISA, 2023). Correspondingly, China has formed a complete family of national and industrial standards on quantum key distribution/quantum secure communication (QKD) (e.g., GB/T 42829-2023, GB/T 43692-2024, YD/T 3834.1-2021, and GM/T 0108-2021), and initiated the "QKD Security Requirements, Testing and Evaluation". The development of a series of national standards for "QKD Security Requirements, Testing and Evaluation" has also been initiated, but the GB/T national standards at the level of post-quantum cryptography (PQC) algorithms have not yet been publicly released, presenting a structural shortcoming of "the engineering chain goes ahead while the national standards for algorithms are lagging behind" (SAMR, 2023; SAMR, 2024; SAMR, 2023; SAMR, 2024; China Communications Standards Association (CCSA), 2021; State Cryptography Administration (SCA), 2021; TC260, 2025).

Accordingly, the conclusions and recommendations are as follows: If a systematic plan of China's PQC national standards + Critical Information Infrastructure (CII) migration routes cannot be formed within three years, China will be passively aligned with the US standards in terms of international cryptographic discourse, hardware and software ecology, and the resilience of the CII, which will bring about supply chain constraints, passive compliance, and uncertainty in long-term confidentiality (NIST, 2024a; OMB, 2022; CISA, 2023). It is recommended to immediately start the "PQC National Standard Project": establish the redundancy mechanism of main algorithm + backup algorithm based on the grid cipher and coded cipher, and ensure that the first batch of KEM and digital signature GB/T standards will be released before 2026, and then connect them with the existing QKD national standard group to construct the "PQC Baseline + QKD Enhancement" standard. + QKD enhancement" dual-track architecture; simultaneously release a national migration roadmap and quantitative assessment covering the party, government, military and critical information infrastructure, and conduct "asset inventory - risk classification - protocol and certificate dual stack - consistency testing - red team assessment - annual assessment". The closed-loop promotion of "asset inventory - risk grading - protocol and certificate double stack - conformance testing - red team evaluation - annual rehearsal" will complete the large-scale replacement of high-value links by 2030; and with the ISO/IEC platform and the "One Belt, One Road" project as a handhold, we will export China's solutions and industrial capabilities, and solidify international interoperability. With the ISO/IEC platform and the "Belt and Road" project as the key, we will export Chinese solutions and industrial capabilities, and solidify our dominant position in international interoperability and supply chain (CISA, 2023; NIST CSRC, 2024).

II. Posture Assessment and National Security Implications

The U.S. has entered the mandatory migration preparation period for Post-Quantum Cryptography (PQC): FIPS 203 (ML-KEM/Kyber), FIPS 204 (ML-DSA/Dilithium), and FIPS 205 (SLH-DSA/SPHINCS+) were officially released and came into force on 2024-08-13, and HQC was selected as the KEM backup algorithm on 2025-03-11, and the fourth round of selection and technical basis was clarified by the NIST IR 8545 system to build a robust system of "Master Standard + Redundancy" (NIST, NIST, IR 8545). On 2025-03-11, HQC was selected as the KEM backup algorithm, and the NIST IR 8545 system was used to clarify the selection and technical basis for the fourth round of selection to build a robust system of "master standard + redundancy" (NIST, 2024a; Federal Register, 2024; NIST, 2025). On the governance side, the White House OMB M-23-02 requires federal

 doi:10.20944/preprints202508.1741.v1

agencies to carry out cryptographic asset inventory and migration planning, and CISA has successively released quantum-ready routes and automated discovery/inventory tool strategies, and promoted quantifiable and auditable migration rhythms with the help of government procurement and supply chain assessment (OMB, 2022; CISA, 2023, 2024). In contrast, China has formed a more complete family of standards and engineering advantages in quantum key distribution/quantum secure communication (QKD) (Beijing-Shanghai Trunk Line, etc.): there are the "Basic Requirements for Quantum Secure Communication Applications" (GB/T 42829-2023), "Quantum Communication Terms and Definitions" (GB/T 43692-2024), "Quantum Communications Terminology and Definitions" (GB/T 43692-2024), and "Quantum Communication Terms and Definitions" (GB/T 43692-2024). (GB/T 42829-2023), "Quantum Communication Terms and Definitions" (GB/T 43692-2024), the communications industry standard "Quantum Key Distribution System Technical Requirements Part 1: QKD System Based on Deceptive State BB84" (YD/T 3834.1-2021), and the cryptographic industry standard "Technical Specification for Deceptive State BB84 Quantum Key Distribution Products" (GM/T 0108-2021), and further initiated the "Security Requirements, Testing and Evaluation of Quantum Key Distribution for Cybersecurity Technology" (GM/T 0108-2021). The National Standard on Security Requirements, Testing and Evaluation Methods for Quantum Key Distribution for Network Security Technology (Call for Comments/Request for Draft) was further initiated to fill in the security evaluation and assessment link (SAMR, 2023; SAMR, 2024; China Association for Standardization of Telecommunications, 2021; State Administration of Cryptography, 2021; TC260, 2024/2025). However, the GB/T national standard for PQC algorithms has not yet been publicly released, and there is a lack of an integrated migration framework and quantitative assessment of "discovery-assessment-replacement-verification" on the side of government affairs and critical information infrastructures (Guanji). There is a structural shortcoming of "engineering chain first, algorithmic national standard lags behind" (based on the comprehensive judgement of national standard information public service platform and TC260 announcement). In the dimension of national security, if a cryptography-related quantum computer (CRQC) that can break RSA/ECC emerges before 2030, intercepting first and decrypting later will expose historical secrets and long-life data to the risk of being decrypted after the fact; accordingly, it should be established that "PQC is the baseline security, and QKD is the enhanced security", Therefore, the dual-track route of "PQC for baseline security and QKD for enhanced security" should be established, and the simultaneous promotion of policy traction and standardisation should be carried out in order to reduce systemic risks and maintain the dominant position in international interoperability and supply chain (OMB, 2022; CISA, 2023).

Figure 1 illustrates the difference in paths between the US and China on quantum cryptography standardisation and their security implications.Progress in the United States: The United States has formally released FIPS 203/204/205 in 2024, and established HQC as the backup KEM (NIST IR 8545) in 2025, combining with the migration inventory of OMB M-23-02 and the CISA toolchain, to complete the closed-loop of "standard-migration-governance" step by step. -governance" closed loop.

Progress in China: China has established a system of QKD application and industry standards (e.g. GB/T 42629-2023, GB/T 43692-2024, YD/T 3834.1-2021, GM/T 0108-2021), and promoted the national standard for testing and evaluation, but there is still a gap in the GB/T national standard for PQC algorithm.

Risk chain: If a cryptography-related quantum computer (CRQC) that can break RSA/ECC appears before 2030, historical data will be decrypted, and there is a risk of communication leakage in critical information infrastructure.

Dual-track defence framework: PQC is seen as a 'baseline defence' for broad systems and long-term data, while QKD is an 'enhanced defence' for high-value links, complementing each other.

 doi:10.20944/preprints202508.1741.v1

Figure 1. US vs China: PQC & QKD StandarizationaLandscape. Illustrated by the author.

Three-phase route: It is recommended that China complete PQC standard development and hybrid suite baseline in 2025-2026, achieve scale migration and conformance validation in key industries in 2027-2028, and promote ≥80% off-base migration in 2029-2034, while participating in the ISO/IEC standards game. At the same time, it will participate in the ISO/IEC standard game, forming a complete path of "domestic solidification + international export".

On the whole, the map highlights the first-mover advantage of the U.S. in PQC standards and migration governance, and China's leading position in QKD engineering deployment. However, if we don't accelerate the introduction of PQC standards and eco-construction, China will be in a passive position in the international code competition in the future.

III. Timeline of the Evolution of Standards in China and the United States

Table 1. Timeline of the evolution of Chinese and American standards.

vintages	United States (PQC)	China (Quantum Communications/QKD Mainline)
2016	Released NISTIR 8105, proposed PQC roadmap	—
2017	First round of 69 candidate algorithms announced on 20 December (NIST, 2019)	—

 doi:10.20944/preprints202508.1741.v1

vintages	United States (PQC)	China (Quantum Communications/QKD Mainline)
2019	Announcement of 26 candidate algorithms for the second round	—
2020	Release of Second Round Status Report NISTIR 8309 (NIST, 2020)	—
2022	Proposed standardised algorithms announced on 5 July: Kyber, Dilithium, SPHINCS+ (Falcon as a backup) (NIST, 2022)	The Ministry of Industry and Information Technology's QKD series of standards for the communications industry and commercial confidentiality industry continue to improve.
2023	OMB M-23-02 Requirement for Federal Agencies to Initiate PQC Migration Readiness	GB/T 42829-2023 "Basic Requirements for Quantum Secure Communication Applications" published (implemented on 2024-03-01) (SAMR, 2023)
2024	Official release of FIPS 203/204/205 on 13 August (NIST, 2024a; Federal Register, 2024)	GB/T 43692-2024 "Quantum Communication Terms and Definitions" published (implemented on 2024-10-01)
2025	11 March Selection of HQC as Alternate KEM and Release of NIST IR 8545 (NIST, 2025)	QKD Safety Requirements, Test and Evaluation Methods (Part 1: Requirements) published for comment on 25 April (TC260, 2025)

Illustrated by the author. Sources. NIST official project pages/bulletins, Federal Register, OMB and CISA documents; National Standard Information Public Service Platform, National Cryptologic Administration, TC260 bulletin (see references at the end of the article for details).

Figure 2 Dual-track timeline (2016-2025) for the evolution of post-quantum cryptography (PQC) and quantum key distribution (QKD) standardisation between the US and China.

This figure shows the parallel evolutionary paths of the US and China in terms of national cryptographic strategies. The upper timeline presents the advancement of the U.S. in the field of post-quantum cryptography (PQC), starting from the release of the NIST IR 8105 roadmap in 2016, through multiple rounds of algorithm selection, to the official release of FIPS 203/204/205 in 2024, and the identification of HQC as an alternate key encapsulation mechanism through NIST IR 8545 in 2025, which has gradually completed the "standard-migration-key-distribution (SMKD) standardisation" process. In 2025, HQC will be identified as an alternate key encapsulation mechanism through NIST IR 8545, gradually completing the closed loop of "standard-migration-ecology". The lower timeline reflects China's standardisation progress in the field of quantum key distribution (QKD) and quantum secure communication, including the continuous improvement of industry and

 doi:10.20944/preprints202508.1741.v1

cryptographic standards, the release of GB/T 42829-2023 and GB/T 43692-2024, and the 2025 draft of the standard on QKD security requirements and testing.

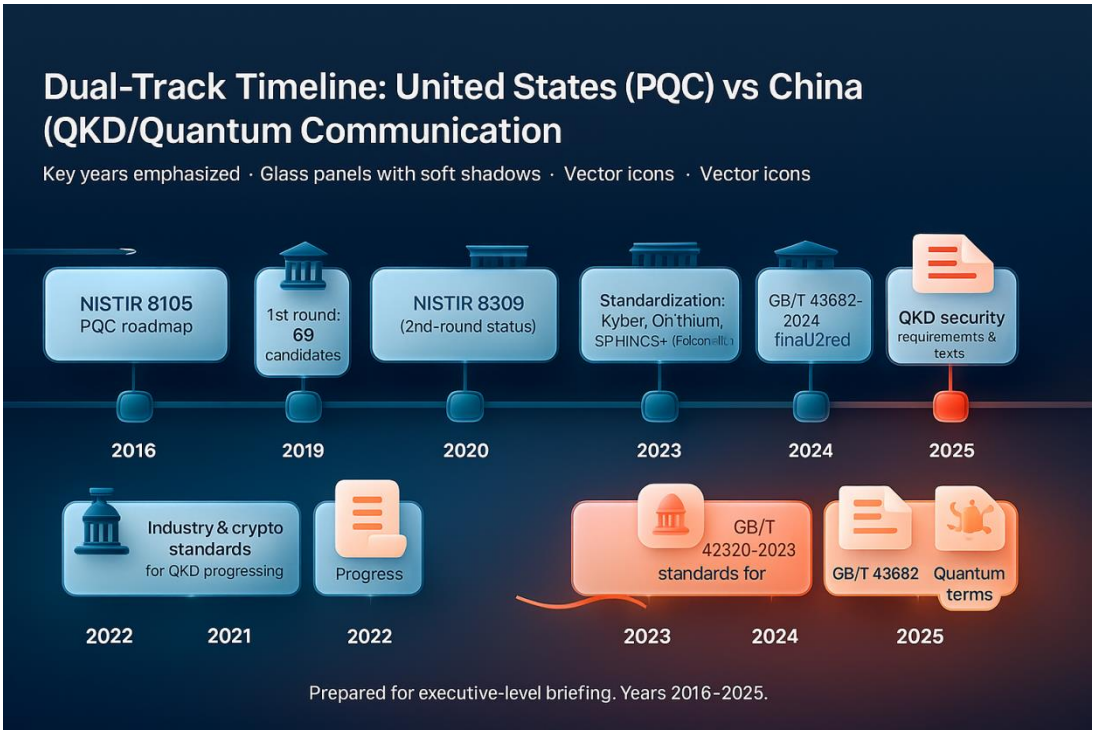

Figure 2. Dual-Track Timeline: United States (PQC) vs China (QKD/Quantum Communication. Illustrated by the author

Comparing the two-track paths, it can be seen that the US has taken the lead in realising the systematic implementation of post-quantum cryptography, while China maintains global leadership in quantum communication/QKD standards and engineering deployment, but there is still a gap in national PQC standards. The key years marked in the figure (2022, 2024, 2025) highlight the divergence nodes of cryptographic strategies of the two countries, revealing the far-reaching impact of cryptographic standardisation in the quantum era on national security and international discourse.

IV. Gaps and Risk Assessment

From the perspective of the three main lines of standard level, migration ecology and international discourse, the United States has formed a closed loop of "standard-assessment-migration" that can be enforced and audited: at the standard level, the official release of FIPS 203/204/205 and the establishment of HQC as the alternate algorithm for KEM are the "main standard + redundancy" structure. At the standards level, the official release of FIPS 203/204/205 and the establishment of HQC as an alternative KEM algorithm are the "master standard + redundancy" structure, supplemented by NIST IR 8545 to give the public basis for the fourth round of technology selection, forming a deep system from mandatory standards (FIPS) to evaluation and route guidance (IR/SP) (NIST, 2024a; NIST, 2025); NIST CSRC, 2024). In terms of migration ecology, White House OMB M-23-02 establishes a governance framework based on cryptographic asset inventory-risk classification-replacement-verification-monitoring, and CISA's quantum-ready routing and automated discovery/inventory tool strategy moves migration from an "initiative" to an "initiative". CISA's quantum-ready path and automated discovery/inventory tool strategy pushes migration from "initiative" to "quantifiable and auditable" operations; NCCoE's practice guidelines and reference implementations bring the process down to a "usable and reproducible" engineering toolchain covering the whole chain of collaboration (from government to vendor). NCCoE, on the other hand, uses practice guides and references to realise a "working, reproducible" engineering toolchain that

 doi:10.20944/preprints202508.1741.v1

covers the whole chain from government to suppliers (OMB, 2022; CISA, 2023, 2024; NCCoE, 2023a, 2023b). In contrast, although China has developed more systematic terminology, application and product specifications for QKD/quantum communication and promoted the standardisation of security assessment, the GB/T national standard for PQC algorithms has not yet been publicly released, and a unified migration methodology and tool stack has yet to be established, which makes it difficult to form a policy tool for "mandatory procurement + consistency testing" and cross-domain collaboration (national standard for PQC algorithms, national standard for PQC algorithms, national standard for PQC algorithms, etc.). It is difficult to form a "mandatory procurement + consistency testing" and cross-domain synergy policy grip in the short term (judging from the national standard information public service platform and public announcements). In the dimension of international discourse, if the ISO/IEC level accelerates the adoption of U.S.-dominated algorithmic families and migration methodologies, there will be a chain risk of "passive alignment - passive acceptance of auditing calibre" in the fields of cross-border data compliance, equipment export, and supply chain security. Therefore, China needs to adopt the dual-track strategy of PQC baseline security + QKD enhanced security, complete the GB/T-level PQC standards and migration governance reference architecture as soon as possible, and simultaneously push forward the conformance testing and interoperability validation, so as to avoid being passive in the new round of standards competition (NIST, 2024a; OMB, 2022; CISA, 2023, 2024; NCCoE, 2023a, 2023b). 2023b).

Figure 3 uses data science visualization method to construct a comparison between China and the United States in the process of quantum cryptography standardisation along three main lines: standard level, migration ecology and international discourse.

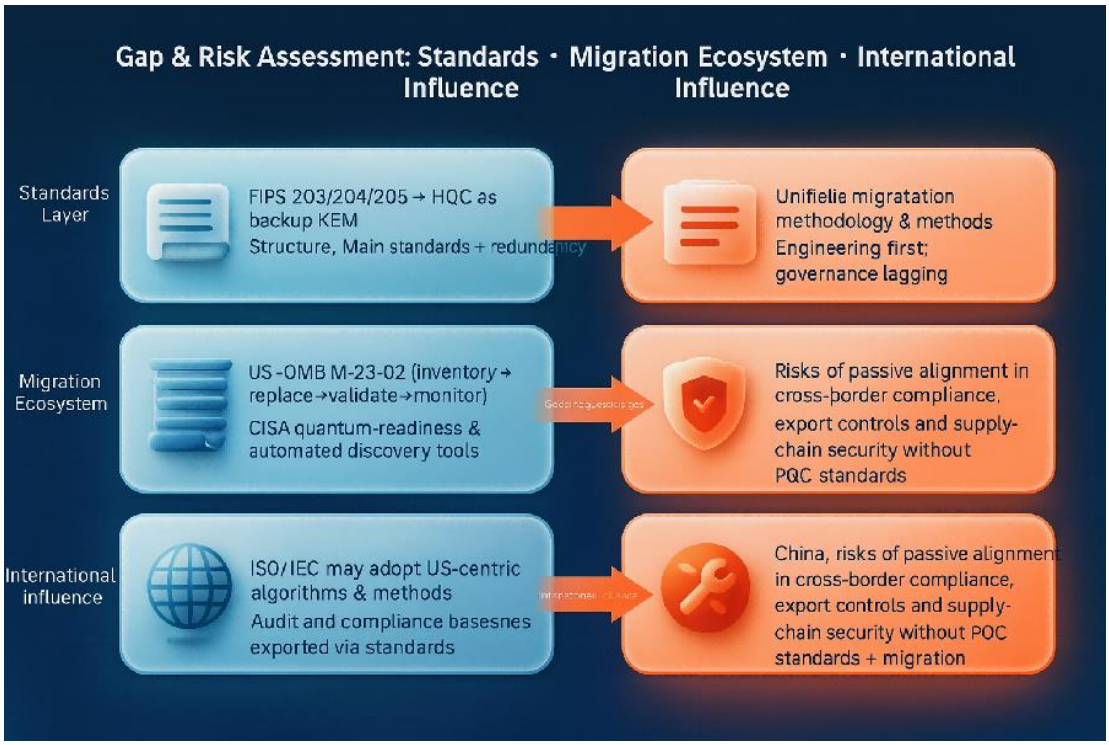

Figure 3. Gap & Risk Assessment: Standards . Migration Ecosystem - International. Illustrated by the author.

Standard level: the United States has completed the official release of FIPS 203/204/205, and identified HQC as the backup KEM through NIST IR 8545, forming a closed-loop structure of "main standard + redundancy"; while China has established a more systematic family of standards at the level of QKD application, terminology and product specification, but the GB/T national standard for PQC algorithm has not yet been released. Although China has established a more systematic standard family at the level of QKD application, terminology and product specification, the GB/T national

 doi:10.20944/preprints202508.1741.v1

standard for PQC algorithm has not yet been released, and there is a risk that the basic standard is missing.

Migration ecology: The United States has taken the White House OMB M-23-02 as the core, combined with the CISA automated inventory tool and the NCCoE practice guide to form a quantitative and auditable migration governance chain of "discovery-replacement-verification-monitoring"; China, on the other hand, still has a QKD governance chain of "detection-replacement-verification-monitoring". China, on the other hand, is still in a situation of engineering first and governance lagging behind, lacking a unified migration tool stack and consistency testing mechanism.

International discourse: The U.S. has strengthened its dominant position in cross-border compliance and supply chain security by pushing ISO/IEC to accept its algorithmic families and methodologies, while China faces the risk of "passive alignment" in terms of standards, compliance, and auditing calibre, which may weaken its discourse in global cryptographic governance.

Overall, the map highlights the structural contrast between US leadership in the closed loop of Standards-Assessment-Migration and China's engineering advantage in QKD and the absence of PQC national standards. The core risk of the gap is that if China fails to complete the PQC standards and migration governance structure within 3-5 years, it will be in a passive position in the international standards competition and security game.

V. China's PQC National Standards and QKD Dual-Track Strategy "3 Years-5 Years-10 Years" Roadmap

Facing the national roadmap of "three years - five years - ten years", it is suggested that China should take the principles of enforceable, auditable, and iterative, and make the three strands of standards engineering, migration governance and internationalisation go hand in hand and resonate at the same frequency:

Stage A (2025Q4-2026Q4, "building standards and setting baselines"), focusing on grid ciphers and coded ciphers, releasing PQC algorithms GB/T (KEM+signature) and consistency test methods, and simultaneously establishing the "main algorithm + backup algorithm" selection and switching. Simultaneously establish the selection and switching mechanism of "main algorithm + backup algorithm" (drawing on the idea of "structural redundancy" of HQC as the backup KEM), and form a "state secret + PQC" hybrid suite for key protocols such as TLS/QUIC/IPsec/5G. At the same time, the state version of the migration roadmap was released, and a closed-loop co-ordination of "asset inventory - risk classification - replacement priority - interoperability - retesting and auditing" was carried out. and Audit" (NIST, 2025; OMB, 2022; CISA, 2023, 2024).

Phase B (2027Q1-2028Q4, "Scale Migration and Verification"), complete "PQC baseline + QKD enhancement" dual-stack deployment in key links such as party and government private networks, central bank clearing/backbone networks, backbone networks of the three major carriers, and grid scheduling, and establish "PQC baseline + QKD enhancement" dual-stack deployment. Dual-stack deployment of "PQC Baseline + QKD Enhancement", establishment of third-party conformance test/certification catalogue and regular mechanism for red-team evaluation; introduction of government procurement list and localisation adaptation list, and promotion of the localisation and performance of hardware and software such as HSM/KMS, crypto cards, accelerators, and other standards.

Stage C (2029Q1-2035Q4, "solidification and internationalisation"), achieve ≥80% scenario migration and regular standby algorithm rehearsal, submit draft standards and interoperability reports for ISO/IEC JTC1/SC27, and build a "PQC+QQC" system. "PQC+QKD" combination programme of the "Belt and Road" overseas channel; the international best practice of FIPS-IR/SP-governance tool chain is used as reference to ensure that the standard level hard constraints and the engineering level are not only the same but also the same. We will use the international best practices of FIPS-IR/SP-governance toolchain as reference to ensure that the hard constraints at the standard level and the soft landing at the engineering level will be taken in parallel, and build a quantum

 doi:10.20944/preprints202508.1741.v1

security base that can maintain its resilience under the iteration of algorithms/evolution of attacks and defences (NIST, 2024a; NIST, 2025; OMB, 2022; CISA, 2023, 2024; NCCoE, 2023).

Table 2. Overall Gantt chart task list for Post-Quantum Cryptography (PQC) migration in China.

Lane	Task	Owner	Start	End	KPI	Milestone	Depends On
Standards	PQC GB/T (KEM v1)	TC260	2025-10-01	2026-09-30	1 standard	✔	-
Standards	PQC GB/T (Signature v1)	TC260	2025-12-01	2026-12-31	1 standard	✔	-
Standards	Conformance test methods v1	SCA	2026-01-15	2026-10-31	1 method	✔	PQC GB/T (KEM v1)
Standards	Backup algorithm policy (selection rules)	SCA	2026-03-01	2026-11-30	policy ready	✘	-
Protocols & PKI	Hybrid suite baseline (TLS/QUIC/IPsec/5G)	MIIT	2025-11-01	2026-09-30	baseline	✔	-
Protocols & PKI	Certificates/keys & Guomi PKI transition spec	PBOC	2026-02-01	2026-10-15	spec	✔	-
Migration Governance	National PQC migration roadmap	SCA	2026-01-01	2026-06-30	roadmap	✔	-

 doi:10.20944/preprints202508.1741.v1

Lane	Task	Owner	Start	End	KPI	Milestone	DependsOn
Scaled Migration	Dual-stack rollout (Gov/Finance/Power/Telcos)	Multi	2027-01-01	2028-12-31	40% links	✕	National PQC migration roadmap
Testing & Certification	Conformity catalog & red-teaming (BAU)	SCA	2027-03-01	2028-12-31	25 rounds/yr	✕	Conformance test methods v1
Procurement & Localization	Gov procurement & localization lists	MOF	2027-04-01	2028-06-30	lists	✔	Conformity catalog & red-teaming (BAU)
Internationalization	≥80% migration / ISO submissions / BRI go-global	TC260	2029-01-01	2035-12-31	≥80% coverage	✕	Phase B complete

Illustrated by the author. ✕ Indicates that the task is marked as a Milestone. ✕ indicates that the task is not a key milestone. The DependsOn column shows the dependencies between tasks.

Figure 4 shows China's quantum security (PQC) roadmap (2026-2036) in a three-five-decade rhythm: the horizontal axis is the years and gates, and the vertical axis is the seven major tracks (standards, protocols and PKI, governance, scale migration, measurement and authentication, sourcing and localisation, and internationalisation); coloured bars indicate start and end, rounded endpoints are milestones, vertical dotted lines are stage gates. phase A (~2026-) completes KEM/Signature v1, compliance testing v1 and alternate algorithmic policies to form a measurable and verifiable baseline; phase B (~2027-2030) drives TLS/QUIC/IPsec/5000 with a hybrid baseline. QUIC/IPsec/5G and state secret PKI transition with hybrid baseline, implement dual-stack and grey scale switching in government, gold, energy and credit industries, and construct regulatory admissible evidence with conformance catalogue + red team confrontation; Phase C (about 2031-2036) promote international landing and mutual recognition of ISO/ITU/BRI on the basis of completion of migration of ≥80% of key assets. The key reliance is "standard + PKI → scale migration → measurement and evaluation closed loop → internationalisation", with procurement localisation and supply chain maturity pulling each other; acceptance and operation are based on coverage (PQC ratio / dual-stack ratio), quality (conformance pass rate / interoperability success rate), security (red team discovery rate / zero major accidents) and internationalisation (international standard pass rate and number of cross-border projects). Internationalisation (international standard adoption and number of cross-border projects) are the core KPIs; major risks include algorithmic divergence, legacy system modification, supply chain and compliance, performance and latency, which are controlled by alternate algorithms and bridging, dual-stack/gateway transition, cataloguing and verifiable BOMs,

 doi:10.20944/preprints202508.1741.v1

protocol tuning and hardware acceleration. The diagram is used for quarterly review and milestone decision making across ministries, regulatory and operational ecosystems.

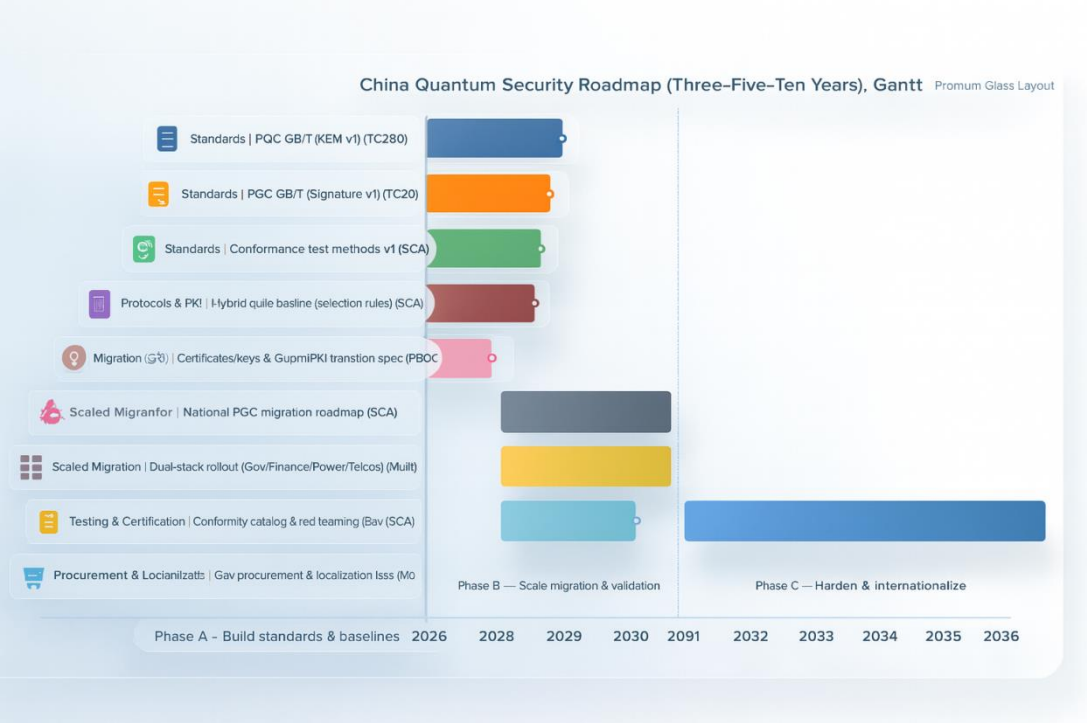

Figure 4. China Quantum Security Roadmap (Three-Five-Ten Years): Gantt - Clean Layout. Illustrated by the author.

Table 3. KPI Matrix (example, for supervision and appraisal).

dimension (math.)	2026	2027	2030
Issuance of PQC GB/T Quantity (KEM / Signature / Test)	≥2 / ≥1 / ≥1	1 round of revisions completed	Formation of a series of families
Asset Inventory Coverage (SS/Kwanji)	60 %	85 %	100 %
Focused Link Dual Stacking (PQC+QKD)	15 %	40 %	70 %
Domestic equipment through the consistency of the proportion of certification	30 %	60 %	80 %+
Number of interoperability tests (cross-vendor / cross-domain)	10	25	50

 doi:10.20944/preprints202508.1741.v1

dimension (math.)	2026	2027	2030
Alternate Algorithm Annual Exercise	1	2	2+

Illustrated by the author. Note: KPIs are policy objectives and do not require external citations; acceptance is based on national/industry testing agency reports.

VI. Governance Structure and Division of Responsibilities

In order to support the national migration project of "PQC Baseline + QKD Enhancement", it is recommended to build a five-level governance structure of "Central Leadership - Technical Accounting - Industry Supervisors - Implementation Subjects - Scientific Research Support". A five-tier governance structure of "central leadership - technical reporting - industry supervisor - implementation body - scientific research support" is proposed to be constructed, and a three-tier coupling of statutory responsibilities, standardisation reporting and assessment and certification is proposed to achieve enforceability and auditability: at the leadership level, the State Cryptography Administration (SCA) coordinates the top-level design of the national standards for PQC, government procurement and certification catalogue, and the assessment of the commercial cryptographic use and application of key information infrastructure. At the lead level, SCA coordinates the top-level design of PQC national standards, government procurement and certification catalogue, assessment of commercial cryptographic use and application for critical information infrastructure, etc., relying on the "unified leadership and hierarchical responsibility" system and departmental authority established by the Cryptographic Law, and forming an engineering and implementation mechanism with the Administrative Measures for Security Assessment of Commercial Cryptographic Applications and Administrative Measures for Commercial Cryptographic Testing Institutions (SCA, 2020; CNG.com, 2019; CNG.com, 2023; SCA, 2023). Administration, 2023; China.gov.cn, 2023). At the technical reporting/coordination level, TC260 (network security) and TC485 (communications) constitute the "dual reporting" of algorithms, protocols and interoperability standards, with the former being responsible for the coordination of national standards related to network security and cryptographic applications, and the latter being responsible for the communications network, basic protocols and test methods under the operational guidance of the Ministry of Industry and Information Technology. The former is responsible for the coordination of national standards related to network security and cryptographic applications, while the latter is responsible for communication networks and basic protocols and test methods under the operational guidance of the Ministry of Industry and Information Technology, forming a closed loop of standardisation that is connected with engineering protocol stacks and interoperability tests (National Technical Committee for Network Security Standardization, n.d.; National Public Service Platform for Standard Information, n.d.-a). The SCA is in charge of the industry, the MIIT is responsible for the regulation and implementation of industry standards in the field of communication and information technology, the CAC is responsible for data security and network content/platform compliance, and leads the sectoral coordination of commercial cryptography, and the People's Bank of China (PBoC) is responsible for financial infrastructures and key payment and clearing scenarios, forming a "regulation-standard-standard-standardisation loop" with the SCA in terms of policy and regulatory indicators. The three parties form a "regulation-standard-assessment" linkage in terms of policy and regulatory indicators with the SCA (State Council, 2008; State Internet Information Office, 2014; Standing Committee of the National People's Congress (NPCSC), 2021; State Internet Information Office, 2025; People's Bank of China (PBOC), 2025). At the implementation level, the People's Bank of China (PBOC) of the National People's Congress (NPC), with the three major telecommunication operators, the State Grid, core banking and clearing institutions, and key equipment and security vendors as the main bodies, promotes the process of "discovery-grading-replacement-verification-retesting". In the implementation layer, the three major telecom operators,

 doi:10.20944/preprints202508.1741.v1

the State Grid, core banking and clearing institutions, and key equipment and security vendors are mainly involved in the "discovery-grading-replacement-verification-retesting" process to promote the migration of versioning, and the certification catalogue of commercial cryptographic products and the directory of testing institutions are embedded in the government procurement and access, so as to achieve a quantifiable audit of the consistency and interoperability (National Cryptography Administration, 2020; National Cryptography Administration, 2024). In the scientific research support layer, universities, institutes and laboratories will undertake tasks such as formal verification, side channel and implementation security assessment, which will be undertaken by qualified testing/assessment organisations and industry test platforms, so as to open up the "standard-implementation-measurement and assessment" verification chain and provide iterative evidence to the upstream. Through qualified testing/assessment institutions and industry test platforms, the "standard-implementation-assessment" verification chain will be opened up and iterative evidence will be provided to the upstream, so that a normalised operation mechanism of "controllable top-level governance, auditable engineering migration, and traceability of the supply chain" can be formed under the national rule of law framework and standardisation system (China.gov.cn, 2019; State Cryptography Administration of China (SCA), 2023).

Figure 5 compresses the national migration governance of "PQC baseline + QKD enhancement" into an observable-verifiable-auditable causal chain: a five-tier governance stack at the top defines the central lead (SCA, regulatory/procurement/certification catalogue), the technical focal point (TC260/TC485, solidifying regulatory requirements into GB/GB-T and interoperability methods), industry authorities (MIIT/CAC/PBOC/SAC, scenario-based regulation for 5G core network, data security and payment clearing), and implementation entities (telecom operators/State Grid/core banking and clearing/OEM & HSM vendors, by (telecom operators/national grid/core banks and clearing/ OEMs & HSM vendors, promoting dual-stack migration according to "discovery → grading → replacement → verification → retesting"), and scientific research support (universities/laboratories/qualified testing and assessment organisations, undertaking formal validation and side-channel assessment); the central triple-coupling will merge regulation - standard - assessment/certification into a closed loop, avoiding "paper-based" regulation. The middle three lines of coupling merge regulation-standard-assessment/certification into a closed loop, avoiding the disconnection between "paper compliance" and "engineering reality"; the lower left implementation lane outputs auditable products (interoperability matrix, certificates/device IDs, and red-team reports); the middle and lower RACI matrices bind key tasks and roles into a single point of accountability; and the lower right approval and escalation processes provide a normalised path of approval and escalation. Approval and escalation processes provide standing paths and event branches (crypto agility: template switching → policy issuance → group rotation → regression testing), and the far right TRL x GRL federated instrumentation serves as a quantitative adjudicator for Stage Gate. Suggested hard thresholds: interoperation coverage ≥95%, handshake success rate ≥99.95%, latency increment ΔLatency ≤5%, certificate/key rotation SLA ≤24h, side channel and constant time/memory security compliance = 100%, red team high-risk defects shutdown and loop closure in ≤14 days, median authentication cycle ≤30 days, government catalogue coverage of key assets ≥90%, annual emergency response The Gate release condition is TRL ≥ 7 and GRL ≥ 7, and the quarterly trend is determined by the leading indicators (Audit Pass Rate, Defect Density, Patch MTTP, Interoperability Regression Failure Rate), and once any of the indicators falls below the threshold, the escalation branch is triggered and the version flow is frozen. As a result, a minimum sufficient path of "regulatory positioning → standard solidification → evaluation and evidence collection → scale deployment → international mutual recognition" is formed from top to bottom in the diagram, and the governance side and engineering side are aligned with the verifiable evidence chain to ensure low-risk and traceable nationwide PQC migration under the prerequisite of statistically verifiable and regulatory admissibility.

 doi:10.20944/preprints202508.1741.v1

Figure 5. China PQC+QKD Governance & Roles (2026–2036). Illustrated by the author.

VII. Technical Baseline

In order to ensure China's rapid landing, auditability and scalability on the dual-track route of "PQC Baseline + QKD Enhancement", the technical baseline should be synergistically promoted in the five directions of protocols, PKI/Key Infrastructure, realisation of security, testing and certification, and contingency planning: First, on the protocol side, develop a hybrid state secret + PQC suite of "signature + key negotiation dual-track" for the interfaces of IPsec/IKEv2 and 5G core network (e.g. PQC KEM in the handshake phase to complete the meeting with PQC), Firstly, on the protocol side, a hybrid suite of state secret + PQC with "dual route of signature + key negotiation" is formulated for TLS 1.3/QUIC, IPsec/IKEv2 and 5G core network interfaces (e.g., the handshake phase completes the establishment of the session key with PQC KEM, while maintaining the state secret signature/digest chain to safeguard the regulation and compatibility), and interoperability and fallback strategies are given to support the phased replacement; secondly, the PKI/key infrastructure should be used to implement security, test and certification, and emergency plan. Second, on the key infrastructure side, update the X.509 certificate template and certificate chain to support the composite/mixed configuration of "PQC public key + state secret chain of trust", and clearly define the classification of confidentiality lifetimes of high-value data and the key rotation cycle to meet the requirements of the "Intercept first, decrypt later" threat model. "Third, on the security side, establish a three-in-one verification route of "open source reference implementation + formal verification + side channel assessment", and promote the parallel development of hardware acceleration and domestic cryptographic libraries, such as cryptographic cards/HSMs/DPUs. hardware acceleration and parallel adaptation of domestic cryptographic libraries, strict constant-time and memory security baselines, and implementation of the principle of giving priority to realisation-side security over pure algorithmic security. Fourth, on the testing and certification side, we have formed three types of baselines for consistency/performance/interoperability and a cross-domain interconnection test network, and we have carried out red-team confrontation and regression testing, so as to open up the "standard-implementation-measurement-assessment-government-procurement" and the "standard-implementation". -Fifth, on the side of the plan, the crypto agility and one-key switching mechanism of "main algorithm + backup algorithm" are established: when there is an academic breakthrough or

 doi:10.20944/preprints202508.1741.v1

engineering vulnerability in the algorithm or implementation, the crypto agility mechanism will be used to ensure that the algorithm can be used to achieve the desired results. When there are academic breakthroughs or engineering vulnerabilities in the algorithms or implementations, we can refer to NIST's positioning of HQC as a KEM backup solution and IR 8545's technical justification, and complete rapid rolling upgrade and certificate/policy synchronisation (NIST, 2025; NIST IR 8545, 2025). The above baseline is compacted in the order of protocol-PKI-implementation-measurement-programming, and the "engineering readiness (TRL)" and "governance readiness (GRL)" are integrated into the baseline. The above baseline is compressed in the order of protocol-PKI-implementation-measurement-preparedness to quantify the "project readiness (TRL)" and "governance readiness (GRL)", thus transforming the policy goal into a national migration project that can be observed, accepted, and traced (OMB, 2022; CISA, 2023; NIST, 2025).

Figure 6 compresses the "PQC+QKD technical baseline (2026-2036)" from a strategic narrative into an observable, acceptable and traceable engineering-governance double closed loop: the three cards in the top row give the overall blueprint → protocol handshake → realisation of the secure "Causal Master Chain", i.e., take Phase A standard and baseline freeze as prerequisite (milestone and dependency arrows), establish dual-track handshake of session key + state-secret signature/digest compliance through PQC KEM at TLS1.3/QUIC, IPsec/IKEv2, 5G interfaces, and built-in Fallback and interoperability branching; synchronised with the trinity of "open source reference implementation - formal verification - side channel evaluation" to constrain constant time and memory security, HSM/DPU acceleration and CI/CD security integration, reducing implementation deviation and latency inflation from the source. deviation and latency inflation from the source.

Figure 6. China PQC+QKD Technical Baseline (2026-2036). Illustrated by the author.

The four cards in the bottom row graft governance readiness (GRL) to engineering readiness (TRL): hybrid X.509 certificate chain specifies composite templates of PQC public key + state secret trust anchors, rotation cycle and secrecy life level (KL-1/3/5); cross-domain test network covers six domains of Gov/Finance/Power/Telcos/Cloud/IoT, with three-layer channelisation by consistency/performance/interoperability. Cross-domain test network with Gov/Finance/Power/Telcos/Cloud/IoT six domain coverage, aligning KPI tables (throughput, latency,

 doi:10.20944/preprints202508.1741.v1

handshake success rate, and interoperability matrix coverage) by consistency/performance/interoperability tiers, providing statistical efficacy and regression baseline for Phase B scale-up and validation; "Crypto-Agile" state machine combines Primary ↔ Backup (e.g., HQC) with triggers (academic breakthrough/vulnerability/compliance update). The "Crypto-Agile" state machine combines Primary↔Backup (e.g., HQC) and trigger conditions (academic breakthroughs/fragile/compliance updates) into a template switching-policy issuance-group rotation-regression testing pipeline to ensure that security degradation and rapid recovery are completed within the RTO/RPO targets in case of anomalies. The joint dashboard drives Gate decision and quarterly review with single-point readings, supplemented by four mini-dials (Coverage/Quality/Security/Internationalisation) to achieve one-screen observation. On the data side, it is recommended to use the causal on-line path of canary → grey scale → dual stack diversion in conjunction with red team confrontation + interoperability regression, and set the hard thresholds: handshake success rate ≥ 99.95%, latency increment ΔLatency ≤ 5%, certificate rotation SLA ≤ 24h, interoperability matrix coverage ≥ 95%, constant time/memory security compliance = 100%, and side channel leakage power lower than the bottom noise of the device by 3σ; on the governance side, the hard thresholds: key assets, key assets, key assets, key assets, and key assets, and key assets. Side hard thresholds: critical asset coverage ≥ 80% (Phase C initiation line), international standard submissions/passes vs. cross-border projects ladder compliance. As a result, a minimum sufficient path of "Standard/PKI→Protocol→Implementation→Assessment→Agile Plan→Threshold Acceptance→Internationalisation" has been formed from the top down in the diagram: as long as the KPIs cross the Gate line consecutively and there is no regression in the regression test, it can be judged that the phase has been completed and advanced to the next phase, so as to realise the national PQC migration on the premise of statistically provable and regulatory admissibility. This enables national PQC migration to be carried out on a low-risk scale under the premise of statistical evidence and regulatory acceptance.

VIII. Key Risks and Responses

For the "PQC Baseline + QKD Enhancement" national level implementation, the four types of systemic risks need to set up "implementable and auditable" countermeasures simultaneously.

Algorithm/implementation uncertainty: Take the crypto-agile framework of "main algorithm + backup algorithm" as the base, establish annual red team drills and rapid rollback/switchover plans; refer to the U.S. use of HQC as a KEM backup bit and disclose the technical trade-offs with NIST IR 8545, and form the evidence-based replacement thresholds and triggering conditions (NIST, 2025). NIST, 2025).

Performance and bandwidth consumption: Follow the engineering path of "compatibility first, optimisation later" at the protocol and system integration level, evaluate CPU/memory/bandwidth overheads for handshake and session phases, introduce hardware acceleration and batch queues such as HSM/crypto cards/DPUs, and support automated discovery-baseline validation tools. Asset Inventory - Baseline Verification tool chain, to put OMB's hard constraints on Federal agencies' Cryptographic Asset Inventory and CISA's quantitative migration path/automated discovery tool strategy into process SLO/SLA (OMB, 2022; CISA, 2023, 2024; NCCoE, 2023).

Patents and Export Controls: Pre-built IP pools and domestic substitution lists around SEP/FRAND and encryption export controls (EAR 15 CFR Cat.5 Pt.2), organising domestic implementations and reference stacks within compliance boundaries to reduce licensing uncertainty and cross-border supply chain risks (BIS, 2021; WIPO, n.d.).

International interoperability: Align the interface and test methods of ISO/IEC JTC 1/SC 27, lead multinational interoperability tests, and carry out cross-vendor and cross-domain validation of de facto standards such as FIPS 203/204/205, so as to shorten the closed-loop path of "national standard - international standard - industrial application" and reduce the risk of licensing uncertainty and cross-border supply chain risks. This will shorten the closed-loop path of "national standard -

 doi:10.20944/preprints202508.1741.v1

international standard - industrial application" and reduce technical trade barriers (NIST, 2024; CISA, 2023).

IX. Discussion

Based on the chain of evidence formed by the uploaded text, this study has made two "most important findings" of ethical and national security significance: first, PQC is the "basic line of defence" in the quantum era, which can provide a minimum dependable security baseline for long-life data and critical information infrastructure; second, QKD is the "enhanced line of defence" for key high-value links, which is used to overlay the backbone in scenarios such as party, government, military, finance, power and carrier backbone. First, PQC is the "basic line of defence" in the quantum era, which can provide a minimum reliable security baseline for long-life data and critical information infrastructure; second, QKD is the "enhanced line of defence" for critical high-value links, which is used to overlay the bottom line in scenarios such as party, government, military, finance, power and carrier backbone, thus forming a "dual-track security" (PQC baseline + QKD enhanced) overall architecture (NIST, 2020). The overall architecture is "dual-track security" (PQC baseline + QKD enhancement) (NIST, 2024a; NIST, 2025; OMB, 2022; CISA, 2023). The U.S. has basically completed the "standards-migration-ecology" closed loop: FIPS 203/204/205 and HQC backup algorithms to build the "master standard + redundancy", supplemented by the governance of OMB and CISA. In contrast, China is leading in QKD engineering and standards, but there are shortcomings in PQC's national standards and migration governance capabilities, which will lead to passivity in international interoperability and supply chain compliance if they are not completed within the time window of "three years to build standards, five years to solidify them" (NIST, 2024a; NIST, 2025; OMB, 2022; CISA, 2023).

OMB M-23 -02 emphasises the governance line of "asset inventory - risk classification - replacement - validation - monitoring", and CISA's quantitative migration route and automated discovery tools advance the migration from an "initiative" to an "initiative". CISA's quantitative migration path and automated discovery tools move the migration from "initiative" to "auditable" engineering operations, which is structurally aligned with the national version of the migration roadmap (Asset Inventory-Interoperability-Review & Audit Closed Loop) proposed in this paper (NIST, 2020). This is highly consistent with the structure of the national version of the migration roadmap (Asset Inventory-Interoperability-Re-test and Audit Closure) proposed here (NIST, 2025; OMB, 2022; CISA, 2023/2024).

In the theoretical sense, although this study focuses on policy and engineering, it still proposes two framework contributions that can be discussed in the academic community: first, the dual-track model of "PQC baseline-QKD enhancement", which maps communication requirements with different confidentiality lifetimes and business values to differentiated defences, and "primary standard + backup standard" to improve system resilience; second, the coupled metric of "TRL × GRL" (engineering readiness × governance readiness), which advocates the integration of standards into the system. Second, the "TRL × GRL" coupling metric (engineering readiness × governance readiness) is proposed, which advocates the integration of standard maturity, tool chain completeness, compliance and audit capabilities into the same metric space to avoid "standards are out, governance readiness is in". Avoid the disconnect of "standards are out, governance is not yet in place".

Regarding the findings that are inconsistent or only partially consistent with the original assumptions: we originally assumed that China could achieve "dual maturity" of national standards and migration toolchain at both the QKD and PQC ends simultaneously; the actual evidence shows that the PQC algorithm GB/T has not yet been publicly released, and that a unified migration methodology and toolchain has not yet been developed, resulting in "Practical evidence shows that the PQC algorithm GB/T has not yet been publicly released, and the unified migration method and tool stack have not yet been established, which makes it difficult to form the policy grip of "mandatory procurement + conformance testing" in the short term. 2024a; CISA, 2023/2024).

 doi:10.20944/preprints202508.1741.v1

The limitations of the study are mainly reflected in three aspects: first, the evidence is mainly based on public standards and authoritative announcements, which is difficult to cover confidential or in-process research calibres and may underestimate the maturity of some domestic in-process research results; second, international standards and industry ecology will still evolve rapidly between 2025-2028, and the conclusions of this study are time-sensitive and context-dependent; third, the thresholds in KPIs and roadmaps are policy recommendation calibres, but caution is needed when extrapolating them. Third, the thresholds in the KPIs and roadmap are policy recommendations, and although they have auditable intent, they have not been empirically tested on a large cross-section of industries, so extrapolation should be done with caution.

Recommendations for further research: In the short term, three types of work should be carried out: (1) Cross-domain comparative experiments on consistency, performance, and interoperability to establish reproducible baseline datasets and test networks; (2) Focusing on protocols such as TLS/QUIC, IKEv2, and 5G core networks, establish reference implementations and formal verification for "national cryptography + PQC" hybrid suites, accompanied by side-channel assessments and hardware acceleration adaptation; (3) Establish an annual red team exercise and rapid switching mechanism for "primary algorithm + backup algorithm," and formalize it as engineering terms for government procurement and access. In the medium term, it is recommended to complete the large-scale migration of "dual stacks (PQC baseline + QKD enhancement)" on key links such as party and government dedicated networks, central bank clearing/backbone networks, operators, and power dispatch, and form a routine quality closed loop with third-party consistency testing/red team evaluation.

The significance of this initiative for professional practice and application lies in the following: it proposes an actionable "three-year–five-year–ten-year" national roadmap and responsibility chain (led by SCA, overseen by TC260/TC485, and implemented by the Ministry of Industry and Information Technology/ Cyberspace Administration of China/People's Bank of China division of labor, implementation by operators and State Grid, and support from universities and research institutes), and transforms policy objectives into observable, verifiable, and traceable engineering practices through a "government procurement list + testing and certification directory + interoperability test network"; simultaneously, through "international interoperability testing + ISO/IEC submission," the closed-loop process from "national standards to international standards to industrial applications" is accelerated, enhancing China's international influence and supply chain leadership in the quantum era (TC260, 2024/2025; SAMR, 2023/2024).

X. Conclusion

In an era of rapidly approaching quantum computing threats, China must establish clear conclusions and strategic approaches from a national security standpoint. Post-quantum cryptography (PQC) should be regarded as the "basic line of defence" in the quantum era, which is meant to provide a minimum dependable security baseline for critical information infrastructures and long-life data; at the same time, quantum key distribution (QKD) should be used as the "enhanced line of defence" for high-value links such as party, government, military, financial and power communications. Meanwhile, quantum key distribution (QKD) is used as an "enhanced line of defence" to reinforce and underpin high-value links such as party, government, military, finance and power communications. The U.S. has taken the lead in completing the closed-loop layout of standard-migration-ecology: with FIPS 203/204/205 and HQC backup algorithm as the core to form the specification system of "main standard + redundancy", supplemented by the mandatory migration led by OMB and CISA. In addition, OMB and CISA are leading the mandatory migration and toolchain landing to drive the comprehensive transformation of the industrial chain and supply chain (NIST, 2024a; NIST, 2025; OMB, 2022; CISA, 2023). In contrast, although China maintains global leadership in QKD engineering and standardisation system, there is a significant lag in PQC national standard system and migration governance capability (SAMR, 2023/2024; SCA, 2021; TC260, 2024/2025).

 doi:10.20944/preprints202508.1741.v1

Therefore, from the perspective of national security strategy, the conclusion should be clear: China must accelerate the construction of the PQC national standard system and the whole chain migration governance mechanism within the timeframe of "three years to build the standard, five years to solidify it, and ten years to internationalise it", and form a dual-track integration with the existing QKD national standard group. This is not only about the long-term security of national confidential data and the resilience of the base, but also directly related to China's initiative in international standard-setting and technological discourse competition. If delayed, China will passively align itself with the U.S. in terms of standards adoption, industrial ecology, cross-border data compliance and supply chain security, and lose the strategic opportunity. Therefore, immediately launching the "PQC National Standard Project" and promoting it in coordination with the QKD standard system is an inevitable choice to ensure national security, industrial security and international strategic interests in the quantum era.

References

Bureau of Industry and Security. (2021, March 29). *Encryption and Export Administration Regulations (EAR).* https://www.bis.doc.gov/index.php/policy-guidance/encryption

CCSA/SAMR. (2021, March 5). *YD/T 3834.1-2021 量子密钥分发(QKD)系统技术要求 第1部分：基于诱骗态BB84协议的QKD系统* [Technical requirements for QKD systems—Part 1: Decoy-state BB84-based QKD]. 全国标准信息公共服务平台. https://std.samr.gov.cn/hb/search/stdHBDetailed?id=C362B3DB621BA067E05397BE0A0A1ED8

Cyberspace Administration of China. (2014, August 1). *国家互联网信息办公室职责* [Functions of the Cyberspace Administration of China]. https://www.cac.gov.cn/2014-08/01/c_1111903999.htm

Cyberspace Administration of China. (2025, July 1). *关键信息基础设施商用密码使用管理规定* [Administrative provisions on the use of commercial cryptography in critical information infrastructure]. https://www.cac.gov.cn/2025-07/01/c_1753083518894995.htm

Cybersecurity and Infrastructure Security Agency. (2023, August 21). *Quantum-readiness: Migration to post-quantum cryptography.* https://www.cisa.gov/resources-tools/resources/quantum-readiness-migration-post-quantum-cryptography

Cybersecurity and Infrastructure Security Agency. (2024, September 26). *Strategy for migrating to automated PQC discovery and inventory tools* (PDF). https://www.cisa.gov/sites/default/files/2024-09/Strategy-for-Migrating-to-Automated-PQC-Discovery-and-Inventory-Tools.pdf

Federal Register. (2024, August 14). *Announcing issuance of Federal Information Processing Standards (FIPS): FIPS 203/204/205.* https://www.federalregister.gov/documents/2024/08/14/2024-17956/announcing-issuance-of-federal-information-processing-standards-fips-fips-203-module-lattice-based

ISO/IEC JTC 1/SC 27. (n.d.). *Information security, cybersecurity and privacy protection.* https://www.iso.org/committee/45306.html

National Cybersecurity Center of Excellence. (2023a, August). *Migration to post-quantum cryptography (PQC) – Fact sheet.* National Institute of Standards and Technology. https://www.nccoe.nist.gov/sites/default/files/2023-08/mpqc-fact-sheet.pdf

National Cybersecurity Center of Excellence. (2023b, December 19). *SP 1800-38B (preliminary draft): Crypto agility considerations—Migrating to post-quantum cryptographic algorithms* (PDF). National Institute of Standards and Technology. https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf

National Cybersecurity Center of Excellence. (2023). *Crypto agility considerations: Migrating to post-quantum cryptographic algorithms (Project page; includes SP 1800-38 resources).* National Institute of Standards and Technology. https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

National Information Security Standardization Technical Committee (TC260). (n.d.). *首页与标准化工作信息* [Homepage and standardization work information]. https://www.tc260.org.cn/

 doi:10.20944/preprints202508.1741.v1

National Public Service Platform for Standards Information. (n.d.-a). *TC485 全国通信标准化技术委员会* [TC485 National Technical Committee on Communications Standardization]. https://std.samr.gov.cn/search/orgDetailView?tcCode=TC485

National Institute of Standards and Technology. (2024, August 13). *NIST releases first 3 finalized post-quantum encryption standards (FIPS 203/204/205).* https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

National Institute of Standards and Technology. (2025, March 11). *NIST selects HQC as fifth algorithm for post-quantum encryption.* https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

National Institute of Standards and Technology. (2025, March). *NIST IR 8545: Status report on the fourth round of the NIST post-quantum cryptography standardization process* (PDF). https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8545.pdf

NIST CSRC. (2024, August 13). *Post-quantum cryptography FIPS approved.* Computer Security Resource Center. https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved

NIST CSRC. (2025). *Post-Quantum Cryptography Standardization (including NIST IR 8545 and HQC selection information).* https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

Office of Management and Budget. (2022, November 18). *M-23-02: Migrating to post-quantum cryptography* (PDF). Executive Office of the President. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

People's Bank of China. (2025). *Order No. 2 [2025] of the People's Bank of China …* https://www.pbc.gov.cn/en/3688253/3689009/4180845/5741155/index.html

SAMR. (2023). *GB/T 42829-2023 量子保密通信应用基本要求* [Basic requirements of quantum secure communication applications]. 国家标准信息公共服务平台. https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=867AE36ABF49F8013D496C24437222A8

SAMR. (2024). *GB/T 43692-2024 量子通信术语和定义* [Quantum communication terminology and definition]. 国家标准信息公共服务平台. https://std.samr.gov.cn/gb/search/gbDetailed?id=14156507D16E0337E06397BE0A0AE656

State Council of the People's Republic of China. (2008, July 17). *工业和信息化部职责、内设机构和编制规定（全文）* [Functions, internal organs, and staffing of the Ministry of Industry and Information Technology]. https://www.gov.cn/zfjs/2008-07/17/content_1048292.htm

State Cryptography Administration. (2020, January 21). *密码政策问答（十五）* [Cryptography policy Q&A (No. 15)]. https://www.oscca.gov.cn/sca/xxgk/2020-01/21/content_1060613.shtml

State Cryptography Administration. (2020, May 11). *商用密码产品认证目录（第一批）* [Catalogue of commercial cryptography product certification (first batch)] [PDF]. https://www.oscca.gov.cn/sca/xwdt/2020-05/11/1060749/files/2dafffd5b75d4e25aab610f357bb5ec9.pdf

State Cryptography Administration. (2021, October 19). *GM/T 0108-2021 诱骗态 BB84 量子密钥分配产品技术规范* [Decoy-state BB84 quantum key distribution product specification]. https://www.oscca.gov.cn/sca/xxgk/2021-10/19/content_1060886.shtml

State Cryptography Administration. (2023, October 7). *商用密码检测机构管理办法（国家密码管理局令第 2 号）* [Administrative measures for commercial cryptography testing institutions (SCA Order No. 2)]. https://www.oscca.gov.cn/sca/xxgk/2023-10/07/content_1061108.shtml

State Cryptography Administration. (2024, November 11). *国家密码管理局公告（第 49 号）* [Announcement No. 49 of the State Cryptography Administration]. https://www.oscca.gov.cn/sca/xwdt/2024-11/11/content_1061214.shtml

The Central People's Government of the People's Republic of China. (2019, October 27). *中华人民共和国密码法* [Cryptography Law of the People's Republic of China]. https://www.gov.cn/xinwen/2019-10/27/content_5445395.htm

 doi:10.20944/preprints202508.1741.v1

The Central People's Government of the People's Republic of China. (2023). *国家密码管理局令（第3号）商用密码应用安全性评估管理办法* [SCA Order No. 3: Administrative measures for the security assessment of commercial cryptography applications]. https://www.gov.cn/gongbao/2023/issue_10846/202311/content_6917320.html

World Intellectual Property Organization. (n.d.). *Standard-essential patents (SEPs).* https://www.wipo.int/en/web/patents/topics/sep