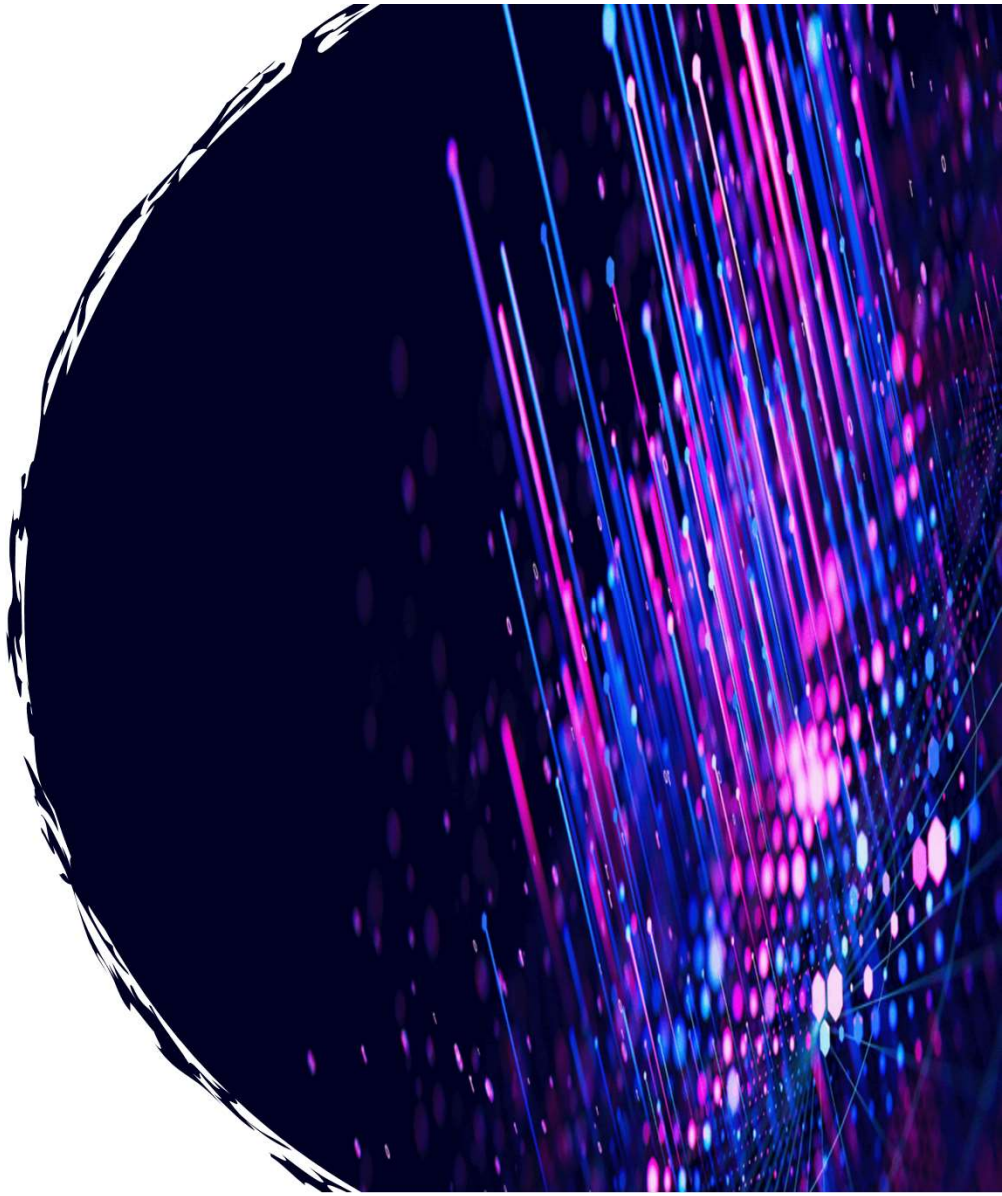
ETSI/IQC Quantum Safe Cryptography Conference 2026

PQC Migration in China's Bank Industries

Jintai Ding Jintai.Ding@xjtlu.edu.cn

Hong Xiang xianghong@cqu.edu.cn



National Key R&D Projects on PQC migration in China

PQC migration on banking industry

On December 13, 2023, China's Ministry of Science and Technology has approved a "National Key Research and Development Plan", called "**The Research on PQC Migrations for banking and its critical infrastructure information systems**"

- **3 goals:** This program attempts to study (1) the regulatory/policy initiatives; (2) general technologies, and (3) migration solutions for the banking industry in China
- **5 sub-program:** This program comprises **five sub-programs**: (1) Framework of migration and its key technologies; (2) Efficient and secure hardware and software implementation; (3) The protocols of PQC migration; (4) Migration evaluations and regulation standards of governments; (5) The development of integration platform for validation and test of PQC migration
- **10 participants:** This program is under the cooperation of ten institutes / commercial banks, including the Research Institute of the People's Bank of China (**Leading Institute**), China Construction Bank, etc.

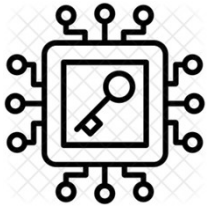
ETSI/IQC Quantum Safe Cryptography Conference 2026

Target 1: Regulatory & Policy

- Research on **risk control and regulatory & policy standards** for Post-quantum Cryptography migration with the banking industry in China

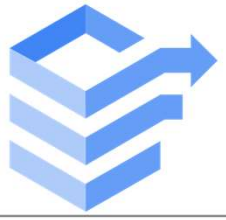
Target 2: General Technologies

- Overcoming **general key technologies** applicable to Post-quantum Cryptography migration in banking information systems



Target 3: Migration Solution

- Establish a secure and reliable Post-quantum Cryptography **migration solution** for China's banking information system



ETSI/IQC Quantum Safe Cryptography Conference 2026

Topic 1: Key Technologies

- Complexity Analysis of Security of Key PQC algorithms and security tools

Our focus mostly on security of lattice schemes – Practical Security Analysis

Shortest Vector Problem – SVP

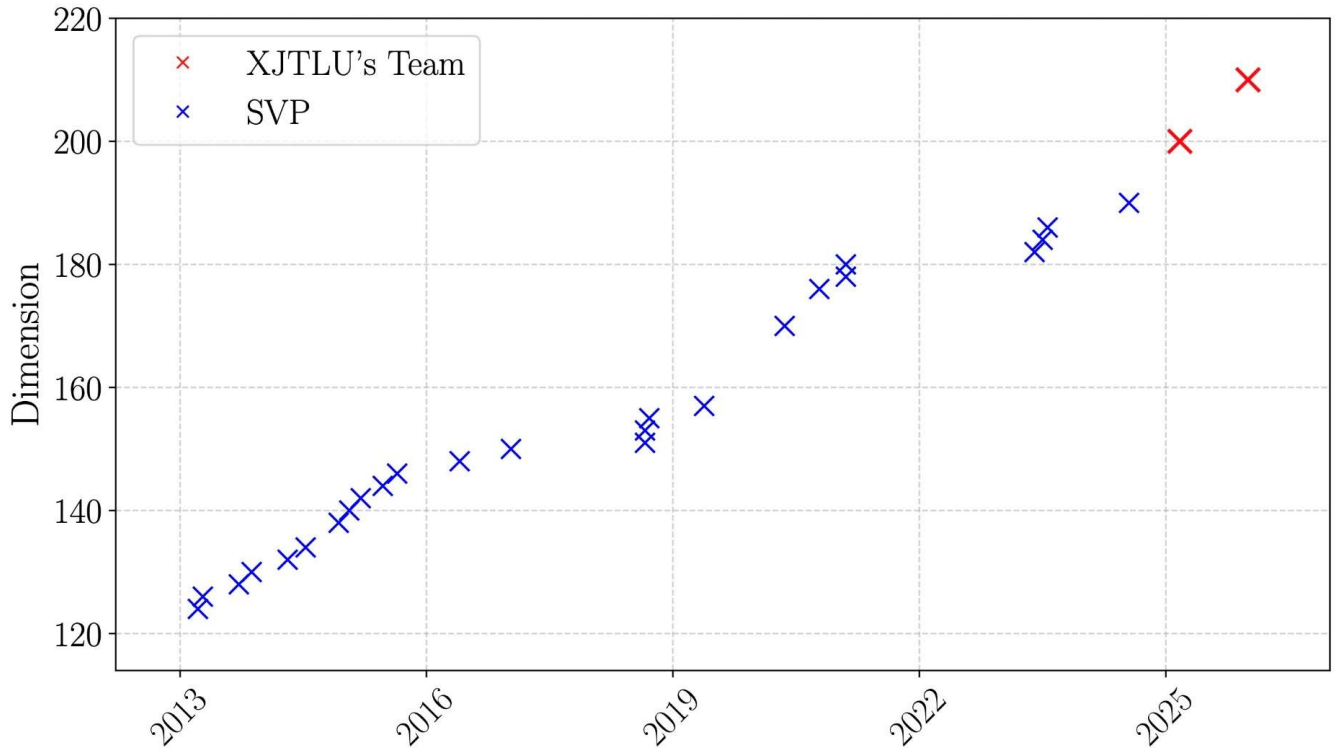
We solve both Darmstadt Challenges:

SVP 200 (2025) and SVP 210 (2026). Eurocrypt 2026

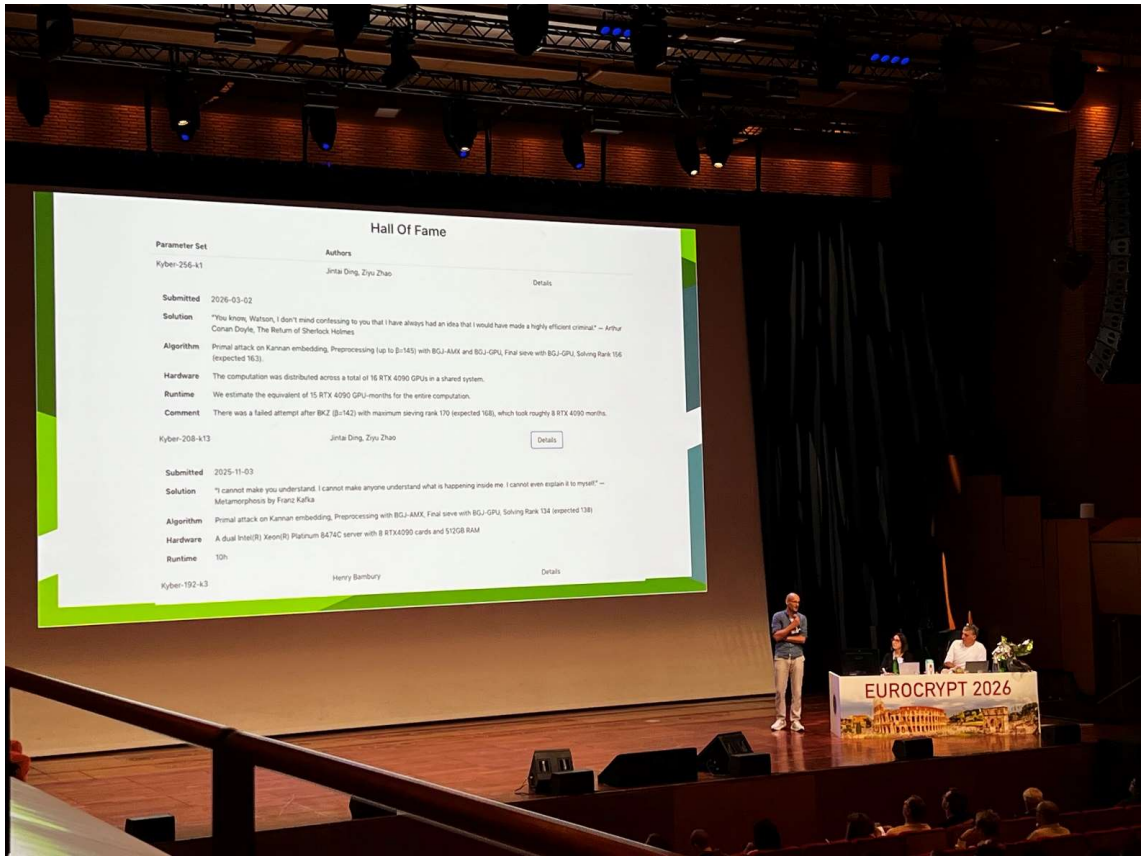
Kyber 208 (2025) and 256 (2026)

ETSI/IQC Quantum Safe Cryptography Conference 2026

Topic 1: Key Technology



ETSI/IQC Quantum Safe Cryptography Conference 2026



ETSI/IQC Quantum Safe Cryptography Conference 2026

Topic 1: Algorithm library for Bank

ETSI/IQC Quantum Safe Cryptography Conference 2026

Topic 2: Protocol for Bank

Heterogeneous Authenticated Key Exchange

	Initiator Long Term Key	⟷	Responder Long Term Key
TLS	SIG		SIG
FSXY	KEM		KEM
HMQV	DH		DH

Existing AKE vs. Ours

Our Protocol

	Initiator Long Term Key	⟷	Responder Long Term Key
KEM-SIG	KEM		SIG
SIG-KEM	SIG		KEM

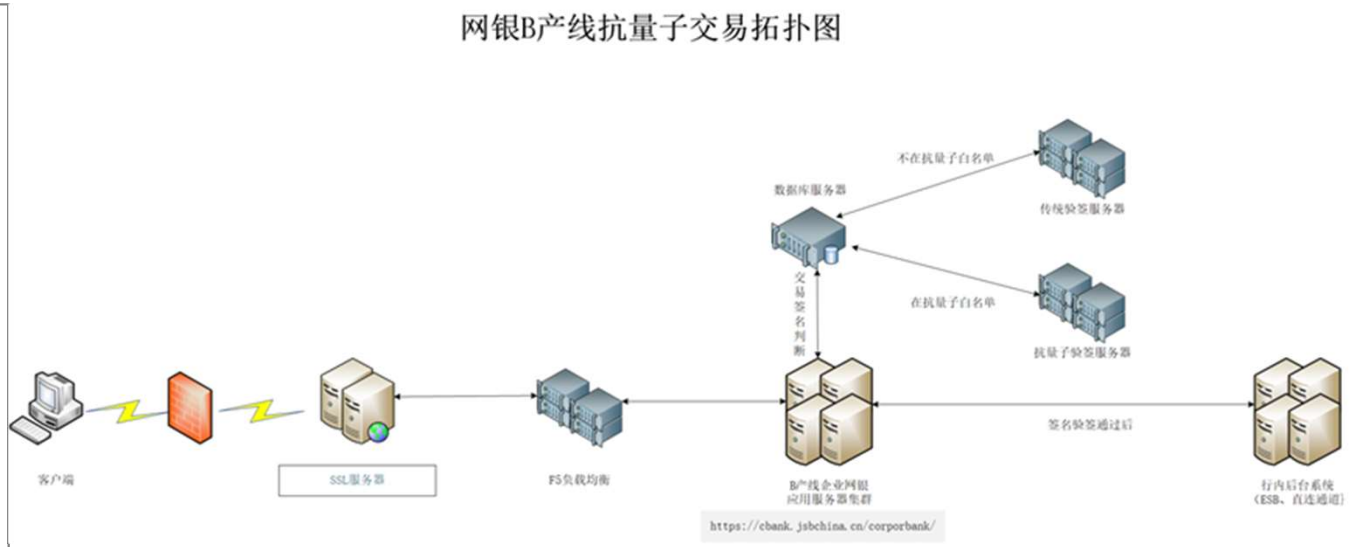
Key Features of Our Protocol

- IND-AA Security under QROM (resists KCI, MEX, state-reveal attacks)
- Mutual authentication with just one round
- Resource-asymmetric: The initiator benefits from lower computation time and bandwidth in KEM-SIG, while the responder gains these advantages in SIG-KEM
- Migration agility: supports mixed PQC adoption

ETSI/IQC Quantum Safe Cryptography Conference 2026

Topic 3: V&V in Commercial Banks

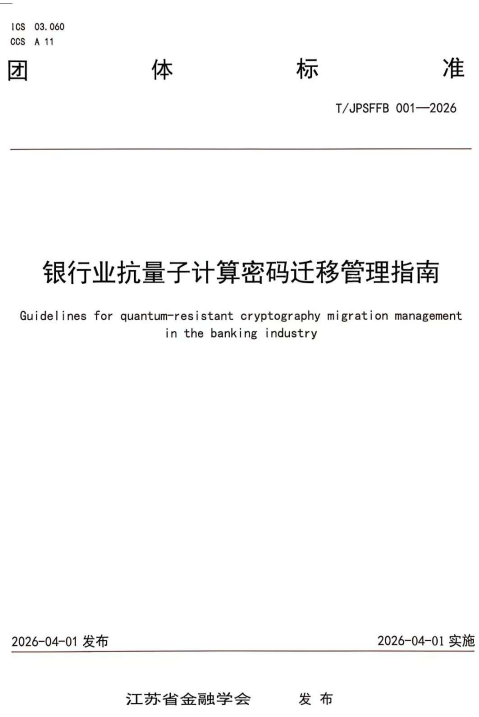
- Test Bed in Jiangsu Province Bank—System B
- System B, which is a system with all bank business functions and banking business data
- System A is the real system for banking business
- Test target in System B: Crypto-agility and hybrid-mod: A plug-in Key with China's SM2 (similar to ECC)



ETSI/IQC Quantum Safe Cryptography Conference 2026

Topic 4: Regulation

- In-progress Industry standards
- White paper of the Global PQC migration in Financial Sector
- Special Study for CRPQC threat


ICS 03.060
CCS A 11

团 体 标 准

T/JPSFFB 001—2026

银行业抗量子计算密码迁移管理指南

Guidelines for quantum-resistant cryptography migration management in the banking industry

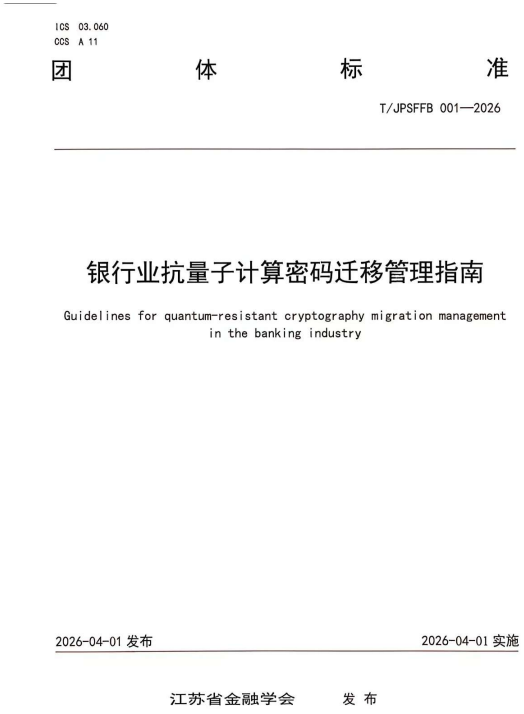
2026-04-01 发布 2026-04-01 实施

江苏省金融学会 发布

ETSI/IQC Quantum Safe Cryptography Conference 2026

Topic 4: Regulation

- "**Guidelines for quantum-resistant cryptography migration management in the banking industry**"
- Principles: compliance, security, agility, robustness
- Readiness and Planning Management
- Cybersecurity Concerns in the banking information systems
- Crypto Application Security
- Awareness Training in the banking industry



ICS 03.060
CCS A 11

团 体 标 准

T/JPSFFB 001—2026

银行业抗量子计算密码迁移管理指南

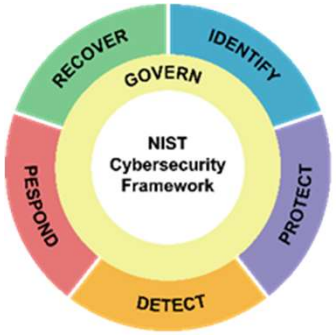
Guidelines for quantum-resistant cryptography migration management in the banking industry

2026-04-01 发布 2026-04-01 实施

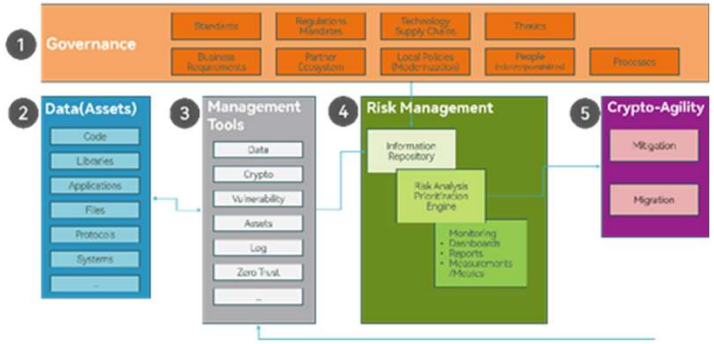
江苏省金融学会 发 布

ETSI/IQC Quantum Safe Cryptography Conference 2026

Topic 4: Frame work & Roadmap



+



NCCoE vs. Ours

- NCCoE：Follows from NIST CSF2.0 and PQC FIPS
- Ours：Follow China Standards（Regulation of Commercial Cryptography, Cybersecurity Level Protection, Information Security Mutual Model, etc.）
- NCCoE: A framework for general use-case
- Ours: A framework for Banking industry

ETSI/IQC Quantum Safe Cryptography Conference 2026

Q&A