

特色专题

统筹发展与安全:中国金融业量子安全迁移

周诚君

摘要 量子计算技术的迭代突破,对依托传统数学难题构建的公钥密码体系形成了现实安全威胁。金融行业作为国家关键信息基础设施的重要领域,其信息系统安全稳定运行直接关乎国家经济安全与全球金融稳定。在全球主要经济体积极推进抗量子计算密码(post-quantum cryptography, PQC)迁移的背景下,中国金融行业正从法律合规框架、算法标准制定、关键技术攻关与区域性工程实践等多个层面系统推进 PQC 迁移工作,为金融系统应对量子安全挑战探索切实可行的实践路径。未来,通过国家战略引导、法治规范与产业实践协同发力,构建自主可控、安全高效的金融量子安全防护体系,对筑牢数字经济时代金融基础设施安全底座、保障金融行业长远稳健发展具有重要战略意义。

关键词 抗量子计算密码(PQC);金融行业关键信息基础设施;密码迁移;量子安全

金融是支撑国家经济社会发展、维护国家安全的战略基石,其平稳高效运行对于维护经济稳定和保障社会信心具有不可替代的作用。现代金融体系高度依赖信息技术,从支付清算到信贷管理,从风险控制到跨境交易,无不建立在信息系统的可靠支撑之上。中国作为全球第二大经济体,2025 年末金融业机构总资产已达 538.86 万亿元^[1]。如此庞大的金融体系,其安全运行离不开密码技术对信息系统的全链条保护。然而,量子计算技术的快速演进,正对当前广泛使用的公钥密码体系形成现实挑战^[2-3]。一旦现有密码体系被量子攻击所突破,金融数据的机密性、交易的真实性以及系统的完整性均将面临严重威胁。因此,前瞻评估金融信息系统在量子时代的安全风险,积极推动抗量子计算密码(post-quantum cryptography, PQC)迁移工作,已经成为保障金融长远安全的重大课题。近年来,国内外金融行业围绕 PQC 迁移开展了多方面探索,涉及法律合规、标准制定、关键

技术攻关与工程实践等不同层面,系统梳理这些进展与经验,对于中国金融业筑牢量子时代的安全底座具有重要现实意义。

1 法律框架与合规驱动

PQC 迁移本质上是一项关系国家数字主权与金融基础设施安全韧性的治理工程。中国在金融领域的量子安全治理,正呈现出“战略规划引领、行业合规驱动、关键领域分步实施”的鲜明特征。

1.1 全球博弈环境下的时间节点与合规预期

在全球大国博弈背景下,数字主权已成为核心利益与必争之地。面对日趋严峻的量子危机(Q-Day),欧美等主要经济体已相继启动国家级量子安全战略并发布 PQC 系列标准^[4-6]。其中,美国先后出台《国家量子倡议法》(National Quantum Initiative Act)(2018)、《芯片与科学法案》(CHIPS and Science Act)(2022)和《量子计算安全准备法案》(Quantum Computing Cybersecurity Preparedness Act)(2022)。2026 年 4 月,

江苏省金融学会,南京 210004

收稿日期:2026-05-13;修回日期:2026-08-15

基金项目:国家重点研发计划项目(2023YFC3305500, 2025YFE0218100)

作者简介:周诚君,研究员,研究方向为货币政策、金融改革与金融科技,电子邮箱:zhoucj@pbc.gov.cn

引用格式:周诚君. 统筹发展与安全:中国金融业量子安全迁移[J]. 科技导报, 2026, 44(16): 132-136; doi:10.3981/j.issn.1000-7857.2026.05.00064

美国参议院商务委员会通过《2026 年国家量子计划重新授权法案》(National Quantum Initiative Reauthorization Act),旨在推动美国量子经济发展与国家安全相关法律法规的融合。欧盟通过更新网络与信息系统指令(network and information systems, NIS),以 2035 年为时间节点敦促成员国重视 PQC 迁移事项。2026 年 1 月,七国集团(G7)网络专家组发布文件,提出以 2035 年为抗量子密码迁移的整体目标日期,并建议成员国将金融系统中最关键的部分优先安排在 2030—2032 年完成迁移^[7]。

面对这一外部环境,中国将量子科技列为关键领域之一。“十五五”国民经济与社会发展纲要对量子科技等战略性新兴产业也进行了前瞻性布局。在金融领域,中国人民银行发布的《金融科技发展规划(2022—2025 年)》首次将量子技术纳入顶层设计,明确探索其突破算力约束、提升并发处理能力与智能运算效率,逐步培育可落地场景。2024 年,中国人民银行等七部门联合印发《推动数字金融高质量发展行动方案》,进一步强调为金融数字化转型提供精准高效的算力支持,将量子科技纳入新型基础设施体系^[8]。与此同时,中国金融行业 PQC 迁移先行先试的研究工作有序推进。2023 年,在中国人民银行科技司支持下,中国人民银行金融研究所牵头承担科技部重点研发计划——“银行业及其关键基础设施信息系统抗量子密码迁移技术”研究。

综合国内外动向,国际金融界已形成基本共识,即在 2035 年前完成 PQC 迁移工作(核心业务系统迁移时间节点或进一步提前)^[9]。中国金融行业可以此为为契机,全面盘点现有信息系统中的密码资产,制定切合自身业务特性的技术演进与系统安全重构路线图,推动从理论探索向实际应用落地。

1.2 完善数字空间安全法治体系

目前,中国尚未专门出台量子科技和量子安全相关法律法规,但现有《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国密码法》《中华人民共和国个人信息保护法》及《关键信息基础设施安全保护条例》等配套法规,已为金融行业密码升级提供了基本法律依据。中国人民银行也出台了一系列金融数字安全相关的条例和指南。上述合规要求形成由顶层法治驱动的刚性约束,正转化为

对金融行业 PQC 迁移风险评估、系统架构重构与软硬件升级的市场需求,成为推动 PQC 应用落地的内生动力。

与此同时,中国商用 PQC 算法征集活动正在紧锣密鼓地进行中^[10]。参照国内外金融行业 PQC 迁移的时间表,预计中国 PQC 迁移工作也将在 2030—2035 年部署推进,从而构筑起中国金融行业关键信息基础设施的量子安全防护网,并与国际金融行业保持量子安全条件下的互联互通(图 1)。

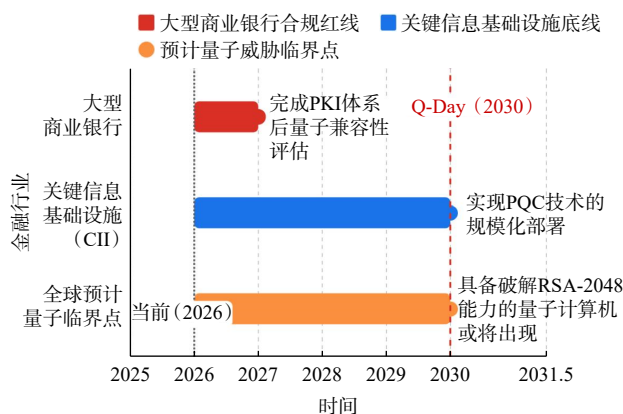


图 1 中国金融行业 PQC 迁移关键合规节点预测

(资料来源:根据行业研究报告整理绘制)

2 标准制定与技术自主

在现代金融工程中,技术与管理标准不仅是应用的通用语言,更是大国博弈的“制度性话语权”。缺乏统一且自主的标准体系,局部安全防线将沦为数字空间孤岛,难以解决网络信息安全的“木桶原理”,即网络信息安全的整体水平将由最薄弱环节决定。中国 PQC 标准化道路,须坚定不移贯彻“高水平科技自立自强”战略方针,探索“自主遴选—团体标准/行业标准先行—国家标准赋能”的演进路径。

2.1 全球 PQC 算法标准竞争与中国自主方案

为从根本上化解量子计算带来的风险并适配数字金融新业态,在国家密码管理局统筹下,商用密码标准研究院(Institute of Commercial Cryptography Standards, ICCS)于 2025 年正式启动“新一代商用密码算法征集活动”(next-generation commercial cryptographic algorithms, NGCC),标志着中国商密体系向量子安全时代的一次重要跨越。

当前,国际 PQC 算法标准主要分为 2 大流派:一类是以美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)为代表的 PQC 算法标准,目前正在成为美国等西方国家 PQC 迁移的主要依据;另一类是中国正在进行的 PQC 算法征集与标准制定活动。PQC 算法标准的制定,不仅考验各国在 PQC 算法理论研究方面的积累^[1],也有效促进 PQC 应用的实践反馈。在 NIST 算法征集和标准制定过程中,大量国际企业积极参与其中;中国金融业 PQC 迁移试点中形成的工程经验,也正反馈到国内 PQC 算法征集活动中,将有效助力遴选出安全裕度高、性能卓越的中国方案。值得注意的是,由于美国 NIST 标准和中国 PQC 标准将长期共存、相互竞合,因此有必要在 PQC 应用落地方面贡献中国自主方案,特别是更多凝聚“一带一路”沿线国家和南方国家共识,共同捍卫金融安全及治理。

2.2 金融业标准先行先试

美国自 2018 年开始布局 PQC 迁移相关工作,但截至目前,国际上尚未发布金融业 PQC 迁移相关的专门指南或行业标准。在这一领域,中国取得积极突破。2026 年 4 月 17 日,江苏省金融学会正式发布了由中国人民银行金融研究所牵头,联合多家金融管理机构、法人银行与科研单位共同起草的《银行业抗量子计算密码迁移管理指南》团体标准^[12],这是中国金融行业在 PQC 迁移领域的首个团体标准,为商业银行规范开展迁移规划、夯实技术储备、实现平滑过渡提供了清晰的管理范式。该标准的出台建立在国家科技重点专项取得的阶段性成果之上,同时充分吸纳了“江苏省商业银行量子安全试验区”的前沿实践经验,后续将持续推动该标准向金融行业标准(JR/T)乃至国家标准(GB/T)跃升。

未来,中国金融行业有望进一步围绕现有国家标准(national standard, GB)和新一代 PQC 标准,持续提升其关键信息基础设施抵御量子计算攻击能力,为国家相关标准体系全面过渡到量子安全状态探索可行路径,最终实现新一代 PQC 技术深度融入数字金融各个领域,为中国金融安全及其深入参与全球金融安全和治理框架作出应有贡献。

3 系统韧性与工程实践

理论的有效性与可行性,须经过金融行业典型应用场景的实践检验。对于金融机构而言,PQC 迁移并非简单的“软件补丁”,而是一次深度的 IT 安全架构解耦与系统韧性重构。在保障核心业务连续性的前提下,实现底层安全根基的平滑替换,是工程落地的关键。在这一过程中,科技部部署的 2 项国家重点研发计划专项发挥了关键作用。

3.1 国家级科研专项“双轮驱动”

在国家宏观科技规划统筹下,中国金融行业 PQC 迁移依托国家重点研发计划项目,形成“对内筑基、对外拓展”的协同攻关格局,为全行业平稳迁移提供了强有力的技术支撑和路径指引。

1) 立足国内金融基础设施的“银行业及其关键基础设施信息系统抗量子密码迁移关键技术研究”项目。该项目由中国人民银行金融研究所牵头,聚焦中国银行业资产庞大、网络结构复杂等特征,面向手机银行、网络银行和跨行交易 3 大典型应用场景,在 PQC 算法安全性评估、抗量子安全通信协议、软硬件高效实现、高仿真环境验证以及敏捷迁移框架等方面取得了一系列科研成果,其中,有 2 项成果取得阶段性重要进展:一是攻克了国际主流 PQC 算法(特别是格密码)安全边界量化分析难题,为国内 PQC 算法遴选和银行业 PQC 算法适配提供了理论支撑;二是在实践基础上出台《银行业抗量子计算密码迁移管理指南》团体标准。此外,在江苏省金融学会指导下,成立金融抗量子计算迁移专业委员会,开展了一系列团体标准的制定和研发工作,并与欧美金融行业以及“一带一路”沿线国家商业银行逐步建立起合作渠道。

2) 面向全球金融互联互通的科技部国际合作重点专项“国际金融银行业典型交易业务抗量子迁移的关键技术验证与应用示范”。该项目致力于攻克“多体系抗量子密码互信互通互认”的国际级难题,联合欧洲、中国香港等地的科研团队及国际大型银行,探索研发多算法融合的金融芯片卡、多协议融合的抗量子安全网关,并在“一带一路”沿线国家开展国际交易场景的迁移验证,该项目不仅致力于保障中国跨境金融业务的连续性与安全性,更在国际金融安全规则与

标准制定领域发出中国声音,输出中国方案。

上述2项国家级重点专项的协同推进,有效打通了从底层算法理论、中层协议网关到上层核心业务应用的全产业链条,为中国金融业在量子时代的数字安全提供了可验证的战略护航。

3.2 平滑过渡的安全架构与“密码敏捷性”演进

PQC迁移是一个长期而复杂的过程^[13]。客观而言,当前主流PQC算法在计算开销、内存消耗和密文传输长度方面,均较传统的密码算法有显著增加。在金融行业超高频交易场景中,采取“一刀切”的替换策略可能存在较高风险。因此,金融机构须构建适应平滑过渡的安全演进架构,确立“密码敏捷性”(cryptographic agility)为核心设计原则。

在上述2个国家级项目中,金融业务与PQC迁移实现了紧密融合,未来,当某类PQC算法安全阈值下降,或国家标准乃至国际相关标准更新时,金融行业的IT系统能够通过策略配置或动态加载,实现底层加密组件的不停机更换,避免业务代码重写,有助于提升金融基础设施在应对未知技术冲击时的系统韧性。

3.3 江苏省商业银行量子安全试验区

在工程化落地方面,依托科技部重点项目,上述项目组积极推动建设“江苏省商业银行量子安全试验区”,将银行业PQC迁移从实验室的理论研究推向更贴近真实生产环境的验证实践。

一方面,积极布局B线环境下的PQC迁移验证工作。B线环境具备银行业全业务要素,采用“白名单”这一风险可控的机制对科技金融的新技术进行试验验证。聚焦手机银行和网上银行抗量子安全升级,针对银行业结算业务在特定时段的高并发特征,进行大规模压力测试,验证系统运行的稳定性;重点推进“抗量子U盾”研发测试,依托其“即插即用”的敏捷性,以及低成本、高效能的终端防护特点,不仅为大额用户网上交易提供了量子安全保障,还为银行业PQC迁移工具箱提供了新的选项。

另一方面,前瞻性研究数字人民币量子安全防护。江苏作为中国数字人民币应用试点的先行地区,也应尽早探索这一领域的安全保障模式。未来,将在国家级科研项目成果基础上,加大对数字人民币安全应用的技术攻关,包括支付交易场景的抗量子签名

(如使用PQC数字签名替代SM2)、新一代哈希安全签名防二维码的替换/伪造、智能合约PQC签名防核心账本的篡改/回溯等,为数字人民币稳定运行提供量子安全保障。

4 结论

“备豫不虞,为国常道”。量子计算时代的来临,对于中国庞大的金融体系而言,既是一场严峻的系统性危机压力测试,更是打破传统技术路径依赖、实现网络空间底层根技术自主创新的重大战略机遇。

纵观全局,从启动银行业PQC迁移先行先试,到关键信息基础设施规模化部署的准备工作;从自主可控的商用密码算法遴选,到商业银行全景式技术与管理验证,中国已初步形成了一条兼顾金融密码安全理论扎实、技术先进及产业协同的PQC发展路径。面向“十五五”新征程,金融机构、关键信息基础设施运营者及科技金融企业需协同发力,以“密码敏捷性”作为核心工程抓手,将金融IT系统的底层重构与PQC迁移规划深度结合。通过国家战略的持续引领、法治规范的不断完善以及广泛金融应用场景的内生驱动,中国自主的金融量子安全体系有望迎来发展的重要时期,为金融业高质量发展提供安全保障,为构建可信的数字经济基础贡献重要力量。

参考文献(References)

- [1] 中国人民银行. 2025年4季度末金融业机构总资产538.9万亿元[EB/OL]. (2026-03-13) [2026-04-15]. <https://www.pbc.gov.cn/goutongjiaoliu/113456/113469/index.html>.
- [2] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. *SIAM Journal on Computing*, 1997, 26(5): 1484-1509.
- [3] Bernstein D J, Lange T. Post-quantum cryptography[J]. *Nature*, 2017, 549(7671): 188-194.
- [4] National Institute of Standards and Technology. Module-lattice-based key-encapsulation mechanism standard: FIPS 203[S]. Gaithersburg: NIST, 2024.
- [5] National Institute of Standards and Technology. Module-lattice-based digital signature standard: FIPS 204[S]. Gaithersburg: NIST, 2024.
- [6] National Institute of Standards and Technology. Stateless hash-based digital signature standard: FIPS 205[S]. Gaithersburg: NIST, 2024.

- burg: NIST, 2024.
- [7] G7 Cyber Expert Group. G7 cyber expert group statement on advancing a coordinated roadmap for the transition to post-quantum cryptography in the financial sector[R/OL]. (2026-01-13) [2026-04-15]. <https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf>.
- [8] 中国人民银行, 国家发展改革委, 工业和信息化部, 等. 推动数字金融高质量发展行动方案[A/OL]. (2024-11-28) [2026-08-15]. https://www.gov.cn/lianbo/bumen/202411/content_6989645.htm.
- [9] 丁津泰, 向宏, 刘锐. 全球金融银行业抗量子安全迁移白皮书(2025)[R/OL]. (2025-12-01) [2026-04-15]. https://www.xjtlu.edu.cn/wp-content/uploads/2025/06/Global-Financial-Banking-Post-Quantum-Security-Migration-White-Paper2025_ZH_v1.0.1.pdf.
- [10] 商用密码标准研究院. 关于开展新一代商用密码算法征集活动的公告[EB/OL]. (2025-02-05) [2026-04-15]. https://www.niccs.org.cn/symmbzyjy/tzgg/pc/content/1937422988373135360/content_1937422988373135360.html.
- [11] Alagic G, Apon D, Cooper D, et al. Status report on the third round of the NIST post-quantum cryptography standardization process: NIST IR 8413 upd1[EB/OL]. [2026-04-15]. <https://doi.org/10.6028/NIST.IR.8413-upd1>.
- [12] 江苏省金融学会. 银行业抗量子计算密码迁移管理指南: T/JPSFFB 001—2026[S]. 南京: 江苏省金融学会, 2026.
- [13] Mosca M. Cybersecurity in an era with quantum computers: Will we be ready?[J]. *IEEE Security & Privacy*, 2018, 16(5): 38-41.

Coordinating development and security: Prospects for the quantum-safe migration of China's financial industry

ZHOU Chengjun

Jiangsu Provincial Society for Finance and Banking, Nanjing 210004, China

Abstract The iterative breakthroughs in quantum computing pose a realistic security threat to public-key cryptosystems built upon traditional mathematical hard problems. As an important field of the national critical information infrastructure, the financial industry relies on the secure and stable operation of its information systems, which bears directly on national economic security and global financial stability. Against the backdrop of major economies actively advancing post-quantum cryptography (PQC) migration, China's financial industry is systematically promoting PQC migration at multiple levels, including the legal and compliance framework, algorithm standardization, key technology research, and regional engineering practice, thereby exploring a practicable path for the financial system to meet quantum security challenges. In the future, building an autonomous, controllable, secure, and efficient quantum-safe protection system for finance through the coordinated efforts of national strategic guidance, rule of law, and industrial practice will be of major strategic significance for consolidating the security foundation of financial infrastructure in the digital economy era and for safeguarding the long-term sound development of the financial industry.

Keywords post-quantum cryptography (PQC); critical information infrastructure of the financial industry; cryptographic migration; quantum safety ●



(责任编辑 王志敏)