

## 特色专题

# 抗量子计算密码进展与中国迁移路径

周诚君<sup>1</sup>, 丁津泰<sup>2,3</sup>

**摘要** 随着可扩展容错量子计算工程化技术的加速突破, Rivest-Shamir-Adleman(RSA)与椭圆曲线密码(elliptic curve cryptography, ECC)等现有公钥密码体系面临颠覆性安全威胁。特别是“先窃取, 后解密”攻击模式的存在, 进一步凸显抗量子计算密码(post-quantum cryptography, PQC)迁移的现实紧迫性。系统梳理 PQC 领域发展历程、前沿研究突破与全球标准化格局, 重点剖析金融行业 PQC 迁移实践与探索; 进一步分析格密码安全性精细化规约、高维最短向量问题(shortest vector problem, SVP)攻防边界的动态演化与主流数字签名方案的工程化演进, 梳理中美欧日韩 PQC 标准化的多极化格局与“密码敏捷性”(crypto-agility)新范式; 结合中国“SM+PQC 双栈融合”演进思路和金融业先行实践, 提出将密码敏捷性列为关键信息基础设施的刚性架构规范, 加快国家密码管理局发布的密码算法(国密)SM 与 PQC 双栈标准协同、建立统一迁移框架等政策建议, 以期为中国下一阶段的技术攻关与标准布局提供参考。

**关键词** 抗量子计算密码; 量子计算; 密码迁移; 商用密码标准; 密码敏捷性

过去 5 年, 量子计算已跨越基础物理实验室, 全面进入工程化扩展阶段。IBM、Google 以及中国科学技术大学等国内外顶尖科研机构相继在超导、光量子等技术路线上实现突破。以 IBM 路线图为例, 其计划在 2029 年交付具备 200 个逻辑量子比特的容错量子计算机<sup>[1]</sup>。学术界普遍认为, 虽然能够运行 Shor 算法、对现有公钥密码体系构成实质性威胁的容错量子计算机仍存在工程不确定性, 但其实现的时间窗口正在逐步收窄, 全球已进入量子安全风险前瞻性应对、系统性布局的战略评估阶段。

抗量子计算密码(post-quantum cryptography,

PQC)的研究与部署, 既是应对未来量子算力突破的长远布局, 也是防范当下现实安全威胁的迫切需求。目前, 高级别国家黑客与 APT(Advanced Persistent Threat)组织正广泛采用“先窃取, 后解密”策略, 大规模截获并存储基于现行公钥体系加密的高价值密文。对于保密期限长达十几年乃至数十年的敏感数据而言, 现有密码体系已无法覆盖全生命周期安全需求, 在时间维度上提前陷入失效困境。因此, 密码系统安全性评估逻辑亟需转变, 须从“当前即时抗攻击能力”转向“数据生命周期内的整体安全性”。

全球数字空间安全架构正处于大规模重构的关键历史窗口期。例如, 美国已明确制定战略目标, 计划 2035 年全面完成国家安全系统向 PQC 体系的迁移<sup>[2]</sup>。2024 年 8 月, 美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)正式发布联邦信息处理标准(Federal Information Pro-

1. 江苏省金融学会, 南京 210004

2. 西交利物浦大学后量子迁移交叉实验室(PQC-X), 苏州 215123

3. 江苏省金融学会抗量子计算迁移专业委员会, 苏州 215123

收稿日期: 2026-05-13; 修回日期: 2026-07-11

基金项目: 国家重点研发计划项目(2023YFC3305500)

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, 电子信箱: zhoucj@pbc.gov.cn

引用格式: 周诚君, 丁津泰. 抗量子计算密码进展与中国迁移路径[J]. 科技导报, 2026, 44(16): 49-56; doi:10.3981/j.issn.1000-7857.2026.05.00051

cessing Standards, FIPS)203/204/205 最终标准<sup>[3]</sup>, 美国国家网络安全卓越中心(National Cybersecurity Center of Excellence, NCCoE)同步推出实施指南, 标志着 PQC 已跨越学术范畴, 成为全球争夺下一代网络空间主导权的战略高地。量子安全迁移已从技术议题升级为国家数字主权与关键信息基础设施安全的战略必答题。为此, 本文依次梳理 PQC 的技术态势与安全边界、国际标准化格局与大国密码主权、中国“SM+PQC 双栈融合”路径与金融业先行实践, 并面向决策者给出分阶段行动路线图与政策建议。

## 1 抗量子计算密码的技术态势与安全边界

密码学的演进本质是攻防双方技术博弈、迭代升级的过程。PQC 的发展历程可清晰划分为 3 个阶段(图 1)。

### 1.1 PQC 的发展历程

1) 第 1 阶段(20 世纪 90 年代—2015 年): 理论拓荒期。Shor 算法的提出, 彻底打破了传统公钥密码体系的安全根基<sup>[4]</sup>, 寻找能够抵御量子计算攻击的数学难题, 成为密码学界的核心命题。这一阶段奠定了 4 大传统技术路线: 基于编码理论的公钥密码(code-based cryptography)<sup>[5]</sup>、具备极高安全性但状态管理难度较大的基于哈希的密码(Hash-based cryptography)<sup>[6]</sup>、签名长度具备显著优势的多变量密码(multivariate cryptography)<sup>[7]</sup>, 以及兼顾效率与安全性的基于格上困难问题的密码(lattice-based cryptography)<sup>[8]</sup>。

2) 第 2 阶段(2016—2024 年): 算法竞赛与标准化时代。2016 年, NIST 面向全球启动 PQC 算法竞赛与标准化项目, 成为推动 PQC 技术快速发展的重要推动力。经历 4 轮严格的密码分析与工程评估, 格密

码逐渐占据主流地位: Kyber(ML-KEM)与 Dilithium(ML-DSA)算法脱颖而出<sup>[9-10]</sup>, SPHINCS+(SLH-DSA)和 HQC 算法则作为保守的后备方案入选<sup>[11]</sup>。这一阶段的标志性特征是理论研究成果向工程实践的高效转化。

3) 第 3 阶段(2024 至今): 标准多极化与产业化落地期。NIST 标准的正式发布, 标志着 PQC 算法遴选阶段的结束, 产业迁移工程实施、长期具体安全评估成为全新的核心挑战。当前, PQC 已迈入标准多极化与产业化落地关键阶段, 包括中国在内的很多国家正积极布局自主可控的 PQC 算法标准体系。全球学术与产业界的关注焦点, 从算法研发全面转向系统迁移、混合 TLS(transport layer security)协议、国家级自主标准竞争以及密码主权生态系统构建等核心环节。

### 1.2 研究突破与前沿动态

1) 格密码理论进展: 安全性的精细化规约。近 5 年来, 基于 LWE(learning with errors)<sup>[12]</sup>与 Module-LWE(module learning with errors)的安全证明研究, 正不断向精细化方向发展。国际密码学界纷纷聚焦格密码归约质量的紧致化、解密失败分析引发的 CCA(chosen-ciphertext attack)攻击隐患, 以及具体安全估计的动态调整等关键问题展开攻关; 与此同时, 围绕 Kyber 在各类侧信道(如 KyberSlash 计时攻击)<sup>[13]</sup>与安全性裕度方面的讨论, 成为近年来密码领域研究热点<sup>[14]</sup>。

2) SVP 挑战的突破: 安全边界动态重构。“以攻促防”是量子安全时代评估密码强度的根本方法——唯有攻击能力持续进步, 才能真实标定防御边界, 攻是手段、防是目的。格密码体制的安全性, 根本上依赖于高维近似最短向量问题(shortest vector problem, SVP)的求解难度。近期, 高维 SVP 破译记录频繁刷

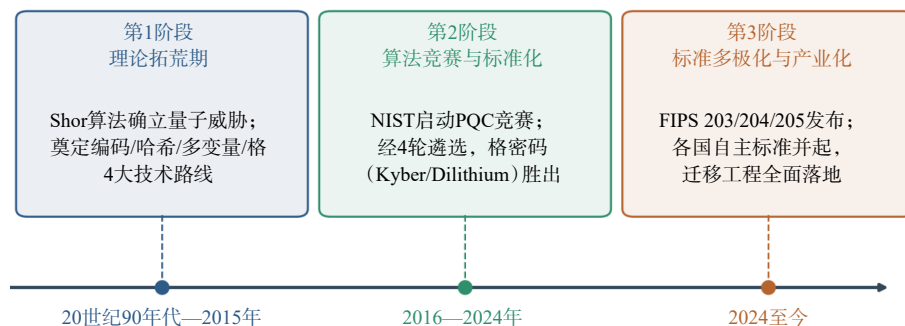


图 1 抗量子计算密码(PQC)发展的 3 个历史阶段

新,主要得益于攻击手段的融合创新——例如将筛法与枚举法深度结合,配合底层代码的极致优化,甚至引入了机器学习来执行高效的剪枝操作<sup>[15]</sup>。由于不同算力模型和预设条件得出的攻击复杂度存在显著差异,从侧面印证了一个关键事实: PQC 算法的安全边界并非一成不变,而是高度依赖于评估模型,并处于动态演化之中。

在这一领域,西交利物浦大学丁津泰团队多次刷新公开挑战记录。继 2025 年 3 月攻克 SVP-200 维后,该团队于 2026 年 1 月成功求解了 SVP-210 维挑战实例,同期破译了 Kyber-208 低维实例<sup>[16]</sup>,随后于 2026 年 3 月成功完成了 Kyber-256 实例的破译<sup>[17]</sup>。需要说明的是,上述纪录针对的是安全强度低于实际部署标准的挑战实例(低维 SVP 与降参数 Kyber 实例),并不意味着 ML-KEM 等标准算法的推荐参数集已被攻破,其意义在于为算法安全裕度的动态评估提供实测标尺。SVP 挑战维度的快速推进表明,PQC 主流算法——格密码参数的安全裕度并非静态,必须建立周期性的重新评估机制,以防范未来可能出现的降维打击。

3) 数字签名: 工程化与效率提升。数字签名是现代大型计算机通信网络的信任基础。正是基于现代公钥密码的数字签名技术,才使得网络空间这一天然不具备可信性的人造空间,构建起基于数学困难问题的信任链。数字签名拥有其他量子安全技术(如量子密钥分发)不具备的独特优势。在 PQC 数字签名领域,工程实用性是核心考量要素。Dilithium 的工程部署优化成为 PQC 迁移领域关注的焦点; Falcon(fast-Fourier lattice-based compact signatures over NTRU)<sup>[18]</sup>

因其极优的带宽效率而备受青睐; 无状态哈希签名在彻底消除状态耗尽风险后,在软件代码签名等场景下取得重要突破,从而为未来全球数字经济的安全保障提供了备选方案。

4) 迁移工程: 协议与设备的系统级适配。当前研究重点已从算法设计转向系统级适配,核心在于解决协议兼容性、性能开销与大规模部署可行性等“最后一公里”问题,包括设计混合握手协议(hybrid TLS)及应对证书链膨胀问题。在产业基础设施层面,亚马逊云科技(Amazon Web Services, AWS)等云计算公司已率先完成阶段性突破,在其密钥管理系统和内部通信中默认启用基于 ML-KEM 的混合 TLS 加密,从工程物理层面验证了 PQC 协议应对超大规模并发场景的能力。互联网工程任务组(Internet Engineering Task Force, IETF)正持续更新基于 NIST 标准的抗量子计算安全协议簇,目前聚焦于 TLS1.3 这一核心枢纽协议,部分征求意见稿(Request for Comments, RFC)已在全球产业界形成共识。PQC 安全协议的更新换代将对全球网络安全产业产生深远的影响,对于中国正积极推动的信息技术应用创新(信创)产业而言,需予以充分重视。

2 国际标准化格局与大国密码主权

在抗量子时代,密码标准正成为大国数字主权的核心壁垒。全球 PQC 标准正朝着多极化方向发展,本质上反映出 PQC 已从单纯技术问题,演变为各国标准主导权与数字安全治理能力的综合性竞争(表 1)。

表 1 全球主要国家/地区抗量子计算密码标准化路线对比

| 国家/地区 | 主导机构            | 代表性标准/算法                   | 路线特点            |
|-------|-----------------|----------------------------|-----------------|
| 美国    | NIST、NCCoE、NSA  | FIPS 203/204/205; CNSA 2.0 | 先发主导,标准+政策+产业布局 |
| 欧洲    | ENISA           | 传统密码/PQC混合保护策略             | 审慎合规,与电信设施平滑集成  |
| 韩国    | NSR(KpqC竞赛)     | HAETAE、AIMer、SMAUG-T       | 本土算法自主遴选        |
| 日本    | CRYPTREC        | 推荐清单纳入ML-KEM               | 对NIST标准独立评估     |
| 中国    | 商用密码标准研究院、TC260 | 新一代商用密码征集; SM+PQC          | 融合演进,依托国密改造经验   |

注: NSA为美国国家安全局(National Security Agency); ENISA为欧盟网络安全局(European Union Agency for Cybersecurity); NSR为韩国国家保安技术研究所(National Security Research Institute); KpqC为韩国后量子密码竞赛(Korea Post-Quantum Cryptography Competition), HAETAE、AIMer、SMAUG-T均为KpqC竞赛遴选出的算法名称(HAETAE取自韩国神兽獬豸, AIMer基于MPC-in-the-Head范式, SMAUG-T基于Module-LWE与Module-LWR); CRYPTREC为日本密码研究与评估委员会(Cryptography Research and Evaluation Committees); TC260为全国信息安全标准化技术委员会。

## 2.1 美国路线:先发制人的全球主导策略

美国通过 NIST FIPS 203/204/205 建立全球事实标准<sup>[3]</sup>,并联合 NCCoE 全面启动“抗量子密码迁移”国家级专项工程。该中心出台了详尽的操作手册与参考架构,强调将构建“密码敏捷性”(crypto-agility)作为企业下一代 IT 架构的刚性框架<sup>[19]</sup>。美国国家安全局(National Security Agency, NSA)发布的商用国家安全算法(Commercial National Security Algorithm, CNSA)2.0 指南强制联邦采购向 PQC 迁移<sup>[2]</sup>。2025 年 6 月,美国政府进一步更新相关行政令<sup>[20]</sup>,要求企业为全美各行业在 2035 年之前完成 PQC 迁移提供关键产品支撑,形成“标准+政策+产业”的全方位主导体系。

## 2.2 欧洲路线:审慎合规与通信基础设施深度集成

以欧盟网络安全局(European Union Agency for Cybersecurity, ENISA)为代表的欧洲机构态度相对审慎,明确强调对现有电信基础设施的平滑演进与“传统密码/PQC”混合保护策略,以避免对单一底层数学难题的过度依赖<sup>[21]</sup>。欧盟网络安全局对 PQC 迁移工作的指导文件高度重视混合加密方案研究,并以案例的方式介绍了需进一步探讨的要点。这也提示中国可根据 PQC 算法征集活动进展,对互联网各类通信协议中的安全协议迁移进行深入分析、前瞻应对。

## 2.3 韩国、日本路线:独立评估与本土化自主布局

韩国国家保安技术研究所(National Security Research Institute, NSR)通过 KpqC 竞赛研发本土算法,并于 2025 年 1 月公布 HAETAE、AIMer、SMAUG-T 等胜选国家标准<sup>[22]</sup>。日本依托密码研究与评估委员会(Cryptography Research and Evaluation Committees, CRYPTREC)对 NIST 标准进行深度独立评估,并于 2026 年初正式将 ML-KEM 纳入电子政府推荐密码清单<sup>[23]</sup>。鉴于日、韩 2 国在全球半导体芯片等领域的重要影响力,其面向未来 IT 产业“量子安全免疫”的布局值得高度关注。

# 3 中国路径:SM+PQC 双栈融合演进与金融先行实践

## 3.1 SM+PQC 双栈融合演进

全盘照搬单一国外密码标准或将面临供应链断

裂风险,《中华人民共和国密码法》也对中国商用密码的自主研究和规范应用有明确法律要求。目前,中国产学研用各界正致力于将 PQC 作为基础防线,构筑坚固的国家网络安全屏障。国家商用密码标准研究院(Institute of Commercial Cryptography Standards, ICCS)已正式面向全球公开征集兼具经典与量子安全的新一代商用密码算法<sup>[24]</sup>。全国信息安全标准化技术委员会(National Information Security Standardization Technical Committee, TC260)已全面启动 PQC 相关的底层算法与协议标准预研立项。可以预见,在未来国际 PQC 迁移领域,中外标准将同台竞技。密码标准发展的历史表明,谁拥有更广泛的应用场景,并驱动形成全栈产业链供应链,谁在密码标准国际舞台上就拥有更多的话语权。

中国 PQC 迁移路线的特色之一是“融合演进”,即构建现有商用密码(ShangMi, SM)系列与新一代 PQC 标准算法的双栈并联标准体系架构。需要澄清的是,SM 体系内部对量子威胁的暴露程度并不一致:SM3 杂凑与 SM4 分组密码属对称类原语,仅受 Grover 算法平方级加速影响,抗量子风险显著低于公钥类算法,必要时可通过增大密钥/输出长度进一步保障;而 SM2(基于椭圆曲线)与 SM9(基于双线性对)属公钥类算法,其安全性依赖椭圆曲线离散对数与配对相关难题,与 RSA、ECC 一样可被 Shor 算法有效攻破。因此,“SM+PQC 双栈”并非“国密照旧、简单叠加 PQC”,而是精准针对 SM2/SM9 所在的公钥层——在迁移期以经典 SM 算法与 PQC 算法混合(hybrid)并联,使整体安全性在任一体系未被攻破时仍可维持;其自主可控的最终形态,则有赖于国家密码管理局新一代商用密码算法征集<sup>[24]</sup>所遴选的国产抗量子公钥算法逐步接替 SM2/SM9 的公钥职能。中国还具备世界前沿的独立进攻性密码分析能力(如前述丁津泰团队的 SVP/Kyber 破译纪录),能够自主验证所部署算法的真实安全性、自主校准安全参数,而非依赖他方安全声明;这种“以攻促防、攻防一体”的自主评估能力,正是密码主权不可或缺的能力底座,也使中国双栈路径区别于纯粹“跟随标准”的被动迁移。事实上,在全球 PQC 迁移工程中,共同面临的难题是如何将已有信息系统中的遗留系统迁移到具备量子安全状态的系统。国际上的共识是采用“混合模式”,即

第一代公钥密码模块与 PQC 模块并存的模式。对中国而言,在国家主管部门的统一部署下,国内重要基础设施信息系统已经历或正在经历“国密改造”工程,这为抗量子混合模式提供了极为宝贵的实践经验。

### 3.2 金融业先行实践

即使 PQC 技术和产品逐步成熟,全球金融业迁移仍面临合规性指导不足的问题。目前,中国已有一些探索性尝试。例如,江苏省金融学会联合国内一流科研院所和部分商业银行,研究编制全球首份《银行业抗量子计算迁移管理指南》团体标准<sup>[25]</sup>。依托中国金融行业丰富的应用场景,为打造具有示范意义的 PQC 行业迁移实践路径提供坚实基础。

#### 3.2.1 金融行业迁移的现实紧迫性与全球前瞻布局

金融系统作为国家经济运行的中枢,是 PQC 规模化应用的优先先行领域。其中,金融长期账本与交易底单是“先窃取、后解密”攻击的首选目标。在国际实践层面,国际清算银行创新中心联合多国央行成功完成了“跃进项目”(Project Leap),在真实支付系统中成功运行了基于 PQC 的混合加密方案<sup>[26]</sup>。以摩根大通(JPMorgan Chase)为首的华尔街银行机构也已出台针对全球金融机构公钥基础设施(public key infrastructure, PKI)架构脆弱性的应对指南。同时,环球银行金融电信协会(Society for Worldwide Interbank Financial Telecommunication, SWIFT)也正积极推进 PQC 升级换代<sup>[27]</sup>。

#### 3.2.2 中国金融业的迁移探索与实践进展

中国金融业 PQC 迁移工作稳步推进,国内部分大型国有银行(如工商银行<sup>[28]</sup>、建设银行、江苏银行等)已率先启动 PQC 演进路线图与应用试点。在中国人民银行的统筹指导下,金融行业的 PQC 迁移探索正从金融机构自发试点逐步走向体系化攻坚。

在国家重点专项方面,由中国人民银行金融研究所牵头,联合国内科研院所及商业银行,共同承担科技部国家重点研发计划项目——银行业及其关键基础设施信息系统的抗量子密码迁移技术研究,项目在底层格密码算法安全分析、抗量子敏捷迁移框架、银行业量子安全预警模型<sup>[29]</sup>,以及行业监管指南编制等领域取得重大阶段性进展<sup>[25]</sup>。

在国际化应用示范验证方面,为应对多体系量子密码互信、互通、互认以及全球协作等挑战,中国

启动首个面向国际金融业的国家级应用示范项目——国家重点研发计划“战略性科技创新合作”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”<sup>[30]</sup>。该项目聚焦国际金融业核心需求,紧密围绕“关键迁移技术链”“系统原型研制”“应用示范验证”3 大核心环节展开攻关,着力搭建多模式抗量子密码迁移验证平台,为全球金融基础设施的平滑过渡、“一带一路”沿线国家和非洲国家的金融安全升级提供中国方案与实践参考。

## 4 分阶段行动路线图与政策建议

基于上述态势研判与中国路径分析,给出可操作的分阶段行动路线图与政策建议如下。

### 4.1 分阶段行动路线图

对标美国 2035 年迁移窗口,建议中国抗量子迁移按“近期—中期—远期”3 阶段、沿“标准供给—金融先行—信创产业”3 条主线推进(图 2)。

1) 近期(2026—2028 年)以“摸清家底、建立标准、金融试点”为主,完成关键信息基础设施密码资产盘点,推进新一代商用密码算法征集与 PQC 国家标准预研立项,落地银行业迁移团体标准并扩大金融场景试点。

2) 中期(2029—2032 年)转向“双栈规模部署、密码敏捷改造”: SM+PQC 双栈标准体系定稿,将密码敏捷性架构规范逐步刚性化,推动金融核心业务链路与信创软硬件栈的双栈混合部署。

3) 远期(2033—2035 年)聚焦“全域迁移、国际互认”:完成关键业务原生 PQC 闭环,推进标准国际互认并参与全球 PQC 协议簇制定,形成全栈量子安全产业生态。

### 4.2 面向决策者的分层政策建议

结合上述路线图,提出 5 条政策建议。

1) 将密码敏捷性列为关键信息基础设施的刚性架构规范。多标准并存将长期存在,建议在重点行业 IT 架构标准中明确密码敏捷性要求,以支持不同标准体系间的互操作与平滑切换。

2) 加快 SM 国密与 PQC 双栈标准协同,建立统一迁移框架。建议依托 ICCS、TC260 加速双栈并联标准体系建设,形成算法—协议—证书—密钥管理全

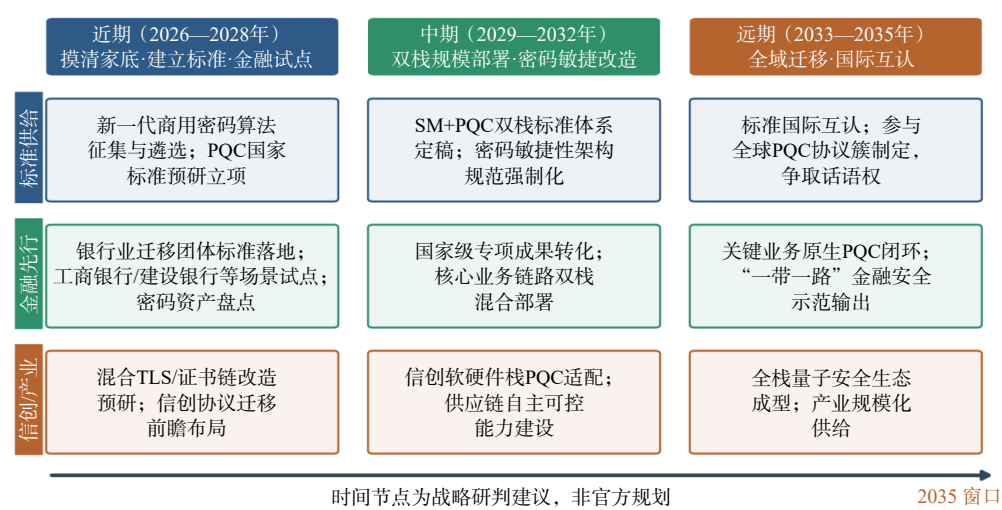


图 2 中国抗量子密码分阶段迁移行动路线图(2026—2035 年)

链条的统一迁移规范。

3) 以金融业为先行示范, 形成可复制推广的行业范式。建议在中国人民银行统筹下, 将金融试点与国家级专项成果提炼为标准化迁移方法, 向其他关键行业与“一带一路”场景推广。

4) 建立密码算法安全裕度的周期性重评估机制, 以“以攻促防”的自主评估能力为支撑。鉴于安全边界动态演化, 建议将进攻性密码分析能力建设纳入国家密码安全体系, 对部署算法参数进行常态化再评估, 防范降维打击。

5) 前瞻布局信创协议迁移与 AI 辅助密码分析。已有研究开始将机器学习用于格基方案的密码分析<sup>[15]</sup>; 建议前瞻布局信创协议栈的抗量子迁移, 并密切跟踪人工智能辅助密码分析的进展。

分认识 PQC 迁移的长期性与复杂性。鉴于量子计算实用化的具体时间表尚不明确, 采取分层级、分阶段、具备渐进验证能力的 PQC 演进方案, 是保障数字基础设施平稳过渡的务实路径。

参考文献 (References)

[1] IBM. IBM lays out clear path to fault-tolerant quantum computing[EB/OL]. (2025-06-10) [2026-04-26]. <https://www.ibm.com/quantum/blog/large-scale-ftqc>.

[2] National Security Agency (NSA). Commercial National Security Algorithm Suite 2.0(CNSA 2.0)Cybersecurity Advisory [R/OL]. (2022-09-07) [2026-04-30]. [https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSA\\_CNSA\\_2.0\\_ALGORITHMS\\_PDF](https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_PDF).

[3] National Institute of Standards and Technology (NIST). NIST releases first 3 finalized post-quantum encryption standards (FIPS 203, FIPS 204, FIPS 205) [EB/OL]. (2024-08-13) [2026-04-26]. <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.

[4] 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.

[5] McEliece R J. A public-key cryptosystem based on algebraic coding theory[J]. *Deep Space Network Progress Report*, 1978, 44: 114-116.

[6] Merkle R C. A digital signature based on a conventional encryption function[C]//*Advances in Cryptology — CRYPTO '87*. Berlin: Springer, 1988: 369-378.

[7] Matsumoto T, Imai H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption[C]//

5 结论

PQC 已从理论研究走向大国数字主权与产业升级的竞争前沿。NIST 标准的发布与中国科技部重点专项的实施表明, 全球数字信任体系的重构已经启动, 量子安全迁移已从技术议题升级为国家数字主权与关键信息基础设施安全的战略必答题。据此, 中国宜走“SM+PQC 双栈融合演进”这一兼顾密码主权、存量兼容与场景优势的独特路径, 以“以攻促防”的自主安全评估能力为支撑、以金融业为先行领域、以分阶段行动路线图为决策落点。面对“先窃取、后解密”攻击常态化以及未来量子算力跃升的潜在风险, 需充

- Advances in Cryptology — EUROCRYPT '88. Berlin: Springer, 1988: 419–453.
- [8] Ajtai M. Generating hard instances of lattice problems [C]//Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. New York: ACM, 1996: 99–108.
- [9] Bos J, Ducas L, Kiltz E, et al. CRYSTALS–Kyber: A CCA-secure module-lattice-based KEM[C]//2018 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway, NJ: IEEE, 2018: 353–367.
- [10] Ducas L, Kiltz E, Lepoint T, et al. CRYSTALS–dilithium: A lattice-based digital signature scheme[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2018(1): 238–268.
- [11] Bernstein D J, Hülsing A, Kibbl S, et al. The SPHINCS+ signature framework[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2019: 2129–2146.
- [12] Regev O. On lattices, learning with errors, random linear codes, and cryptography[J]. *Journal of the ACM*, 2009, 56(6): 1–37.
- [13] Bernstein D J, Bhargavan K, Bhasin S, et al. KyberSlash: Exploiting secret-dependent division timings in Kyber implementations[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2025(2): 209–234.
- [14] Zhao Z Y, Ding J T, Yang B Y. Sieving with streaming memory access[J]. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2025(2): 362–384.
- [15] Bassotto C. ML-based Attack on Module-LWE: Assessing the security of module-lattice-based schemes[D]. Barcelona: Universitat Pompeu Fabra, 2025.
- [16] Xi'an Jiaotong–Liverpool University. XJTLU team breaks its own world record in post-quantum security analysis [EB/OL]. (2026–01–14) [2026–04–26]. <https://www.xjtlu.edu.cn/en/news/2026/01/xjtlu-team-breaks-its-own-world-record-in-post-quantum-security-analysis>.
- [17] Xi'an Jiaotong–Liverpool University. XJTLU's PQC–X lab cracks Kyber challenge[EB/OL]. (2026–03–13) [2026–04–26]. <https://www.xjtlu.edu.cn/en/news/2026/03/xjtlu-pqc-x-lab-cracks-kyber-challenge>.
- [18] Fouque P A, Hoffstein J, Kirchner P, et al. Falcon: Fast-Fourier lattice-based compact signatures over NTRU: Specification v1.2[EB/OL]. (2020–01–10) [2026–04–26]. <https://falcon-sign.info/falcon.pdf>.
- [19] National Institute of Standards and Technology (NIST). NIST CSWP 39: Considerations for achieving cryptographic agility[R/OL]. [2026–04–30]. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.39.pdf>.
- [20] The White House. Sustaining select efforts to strengthen the nation's cybersecurity and amending Executive Order 13694 and Executive Order 14144[EB/OL]. (2025–06) [2026–04–30]. <https://www.whitehouse.gov/presidential-actions/2025/06/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694-and-executive-order-14144/>.
- [21] European Union Agency for Cybersecurity(ENISA). Post-quantum cryptography: Anticipating threats and preparing the future[R/OL]. (2022–10–19) [2026–04–26]. <https://www.enisa.europa.eu/news/enisa-news/post-quantum-cryptography-anticipating-threats-and-preparing-the-future>.
- [22] Korea Post-Quantum Cryptography (KpqC) Competition/NSR. The 2nd Round Final Results of the KpqC Competition[EB/OL]. (2025–01) [2026–04–26]. [https://www.kpqc.or.kr/competition\\_02.html](https://www.kpqc.or.kr/competition_02.html).
- [23] CRYPTREC(Cryptography Research and Evaluation Committees). 電子政府における調達のために参照すべき暗号のリスト(CRYPTREC Ciphers List 2026 Revision) [EB/OL]. [2026–04–26]. <https://www.cryptrec.go.jp/list.html>.
- [24] 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) [2026–04–26]. [https://www.niccs.org.cn/symmbzyjy/tzgg/pc/content/1937422988373135360/content\\_1937422988373135360.html](https://www.niccs.org.cn/symmbzyjy/tzgg/pc/content/1937422988373135360/content_1937422988373135360.html).
- [25] 中国社会科学网. 我国金融行业首个抗量子计算密码领域团体标准发布 [EB/OL]. (2026–04–21) [2026–04–27]. [https://www.cssn.cn/skgz/bwyc/202604/t20260421\\_5981542.shtml](https://www.cssn.cn/skgz/bwyc/202604/t20260421_5981542.shtml).
- [26] Bank for International Settlements(BIS). Project Leap: Quantum-proofing the financial system[EB/OL]. [2026–04–26]. <https://www.bis.org/publ/othp67.htm>.
- [27] Swift. Introduction to Post-Quantum Security / Swift Customer Security Programme (CSP) [EB/OL]. [2026–04–30]. <https://www.swift.com/myswift/services/training/swift-training-catalogue/browse-swift-training-catalogue/introduction-post-quantum-security>.
- [28] 中国电子银行网. 工行完成3类场景抗量子密码算法试点, 以防范量子计算攻击 [EB/OL]. (2024–11–04) [2026–04–26]. <https://www.cebn.net.cn/20241104/102974085.html>.
- [29] 周诚君, 李一, 王启宇, 等. 时不我待: 量子计算威胁、银行业脆弱性与金融系统性风险[M]. 北京: 中国金融出版社, 2026.
- [30] 苏州国芯科技股份有限公司2025年年度报告[R/OL]. [2026–04–27]. [https://static.sse.com.cn/disclosure/listedinfo/announcement/c/new/2026-04-24/688262\\_20260424\\_RMYX.pdf](https://static.sse.com.cn/disclosure/listedinfo/announcement/c/new/2026-04-24/688262_20260424_RMYX.pdf).

## Progress in post-quantum cryptography and China's migration path

ZHOU Chengjun<sup>1</sup>, DING Jintai<sup>2,3</sup>

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

2. Post-Quantum Migration Interdisciplinary Laboratory (PQC-X), Xi'an Jiaotong-Liverpool University, Suzhou 215123, China

3. Special Committee on Post-Quantum Cryptography Migration, Jiangsu Provincial Society for Finance and Banking, Suzhou 215123, China

**Abstract** The public-key cryptosystems represented by Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (ECC) are facing disruptive threats from scalable fault-tolerant quantum computing, and the "harvest-now-decrypt-later" attack pattern further underscores the urgency of post-quantum cryptographic (PQC) migration. In 2024, the U.S. National Institute of Standards and Technology (NIST) formally released the first batch of PQC algorithm standards, launching the quantum-safe upgrade of the global digital security infrastructure. Over the past five years, PQC has made important progress in the dynamic assessment of theoretical security boundaries, the global competition over algorithm standards, and the systematic exploration of industry migration paths. China has also accumulated staged results in the construction of the next-generation commercial cryptography (ShangMi, SM) standard system and pilot applications in key industries. This paper systematically reviews the development history, cutting-edge research breakthroughs and global standardization landscape of PQC, with a focus on the migration practice and exploration in the financial industry, and puts forward policy recommendations such as designating cryptographic agility as a mandatory architectural specification for critical information infrastructure and accelerating the coordination of SM and PQC dual-stack standards to establish a unified migration framework, providing a reference for China's next-stage technical research and standardization deployment.

**Keywords** post-quantum cryptography; quantum computing; cryptographic migration; commercial cryptography standards; cryptographic agility ●



(责任编辑 王志敏)