

特色专题

全球金融基础设施与 SWIFT 网络后量子密码 (PQC) 迁移战略与技术演进

梁蓓¹, 孟圣哲², 常达¹, 覃悦¹, 周旭¹, 李锐³

摘要 后量子密码(post-quantum cryptography, PQC)是用于抵御量子计算机攻击的新一代密码技术,被视为传统金融安全系统的必然替代方向。系统梳理了量子计算时代金融体系面临的系统性威胁,分析了全球 PQC 监管框架演进态势与算法标准化进程,并强调了密码敏捷性的关键作用:主要经济体已普遍将 2030—2035 年设定为经典公钥密码的强制退役窗口,密码敏捷性由此成为金融机构满足合规时间线的先决能力。从核心基础设施的技术博弈、环球银行金融电信协会(Society for Worldwide Interbank Financial Telecommunication, SWIFT)网络的抗量子演进路线、全球头部商业银行的防御体系等多个层次展开深度评估,探讨了解决“数据包膨胀”、混合加密模式下算力挑战与带外证书分发等关键技术难题的思路:国际清算银行(Bank for International Settlements) Project Leap 两阶段实验验证了 PQC 嵌入央行级支付系统核心流程的功能可行性,但 ML-DSA(Module-Lattice-Based Digital Signature Algorithm)等后量子签名带来的近 10 倍报文载荷膨胀与混合模式的双轨验证开销,仍是高吞吐清算环境面临的主要系统性约束;SWIFT 则确立了以 SwiftNet 8.0 为核心节点的分阶段迁移路线。总结了向 PQC 全面过渡的企业级战略部署、时间线跨度及宏观经济效应,指出金融机构的整体迁移周期约需 5~15 年,密码敏捷性建设与跨机构、跨辖区协同是决定迁移成败的关键变量,为现代金融系统的底层架构重组与数字信任体系演进提供参考。

关键词 后量子密码;金融基础设施;SWIFT 网络;密码敏捷性;数字签名

自 20 世纪中叶以来,全球数字经济与现代金融体系的信任根基始终建立在经典密码学之上。以 RSA(Rivest-Shamir-Adleman)、椭圆曲线密码(elliptic curve cryptography, ECC)和 Diffie-Hellman 为代表的公钥密码算法为全球海量的数据传输、身份认证和不可抵赖性提供了底层安全保障。然而,量子计算

的跨越式发展正在彻底颠覆这一基于经典计算复杂度的安全基础。一旦具备足够容错量子比特的“密码学相关量子计算机”(cryptographically relevant quantum computer, CRQC)进入商用阶段,Shor 算法^[1]将在几分钟至几小时内瓦解需要经典计算机演算数千年的公钥密码体系。同时, Grover 算法也将迫使对称加密的密钥长度翻倍才能维持现有的安全边界。关于 CRQC 能够完全攻破现有密码体系的理论时间节点(业界将其称为“Q-Day”),全球科技界与情报机构的预测正在持续提前^[2]。Google 研究团队于 2026 年第

1. 北京雁栖湖应用数学研究院, 北京 101408

2. 清华大学数学科学系, 北京 100084

3. 中国人民银行金融研究所, 北京 100800

收稿日期: 2026-05-13; 修回日期: 2026-08-24

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

作者简介: 梁蓓, 副教授, 研究方向为后量子密码与金融信息安全, 电子邮箱: lbei@bimsa.cn

引用格式: 梁蓓, 孟圣哲, 常达, 等. 全球金融基础设施与 SWIFT 网络后量子密码(PQC)迁移战略与技术演进[J]. 科技导报, 2026, 44(16): 73-84;

doi:10.3981/j.issn.1000-7857.2026.05.00060

一季度将 Q-Day 预期大幅提前至 2029 年,显著短于此前普遍预期的 2030 年中期。与此同时,世界经济论坛(World Economic Forum, WEF)、国际清算银行(Bank for International Settlements, BIS)以及美国麦肯锡咨询公司(McKinsey & Company)等机构亦指出,全容错量子计算机(fault-tolerant quantum computer, FTQC)大概率将在 2028—2035 年间广泛具备破译能力^[3]。这意味着,全球金融体系所剩的准备窗口期正在急剧收窄。

在此紧迫背景下,全球中央银行、国际金融报文网络(如环球银行金融电信协会, Society for Worldwide Interbank Financial Telecommunication, SWIFT)等机构面临双重且极为严峻的量子威胁。第 1 种被广泛认知的攻击路径是“先存储,后解密”(store now, decrypt later, SNDL)。在这一攻击模式下,拥有国家级资源背景的高级持续性威胁(advanced persistent threat, APT)行为体正持续、系统性拦截并海量存储金融业加密数据流量,待量子算力成熟后批量解密。花旗(Citi)在报告中明确指出,若金融机构仅在未来被动部署后量子密码(post-quantum cryptography, PQC),其防护效力只能覆盖升级后产生的新数据流,而已被敌方截获的长生命周期资产(例如长达 30 年的抵押贷款审批记录、国家战略贸易融资信贷档案、代币化资产凭证、涉及国家安全的机密防务转账信息)的保密性将遭到无可挽回的破坏^[4]。目前看来,从根本上对抗这种历史隐私丧失的防御机制是确保数据保密需求期限在量子计算机问世前自然到期,但对于高度依赖长效信任的金融系统几乎无法实现。

除了数据隐私泄露,第 2 种攻击路径——“先信任,后伪造”——对金融基础设施的底层结算逻辑构成了更具灾难性的系统性挑战。所谓“先信任,后伪造”(亦称“先信任、后攻击”),是与 SNDL 互为镜像的另一类量子威胁: SNDL 危及的是加密数据的机密性,而该路径危及的是数字签名所承载的真实性与不可抵赖性。其攻击逻辑在于,攻击者在量子算力成熟之前并不发动任何可见攻击,而是任由目标机构继续使用基于 RSA、ECC 等传统算法的长期签名密钥与数字证书,这些密钥与证书在此期间始终处于系统信任链之内(即“先信任”);待 CRQC 问世后,攻击者即可利用 Shor 算法从公开的公钥或历史签名中反推出

对应私钥,从而以“合法”身份实时伪造支付指令与结算报文,甚至回溯性地篡改历史交易记录,且伪造内容能够无缝通过既有验证机制(即“后攻击”,亦即“后伪造”)。与 SNDL 不同,这一威胁无法通过缩短数据保密期限加以化解,因为其打击对象是信任体系本身:只要根证书、代码签名密钥或成员机构身份凭据等长生命周期信任凭证仍依赖传统公钥算法,整个验证链条便面临被整体接管的风险。如果量子计算能力足以破坏用于身份验证的非对称签名算法,攻击者将能实时伪造跨境结算指令、篡改分布式账本历史区块记录,或劫持银行间的代理验证凭据。一旦历史交易和实时交易的不可否认性被破坏,全球资本市场的流动性信任将面临崩塌风险,进而可能引发波及众多经济体的系统性金融危机。

在此背景下,从经典密码学向 PQC 的全面迁移^[5],绝非一次简单的软件补丁升级或孤立的 IT 运维任务,而是一场涉及硬件加速器、云服务、应用程序编程接口(application programming interface, API)接口规范以及跨国监管协同的全球性密码基础设施协同重构。由于 PQC 算法的底层数学机制与传统密码算法存在本质差异,其密钥与数字签名尺寸显著膨胀,这对长期围绕低延迟与超高吞吐量进行深度优化的现代金融支付网络(如 SWIFT 与 TARGET2)带来了前所未有的技术挑战。在这场波及全球且资源投入极其庞大的架构演进过程中,国际标准化组织、各国金融监管机构、环球银行金融电信协会以及大型跨国银行,正共同摸索着一条充满未知变量的密码学重构之路。

本文采用“监管标准—核心基础设施—商业机构”3 层递进的分析框架:在监管标准层,比较主要经济体公开发布的 PQC 政策文本、算法选型与合规时间线;在核心基础设施层,以 BIS Project Leap 公开实验结果与 SWIFT 官方技术文件为依据,从密钥与签名尺寸、报文载荷、验证开销等可量化维度评估 PQC 对高吞吐支付网络的性能与架构影响;在商业机构层,通过代表性银行的公开试点案例考察量子安全技术的工程落地形态。文中论断所依据的资料均为 2023—2026 年间各监管机构、国际组织、基础设施运营方与商业银行公开发布的政策文件、技术报告与白皮书,并在文末参考文献中一一列出,分析过程可循此复现。

1 全球监管框架演进、算法标准化进程与密码敏捷性指令

面对即将到来的量子霸权,全球标准制定机构、主权国家安全部门以及金融行业监管机构正在加速制定 PQC 合规与标准化拼图。这些自上而下的政策性压力不仅确立了明确的技术演进路线图,更以此倒逼庞大的金融机构立即开展底层密码资产盘点并构建长效的密码敏捷性防御体系。

1.1 国际 PQC 标准成型

凭借长期主导 PQC 标准化进程,美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)已成为 PQC 领域事实上的全球标准制定中枢。在 2024—2025 年的关键窗口期内, NIST 正式确立并发布了 3 项核心抗量子算法联邦信息处理标准(Federal Information Processing Standards, FIPS): 用于密钥建立机制的 FIPS 203(Module-Lattice-Based Key-Encapsulation Mechanism, ML-KEM)、作为通用数字签名主力的 FIPS 204(Module-Lattice-Based Digital Signature Algorithm, ML-DSA), 以及基于传统哈希函数的备用签名方案 FIPS 205(Stateless Hash-Based Digital Signature Algorithm, SLH-DSA)^[6]。

然而,这 3 大核心标准存在庞大的计算开销和数

据体积,从而在 EMV(Europay, Mastercard and Visa)标准的智能银行卡、低带宽物联网支付终端等受限金融场景中显得捉襟见肘。为此, NIST 正在评估并推进第 4 轮附加算法的标准化。此外,诸如 SQIsign 和 HAWK 等正接受学术评估的非标准化候选方案,因其提供了相对大幅缩减的签名尺寸特征,正被金融业视为解决未来网络带宽瓶颈的潜在方案。在应用层面上,互联网工程任务组(Internet Engineering Task Force, IETF)等组织正积极将上述 PQC 算法集成到诸如传输层安全协议(TLS 1.3)和安全外壳协议(Secure Shell, SSH)等骨干网络协议之中,旨在为商业产品和现代数字系统奠定坚实且具备广泛互操作性的底层安全基石^[7]。

1.2 跨国监管强制力的时间表与地缘合规差异

在美洲、欧洲及亚太等核心金融市场,监管机构通过行政命令或行业规范设定的 PQC 合规时间节点正变得空前明确和强硬。2026 年被普遍定义为“规划与盘点元年”,而 2030—2035 年则被确立为强制淘汰经典密码算法并全面转向 PQC 算法的“关键过渡窗口期”。

表 1 系统梳理了当前全球主要经济体及核心网络机构在 PQC 迁移中的监管框架、首选算法体系以及关键迁移阶段与合规时间线。

表 1 全球主要经济体或核心机构 PQC 迁移概况

监管辖区或主导机构	核心政策与指导框架	PQC 首选算法体系	关键迁移阶段与合规里程碑时间线
美国	国家安全局(NSA) CNSA 2.0; 2025 年 1 月总统行政令; OMB 授权指令	NIST FIPS 系列标准	2025 年: 新版软件及固件数字签名必须迁移至 PQC 2026 年: VPN、路由器等传统网络通信设备实现 PQC 支持; 联邦机构完成密码资产清单清点 2030 年: 全面开始淘汰无法支持 CNSA 2.0 的遗留业务系统; 高风险系统全面开始切换 2035 年: 所有国家安全系统(NSS)与关键基础设施彻底实现抗量子化
欧盟	欧洲协同 PQC 路线图; 数字运营弹性法案(DORA); 网络与信息安全指令 2(NIS2)	NIST 标准为主, 兼顾欧洲本地验证算法	2026 年底前: 成员国必须完成对国家级初始过渡路线图的制定, 启动资产识别与高危用例的初步盘点 2030 年底前: 所有高风险金融用例及关键金融基建必须默认升级至 PQC 机制, 并完成资源分配与沙盒试点 2035 年底前: 尽可能全面完成剩余数字生态系统的量子安全过渡
澳大利亚	澳大利亚信号局(ASD) 信息安全手册	NIST FIPS 系列标准	2026 年底前: 机构必须制定经过充分改进与验证的全面过渡计划 2028 年底前: 开始对涉及国家和金融命脉的关键系统及核心数据启动实质性迁移进程 2030 年底之后: 绝对禁止在关键系统框架内继续使用传统非对称密码学算法

表 1 全球主要经济体或核心机构 PQC 迁移概况 (续)

监管辖区或主导机构	核心政策与指导框架	PQC首选算法体系	关键迁移阶段与合规里程碑时间线
加拿大	加拿大通信安全局 (CSE)PQC指南与采购指引	NIST FIPS系列标准	2026年4月起: 制定部门级别的初始迁移规划,并要求从此开始建立年度PQC进度强制报告机制 2031年底前: 必须彻底完成高风险、高优先级骨干系统的PQC替换 2035年底前: 完成全社会剩余网络系统的过渡
中国	国家密码管理局等机构 (中国特定标准体系)	国家自研商用密码 (China Specific)	2025年10月—2026年6月: 启动国内主导的PQC算法提交、选型与验证评测工作;后续将结合国密标准制定强制性的国家级PQC演进路线图
SWIFT网络	SWIFT全球报文演进战略	兼容NIST与国际通用标准	2025年11月: 启用混合邮政地址等底层数据结构改革 ^[8] 2027年: 发布全面具备PQC支持能力的SwiftNet 8.0版本,并在其前后执行为期约15个月的高强度全球网络节点迁移窗口期

注: NSA为美国国家安全局(National Security Agency); CNSA 2.0为商用国家安全算法套件2.0(Commercial National Security Algorithm Suite 2.0); OMB为美国行政管理和预算局(Office of Management and Budget); VPN为虚拟专用网络(Virtual Private Network); NSS为国家安全系统(National Security Systems); DORA为《数字运营弹性法案》(Digital Operational Resilience Act); NIS2为《网络与信息安全指令2》(Network and Information Security Directive 2); ASD为澳大利亚信号局(Australian Signals Directorate); CSE为加拿大通信安全局(Communications Security Establishment)。

表 1 揭示了一个严峻的国际协作挑战^[9]: 尽管大多数西方国家在算法选择上向 NIST 标准靠拢,但地缘政治考量促使部分国家(如中国)推行自主研发的特定商用 PQC 标准。这种算法标准的地理与司法管辖权断裂,为全球性商业银行制造了难以跨越的鸿沟。跨国银行不仅需要维持与 NIST 标准体系的互操作性,还必须在局部区域网络中兼容完全不同的密码逻辑。对此,WEF 发布的研究报告《金融行业量子安全: 为全球监管方法提供信息参考》(Quantum security for the financial sector: Informing global regulatory approaches)强烈呼吁各国监管者秉持“避免碎片化”原则,通过知识共享和政策互认机制,防范因地缘政治导致密码孤岛效应,以确保跨境金融系统底层互操作性的连续性与平滑性^[10]。

1.3 密码敏捷性(crypto-agility)的核心地位

在应对错综复杂的监管要求与算法迭代时,“密码敏捷性”成为金融机构生存的核心哲学。正如美国国家网络安全卓越中心(National Cybersecurity Center of Excellence, NCCoE)和金融服务信息共享与分析中心(Financial Services Information Sharing and Analysis Center, FS-ISAC)所强调的,现代金融机构必须彻底摒弃过去将特定密码算法“硬编码”到程序底层的传统开发模式^[11]。真正的密码敏捷性要求系统架构能够在模块化、零信任的框架内实现底层密码算法的即插即用和快速轮换,以便在 NIST PQC 标准被发现漏

洞或监管指令突变时,无缝切换至备用算法而无需中断核心金融业务。构建此类敏捷能力的前提是利用自动化密码盘点工具对银行内部和云环境中散落的所有证书、密码调用、数据库连接及第三方 API 进行彻底的摸底排查,这也是目前大多数银行在规划其第 1 阶段战略时的重中之重^[12-14]。

2 核心基础设施的技术博弈:BIS Project Leap 与支付网络的性能大考

在宏观金融基础设施体系中,SWIFT 跨境金融报文网络(其自身承担报文传递职能,并不直接完成资金的清算与结算)与由各国央行运营的实时全额支付系统(real-time gross settlement, RTGS)共同支撑着全球资金清算、结算与跨境支付的信息传递和价值转移过程。此类系统具有高并发、低时延、高可用和强合规等典型特征,因此其密码迁移不仅是算法替换问题,更涉及底层通信协议、报文格式、证书体系、遗留系统兼容性以及运行风险控制等多维度约束。为评估 PQC 在真实金融基础设施环境中的部署可行性,BIS 创新中心发起了 Project Leap。该项目围绕央行级支付系统的后量子迁移开展实验验证,重点评估了 PQC 在关键金融基础设施中的协议适配性、运行性能、系统兼容性与部署边界,其实验结果为金融支付网络的后量子升级提供了重要工程依据^[15]。

2.1 Project Leap 的阶段性演进:从安全通信隧道到核心清算网络

作为 BIS 创新中心面向金融基础设施后量子迁移开展的重要实验项目, Project Leap 采用分阶段验证路径, 逐步将测试范围从跨 IT 中心的安全通信通道扩展至中央支付系统的核心业务流程。第 1 阶段实验由 BIS 创新中心联合法国央行和德国联邦银行开展, 主要目标是在位于巴黎和法兰克福的服务器之间建立同时支持传统公钥密码算法与 PQC 算法混合机制的虚拟专用网络隧道。该阶段实验表明, 在 2 个相互分离的 IT 中心之间, 引入传统公钥密码与 PQC 算法并行运行的混合机制, 可以在保持现有通信架构兼容性的同时, 增强支付报文传输通道面对量子计算攻击时的长期安全性, 从而为后续面向核心支付系统的进一步实验奠定基础^[16-21]。

在通信通道层面完成初步验证后, Project Leap 第 2 阶段将关注重点转向中央支付系统核心业务流程中的密码机制替换与系统适配问题。该阶段成果于 2025 年 12 月正式公布, 参与方在 BIS 创新中心、法国央行和德国联邦银行的基础上, 进一步扩展至意大利央行、支付服务商 Nexi、网络服务商 Colt 以及全球金融报文基础设施提供方 SWIFT。不同于第 1 阶段主要验证安全通信隧道的后量子迁移可行性, 第 2 阶段以欧元区 TARGET2 系统相关业务场景为实验对象, 重点考察后量子数字签名机制在中央支付系统流动性调拨与清算处理流程中的功能正确性、系统兼容性与性能影响。在该阶段实验中, 测试团队不只对外层通信通道进行加固, 而是进一步触及支付报文验证和权限确认等核心处理环节。具体而言, 项目组对传统数字签名验证机制进行了替换性测试, 将部分验证功能迁移至 PQC 协议框架下, 并相应修改了大量基础设施的底层系统组件, 以满足新型密钥、签名和证书结构的兼容性要求。实验结果显示, 预设业务场景均能够正确执行, 说明 PQC 机制在世界级支付系统关键业务流程中的嵌入具有一定的工程可行性。

然而, 功能层面的可行性并不意味着工程部署层面的直接可替换性。第 2 阶段测试同时揭示出 PQC 与传统公钥密码之间显著的性能差异。相较于传统签名算法, 后量子签名算法通常具有更大的密钥尺寸、更长的签名长度、更复杂的证书链结构以及更高

的验证开销。这些因素在中央清算系统的高并发业务环境中会被进一步放大, 可能导致消息处理延迟上升、缓冲区压力增加、验证链路拥塞以及整体吞吐能力下降等问题。

因此, Project Leap 第 2 阶段的意义不仅在于验证了 PQC 在特定业务流程中的功能适配性, 更在于揭示了 PQC 进入关键金融基础设施时所面临的系统级约束。对于中央支付系统而言, 后量子迁移并非单一密码模块的等价替换, 而是涉及算法性能、报文结构、证书体系、验证链路、系统架构与业务连续性保障的全链路重构过程。其核心挑战在于, 如何在破坏金融基础设施安全性、稳定性和连续性的前提下, 将后量子安全能力嵌入既有支付网络的关键运行环节之中。

2.2 后量子签名尺寸增长及其系统性能约束

Project Leap 第 2 阶段中观察到的延迟增加和性能下降, 并非主要源于实现层面的缺陷, 而是与 PQC 算法本身的结构特征密切相关。相较于基于整数分解或离散对数问题的传统公钥密码, 许多后量子签名方案为了抵御量子攻击, 需要使用更大的公钥、更长的签名以及更复杂的证书结构。密码对象尺寸的显著扩张会直接改变金融报文在传输、缓存、解析和验证过程中的资源占用特征, 并由此形成报文载荷膨胀问题。

如图 1^[22]所示, 传统 RSA-2048 的公钥和签名长度通常约为 256 B。长期以来, SWIFT 报文网络、央行支付系统及其相关中间件的通信协议、缓存机制和验证流程, 通常是在传统公钥、签名和证书体积较小的前提下设计和优化的。较小的密钥和签名体积降低了单笔报文的传输与处理负担, 使高频支付清算网络能够在严格时延约束下维持较高的并发吞吐能

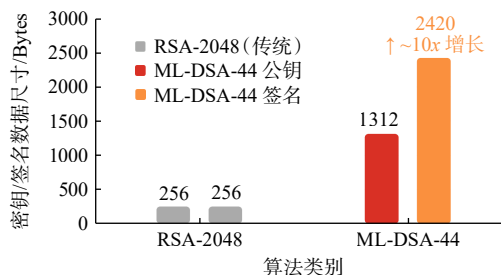


图 1 传统算法与 PQC 算法的物理尺寸对比:
数据包膨胀的根源

力。相比之下, NIST 标准化的 ML-DSA-44 在相近安全等级下具有更大的公钥和签名尺寸, 其公钥长度约为 1312 B, 签名长度约为 2420 B。由此可见, 仅从单笔报文所携带的签名相关数据看, 后量子签名机制相较于传统 RSA 签名已经可能带来数倍至近 1 个数量级的载荷增长。在央行级支付基础设施每秒处理大量报文的场景中, 这种单笔载荷扩张会被高并发业务流持续放大, 并进一步传导至网络传输、消息队列、缓冲区管理和签名验证等多个环节, 从而形成系统级性能压力^[23]。这种报文载荷膨胀在遗留支付系统中还会进一步表现为接口边界和处理边界的适配问题。Project Leap 的测试结果显示, 较长的 PQC 签名可能触及甚至突破既有系统预设的最大报文长度、缓冲区容量或消息处理限制, 进而引发报文解析失败、队列阻塞、验证延迟上升以及异常处理频率增加等问题。

进一步看, 后量子签名长度增加对支付系统性能的影响并不局限于单笔报文传输字节数的增加。对于金融支付这类连续、密集且对尾部时延高度敏感的交易数据流, 签名长度增加会延长报文完整到达所需时间, 并推迟后续的完整性检查、签名验证和业务确认流程。此外, Amazon 的相关研究指出, PQC 算法在传输阶段可能因签名长度较长而显著增加最后字节到达时间, 从而在高负载条件下放大端到端处理时延和峰值时延波动^[24]。因此, PQC 在金融基础设施中的性能瓶颈并非单纯来自算法计算复杂度, 而是由公钥、数字签名和证书尺寸、报文格式、网络传输、缓存机制、证书链管理和验证调度共同作用形成的系统性约束。对于 SWIFT 网络和央行级支付系统而言, 后量子迁移必须同时评估密码安全强度与基础设施承载能力之间的匹配关系, 否则算法层面的安全性增强可能转化为报文处理链路中的吞吐瓶颈和运行风险。

2.3 混合加密模式(hybrid mode)的工程代价与过渡创新方案

在后量子迁移的过渡阶段, NIST、CISA 等标准化与网络安全机构以及互联网产业界普遍建议采用混合模式。该模式的基本思想是在同一系统、同一通信会话或同一交易流程中, 同时使用传统公钥密码算法与 PQC 算法, 以降低单一密码体系切换所带来的安全和兼容性风险。一方面, PQC 组件能够为系统提

供面向量子计算攻击的长期安全能力; 另一方面, 传统密码组件仍可依托其长期应用积累和成熟的安全性分析, 在 PQC 算法尚未经充分长期检验的阶段提供安全冗余。同时, 混合模式也有助于维持与尚未完成升级的遗留系统之间的互操作性, 从而降低金融基础设施分阶段迁移过程中的协调成本。

然而, 当混合模式被引入至中央清算系统等高吞吐基础设施时, 其工程代价十分显著。混合模式通常要求系统同时处理 2 套密钥体系、2 类签名对象、2 条证书链以及相应的验证逻辑。这不仅增加了单笔报文的载荷体积, 也显著提高了签名验证、证书解析、路径构建和撤销检查等环节的计算与内存压力。BIS 相关测试表明, 在缺乏底层架构改造的情况下, 要求核心处理链路同时完成传统签名和后量子签名验证, 将对现有系统吞吐能力构成较大挑战。为维持测试环境下的可操作性, Project Leap 第 2 阶段采用了双重路由和分流处理机制, 将入站报文分别送入传统算法验证路径与 PQC 验证路径。该方法在实验中能够缓解单一路径上的处理压力, 但其本质是以额外的系统复杂性换取迁移可行性。双轨验证不仅增加了计算资源的消耗, 也会由于双重签名和双重证书链的存在进一步放大报文载荷膨胀问题。因此, 混合模式虽然是后量子迁移阶段的重要风险缓释策略, 但在高性能金融基础设施中的应用必须与系统架构优化、网络资源规划和证书体系重构同步推进。

在上述背景下, 学术界和金融科技产业界开始探索更具工程可行性的过渡方案, 其中具有代表性的是签名压缩与带外证书分发机制。传统安全协议通常在握手或交易认证过程中携带完整证书链, 以支持接收方进行端到端的身份验证和信任路径构建。与此不同, 带外证书分发方案试图将完整 PQC 证书链的分发、缓存和验证过程从单笔交易报文中剥离出来, 转由银行支付网关、代理服务器或其他网络边缘节点预先完成。交易报文在实时传输过程中仅携带压缩后的认证标识符、证书引用或短标签, 从而降低单笔报文的直接网络载荷。该方案在理论上能够有效缓解 PQC 证书链尺寸过大带来的传输压力, 并有助于降低高频交易环境中的尾部时延。然而, 其大规模部署也提出了新的基础设施要求。首先, 金融机构之间需要建立高度协同的全局证书分发、缓存更新和生命

周期管理机制。其次,系统必须支持低时延、强一致的证书撤销与状态同步,以避免被撤销或过期的证书继续被交易节点接受。最后,带外证书分发还需要解决跨辖区监管、信任锚管理、证书版本控制以及异常状态回退等问题。因此,该方案虽为后量子迁移提供了重要优化方向,但其实现依赖于更复杂的公钥基础设施(public key infrastructure, PKI)治理体系和跨机构基础设施协同机制,在现有支付清算体系中仍需进一步验证和完善^[25]。

值得说明的是,上述3项要求在SWIFT现有体系中已有部分对应机制,但尚不能完全满足带外分发场景的需要。其一,就全局证书分发与生命周期管理而言,SWIFT长期运营着一套封闭的公钥基础设施(SWIFTNet PKI):证书由SWIFT统一签发,成员机构通过Alliance系列接入组件与硬件安全模块完成密钥生成、证书申请、续期与托管,网络内的证书注册与吊销遵循统一规则,这意味着在SWIFT封闭网络内部,“高度协同的全局证书分发与生命周期管理”已具备组织与技术雏形。其二,就撤销与状态同步而言,SWIFTNet PKI主要依托集中式证书撤销列表(certificate revocation list, CRL)的周期性发布与缓存实现撤销状态传播,尚达不到带外分发所要求的低时延、强一致的实时同步能力,而PQC迁移后更大的证书对象与更频繁的算法轮换将进一步放大这一差距。其三,就跨辖区治理而言,SWIFT现有信任锚高度集中于其自营证书机构,并辅以关系管理应用(relationship management application, RMA)管理机构间的报文交换授权,这一模式在单一信任域内行之有效,但带外分发所要求的跨辖区多信任锚治理、证书版本控制与异常回退机制,已超出现行单一封闭信任模型的覆盖范围。因此,SWIFT既有PKI为带外证书分发提供了可资扩展的制度与设施基础,而实时撤销一致性与跨辖区信任治理,则是其向PQC演进过程中必须补齐的能力短板。

综上所述,Project Leap表明,PQC在关键金融基础设施中的应用不是单一密码模块的替换过程,而是涉及报文结构、验证链路、证书体系、网络吞吐与跨机构协同的系统性迁移工程。对于SWIFT网络而言,这一迁移过程还将受到全球成员机构异步升级、跨境监管要求、报文标准兼容性以及金融业务连续性

约束的共同影响。因此,下一章将以SWIFT网络为具体对象,进一步分析其后量子演进路线及关键技术挑战。

3 SWIFT网络的后量子演进路线

Project Leap的第2阶段为SWIFT网络的后量子迁移提供了重要的工程参照。该项目并未停留于安全通信隧道层面的验证,而是在欧洲支付系统相关环境中考察后量子数字签名机制对嵌入央行间流动性调拨流程后的功能正确性、系统兼容性与性能影响。其实验结果表明,PQC在特定业务场景中的功能可行性并不意味着生产环境可以直接完成密码体系切换;运行性能、系统互操作性、证书体系适配以及密码敏捷性,构成后续大规模迁移的关键约束。作为维系全球1万多家金融机构、主导绝大部分跨境银行间支付报文传输与结算指令交换的骨干枢纽,SWIFT的后量子迁移不仅关系到自身网络协议和安全机制的升级,也将影响成员机构、代理行、市场基础设施以及监管主体之间的协同节奏。因此,SWIFT已将后量子迁移纳入其网络升级路线,而且SWIFT网络的后量子演进不能被理解为单一密码算法的替换,而应被视为覆盖通信通道、身份认证、证书体系、终端接入、报文处理和跨机构互操作的系统性迁移工程。根据SWIFT对外披露的材料显示,SwiftNet 8.0预计于2027年发布,并将作为支持PQC能力的升级网络版本;相关Alliance产品线也将围绕该版本安排迁移路径,客户需在约15个月迁移窗口内完成接入侧准备。与此同时,SWIFT报文体系自身正处于结构性升级窗口:跨境支付报文已于2025年11月完成从传统MT格式向基于ISO 20022国际标准的MX格式的整体切换^[26],其更丰富的结构化数据模型为未来在报文层承载PQC签名扩展字段、证书引用等新增密码学元素预留了空间,也使报文标准迁移与密码体系迁移在时间与工程上相互耦合,进一步凸显了统筹规划的必要性。这一安排表明,SWIFT网络的底层密码迁移需要以分阶段、可回退和可协调的方式推进,而难以采取一次性整体替换路径。

在这一背景下,SWIFT于2025年8月17日正式发布了《SWIFT PQC迁移综合实施指南》(SWIFT PQC

Migration Comprehensive Implementation Guide)。该指南系统阐述了 SWIFT 向 PQC 迁移的结构化方案,涵盖量子威胁剖析、监管考量及分阶段实施策略,为相关决策者与技术团队提供切实可行的行动指引。该指南的核心是一套总周期为 16~22 个月的 5 阶段实施计划:第 1 阶段为迁移前的差距评估、算法选择与战略制定,第 2 阶段为混合加密方案的设计与集成开发,第 3 阶段为在隔离环境与 SWIFT 测试环境中的验证,第 4 阶段为生产环境中的分阶段部署与实施,以及第 5 阶段为部署后的性能优化、合规性监控与密码敏捷性框架建设。该计划与 SWIFT 此前宣布的 15 个月全球节点迁移窗口期基本吻合^[27]。

在该指南中,SWIFT 明确指出需要克服的根植于全球金融生态系统深层结构中的系统性 4 大核心实施挑战与建议解决方案。(1) PQC 算法的计算资源消耗远超传统算法,并需要更大的密钥和签名,因此建议采用硬件加速(如专用集成电路 ASIC、现场可编程门阵列 FPGA)、优先保障高价值交易的 PQC 保护,并对网络配置进行针对性优化。(2) 大量仍在运行的旧版 SWIFT 接口因硬编码的加密假设或有限的可扩展性而难以直接适配 PQC 算法,从而带来系统兼容性问题。指南建议部署加密转换网关作为过渡桥梁,制定优先级更换计划,并对短期内无法升级的系统实施补偿性控制措施。(3) SWIFT 面临的最艰巨挑战是克服其生态系统内的跨机构、跨辖区协调难题。一笔典型的跨境支付并非在 2 个机构间直接完成,而是需要经过发起行、代理行、SWIFT 网络、接收行、受益行及相关市场基础设施等多个节点,每个节点又受限于各自的监管规则、证书体系、硬件安全模块(hardware security module, HSM)能力和升级周期。在此背景下,PQC 迁移的主要风险不在于某一机构能否率先部署抗量子算法,而在于整条支付链条能否在同一窗口期内保持兼容。这一挑战具体表现为 4 类可能的错配:算法错配(一方已支持 PQC 混合握手,另一方仍只支持 RSA 或 ECC)、证书错配(不同机构采用的证书格式、验证库和生命周期管理规则不一致)、能力错配(大型银行可较早升级 HSM 和网关,但中小机构、代理行和部分基础设施节奏较慢)、监管错配(不同司法辖区对算法退役时间、PQC 接受范围及审计规则的要求不完全一致)。针对上述挑战,指

南建议尽早与主要交易对手沟通迁移计划、延长混合模式的维护窗口期,并积极参与行业工作组以协调步伐。(4) 由于 NIST 的 PQC 标准化工作仍在推进之中,目前选择的算法可能在数年后因新漏洞或更优方案的出现而面临修订,指南强调必须建立“密码敏捷性”框架,即将加密操作与具体算法分离以建立密码敏捷性,设计参数可调性,并持续跟踪行业论坛动态。

4 全球头部商业银行的前沿防线:从代币化资产保护到量子密钥分发(quantum key distribution, QKD)

在国际组织和中央银行致力于重构底层互操作网络的同时,大型跨国商业银行并未坐以待毙。由于“先存储、后解密”威胁的日益紧迫,摩根大通(JPMorgan Chase)、汇丰银行(Hongkong and Shanghai Banking Corporation, HSBC)、高盛集团(Goldman Sachs)等金融巨头正积极与国际商业机器公司(International Business Machines Corporation, IBM)、亚马逊云科技(Amazon Web Services, AWS)、东芝(TOSHIBA)、Quantinuum、英国电信集团(BT Group)等顶级科技供应商结成具有深厚排他属性的定制化研发联盟,力争在其外围高频业务、内部数据中心通信以及前沿数字资产应用领域率先落地并试验量子安全技术^[28-29]。

4.1 摩根大通:构建基于物理层防护的量子密码敏捷网络

在全球投资银行界,摩根大通的防御姿态尤为激进^[30]。2024 年 5 月,该行宣布其技术团队已成功部署了一个全功能的高速“量子安全密码敏捷网络”(quantum-secured crypto-agile network, Q-CAN),实现了 2 个分离数据中心之间基于物理光纤的高强度互联。该项目的开创性意义在于其验证了金融业应对量子危机的“双重补救战略”,即将依赖复杂数学算法的 PQC 与基于量子物理测不准原理的 QKD 技术进行了深度融合。在东芝和 Ciena Corporation 公司量子光子学技术的支持下,摩根大通在单根高达 100 Gb/s 带宽的光纤上,成功运用 QKD 分配的高熵物理密钥,保卫大量并发、独立的虚拟专用网络(virtual private network)流量,且未触发明显的业务延迟崩溃。这一

工程实践标志着 QKD 这种以往被认为昂贵和受制于传输距离的前沿技术,正式跨越了实验室的理论门槛,成功证明了其能够融入并支撑金融服务业对实时海量并发具有极致要求的生产级高速任务环境。

4.2 汇丰银行:重塑代币化实物资产防护圈与量子辅助交易

作为传统银行体系中拥抱前沿资产数字化的代表,汇丰银行展现了在应用端对抗量子威胁的另一极。为了消除高净值客户对下一代资产数字化的隐忧,汇丰成功完成了全球首个将量子安全技术应用于代币化实物黄金买卖的真实环境防御试验^[31]。该项目引入了全栈量子计算公司 Quantinuum,依托其名为 Quantum Origin 的量子物理随机性生成技术及全套的 PQC 算法标准,对黄金代币等珍贵的底层数字资产实施了全方位数据防护验证。该试验不仅限于单一内网环境,还深度测试了在不同分布式账本架构下使用 PQC 安全移动数字资产的互操作能力,以及将汇丰黄金代币与以太坊标准 ERC-20 可替代代币进行无缝双向转换的技术闭环。

4.3 国家沙盒内的探索局限:新加坡金融管理局(Monetary Authority of Singapore, MAS)联合项目

国家意志的直接介入并协同商业银行进行规模化沙盒验证,也成为了全球量子防御网格布局的一大显著趋势。2025 年 9 月, MAS 联合星展银行(Development Bank of Singapore, DBS)、汇丰银行、华侨银行(Oversea-Chinese Banking Corporation, OCBC)及大华银行(United Overseas Bank, UOB)等核心机构,在 SPTel 和 SpeQtral 两家量子网络新锐企业的协助下,成功完成了针对 QKD 机制在全岛金融部门高危通讯场景下应用效能的深度概念验证(proof of concept, PoC)沙盒实验^[32]。该项目成功证明了 QKD 体系能够作为高安全等级的通信管道,保护金融机构与高度机密数据中心之间的信息传输。然而, MAS 随之发布的技术评估报告冷静地指出了 QKD 商用化的诸多痛点。报告指出,当前 QKD 技术在电信网络层的集成中依然缺乏统领全局的协议标准,尤其在如何构建防物理篡改、可实时审计的“可信中继节点系统”,以及如何在异构设备厂商间建立畅通的横向互操作性等核心命题上,业界需付出的协调精力甚至大于技术攻关本身。德勤(Deloitte)在其最新的行业研究简报

中也做出精准判断:受制于部署极度专门化的重资产物理硬件要求及高昂资本支出, QKD 在可预见的 5 年内都不太可能成为惠及中小金融机构的普适性基座方案。更为理性且符合商业逻辑的实施路径是分层防御机制,即政府核心设施和头部金控集团将 QKD 作为特定极高密级场景的顶级附加组件,而海量商业与零售级通信流量则依靠具备高度密码敏捷性的 PQC 进行广泛部署^[33-34]。

5 企业级迁移战略部署、时间线跨度与宏观经济效应

向 PQC 的全面过渡,被公认为一项从密码学延伸至企业管理、预算治理、人力资源储备以及 IT 供应链审核的综合性组织行为工程。企业管理层若轻视其难度,将可能导致灾难性的业务断崖与合规崩盘。

5.1 打破时间幻觉:极度漫长的基础设施重组周期

金融机构决策层极易陷入一种历史经验主义的误区,认为此次升级不过是从 SHA-1 迁移至 SHA-2 的翻版。然而,多层次综合建模分析彻底打破了这种不切实际的乐观情绪。历史上的加密机制转型往往只需更换软件函数库配置参数,但本次 PQC 迁移的本质,如同在飞行途中更换飞机的发动机——必须在旧系统维持高并发运转的同时,将底层核心密码逐步替换为量子安全架构。多项行业分析与学术研究^[4,25-37]对底层硬件加速器更换成本(如 HSM 模块)、云计算厂商的退出与兼容策略、密码学高级工程师存量稀缺、可用合规预算上限以及跨企业点对点网络同步要求等多重因素进行了详尽分析,刻画出一条漫长且充满挑战的迁移基准时间线:在保障业务基本不受灾难性冲击的前提下,即便是小型金融科技企业,其过渡周期也需长达 5~7 年;对于业务线庞杂、老旧系统积重难返的中型区域性商业银行而言,这一数字将攀升至 8~12 年;而对花旗、摩根大通这样的大型跨国金融集团而言,若无强力的国家政策补贴支持,全面的后量子重塑历程甚至将超过 15 年。在这漫长的十余年中,商业银行不仅要承担旧有硬件更换带来的海量设备沉没成本,更要经受为维持 API 兼容性而被迫进行的无止境互测试认证。对于高度依赖嵌入式设备和物联网支付终端的机构,问题更加棘手——

加密加速器在芯片流片时已物理固化,软性算法替换可能直接导致终端算力过载甚至瘫痪,引发区域性业务中断恐慌^[22]。

5.2 战略框架重塑:WEF 四阶段指南

为避免全球金融行业在迁移压力下面临的失序与市场失灵风险,WEF 联手顶尖咨询机构提出了应对系统性量子威胁的 4 项宏观指导原则,即“复用与改造(优先利用既有网络安全框架)”“划定不可妥协底线(设定强制性的 PQC 基准规范)”“全力避免生态碎片化(推动监管互信与跨国互操作性)”以及“提高信息透明度”。在这些原则的统领下,WEF 向全球金融首席信息安全官(chief information security officer, CISO)和董事会推介了一条具备可执行性和高度逻辑严密性的 4 阶段战略部署路线^[10,28]。

1) 第 1 阶段:评估与筹备期。在 2026 年合规截止日期前,当务之急是对高管及技术人员进行密集量子危机教育,以消除认知盲区。更核心的任务是利用先进的嗅探工具对企业 IT 资产执行一次彻底的加密应用普查与建档,摸清传统加密算法的整体部署情况,以形成准确的基线图谱。

2) 第 2 至第 3 阶段:策略明晰与执行辅导期。机构需在此期间根据风险敞口的严重程度,制定有针对性的迁移战略。对于涉及代币化资产清算、长期跨境贷款合同归档等长生命周期、高频高净值的系统,应实施重点监控并分配专项迁移预算。

3) 第 4 阶段:全面重构与持续监测演进期。这一阶段包括在生产环境中部署混合加密机制,对异常流量进行持续监测与回溯分析,并建立敏捷的架构迭代机制,以紧跟 NIST 备选标准的更新步伐。WEF 明确指出,主权国家的监管当局不应只扮演惩罚者的角色,更应考虑出台具有建设性的政策支持乃至财务激励机制,以提升无力独立承担升级成本的中小型金融机构的防御能力,从而堵住整个金融供应链防线上的脆弱缺口。

6 结论

综上所述,量子计算的成熟引发的绝不是单纯的技术迭代危机,而是数字化时代以来最大规模的信任根基动摇。目前,以 NIST 和 NSA 主导的 PQC 标准

虽然已在理论层面成熟,但其较大的密文体积,对追求轻量高效、快速互联的全球金融支付清算架构构成了严峻挑战。BIS Project Leap 在欧元区 TARGET2 环境下的测试^[16]表明:简单直接的硬性系统替换难以奏效;唯有通过全行业层面的协议优化革新(如结构化变长报文、大规模带外证书分发及并行路由缓存技术),坚决部署基于多路径分布式的密码敏捷性框架,方能满足金融交易对微秒级延迟的严苛要求,保障系统平滑过渡。在这场波及数 10 万亿美元资产、横跨 10~15 年,且各国司法与监管体系必须在高度不信任的世界格局中携手避免生态断裂的宏大历史工程面前,警钟已经敲响,按业界较为激进的预测,距离 CRQC 问世可能已不足 4 年,所有的金融决策者、首席安全官及全球交易网络在这紧迫窗口期内必须立刻放弃观望,以透明、果断、开放互联的姿态投身这场重构浪潮,这已成为整个现代信用社会不被历史无情淘汰的关键路径。

参考文献(References)

- [1] 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.
- [2] Mosca M. Cybersecurity in an era with quantum computers: Will we be ready?[J]. *IEEE Security & Privacy*, 2018, 16(5): 38–41.
- [3] McKinsey & Company. Quantum technology use cases as fuel for value in finance[EB/OL]. [2026–08–20]. <https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/tech-forward/quantum-technology-use-cases-as-fuel-for-value-in-finance>.
- [4] Citi Institute. Quantum threat: The trillion-dollar security race is on[R/OL]. [2026–08–20]. https://www.citigroup.com/rcs/citigpa/storage/public/Citi_Institute_Quantum_Threat.pdf.
- [5] Bernstein D J, Lange T. Post-quantum cryptography[J]. *Nature*, 2017, 549(7671): 188–194.
- [6] National Institute of Standards and Technology. Post-quantum cryptography[EB/OL]. [2026–08–20]. <https://www.nist.gov/pqc>.
- [7] Crockett E, Paquin C, Stebila D. Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH[C/OL]. Proceedings of the 2nd NIST PQC Standardization Conference. (2019–08–01) [2026–08–20]. <https://csrc.nist.gov/CSRC/media/Events/Second-PQC-Standardization-Conference/documents/accepted-papers/stebila-prototyping-post-quantum.pdf>.

- [8] SWIFT. Hybrid postal address[R/OL]. (2025-07-01) [2026-08-20]. https://www.swift.com/sites/default/files/files/pmpg-hybrid-postal-address-v1.06_202507.pdf.
- [9] GSMA. Post Quantum Government Initiatives by Country and Region[EB/OL]. (2026-02-23) [2026-08-20]. <https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/>.
- [10] World Economic Forum. Quantum security for the financial sector: Informing global regulatory approaches[R/OL]. [2026-08-20]. https://www3.weforum.org/docs/WEF_Quantum_Security_for_the_Financial_Sector_2024.pdf.
- [11] National Institute of Standards and Technology NCCoE. Migration to post-quantum cryptography[EB/OL]. [2026-08-20]. <https://www.nccoe.nist.gov/applied-cryptography/migration-to-pqc>.
- [12] Cryptomathic. A banker's guide to quantum safe cryptography—Part 3: Roadmap to PQC migration for financial institutions[EB/OL]. [2026-08-20]. <https://www.cryptomathic.com/a-bankers-guide-to-quantum-safe-cryptography-part-3-roadmap-to-pqc-migration-for-financial-institutions-cryptomathic>.
- [13] Cybersecurity and Infrastructure Security Agency. Strategy for migrating to automated post-quantum cryptography discovery and inventory tools[R/OL]. (2024-09-01) [2026-08-20]. <https://www.cisa.gov/sites/default/files/2024-09/Strategy-for-Migrating-to-Automated-PQC-Discovery-and-Inventory-Tools.pdf>.
- [14] Sasivehalli S. Post-quantum cryptography: Reading the signals[EB/OL]. Medium. [2026-08-20]. <https://medium.com/@sasivehalli/post-quantum-cryptography-reading-the-signals-debb33c3b18e>.
- [15] Bank for International Settlements. Project Leap: Quantum-proofing the financial system[EB/OL]. (2023-06-01) [2026-08-20]. <https://www.bis.org/publ/othp67.pdf>.
- [16] Bank for International Settlements. Project Leap phase 2: Quantum-proofing payment systems[EB/OL]. (2025-12-11) [2026-08-20]. <https://www.bis.org/publ/othp107.htm>.
- [17] Banca d'Italia. Project Leap Phase 2: Results of testing quantum-resistant cryptography in real-world payment systems[EB/OL]. (2025-12-11) [2026-08-20]. <https://www.bancaditalia.it/media/notizia/project-leap-phase-2-results-of-testing-quantum-resistant-cryptography-in-real-world-payment-systems>.
- [18] Bank for International Settlements. Project Leap: Quantum-proofing the financial system[EB/OL]. [2026-08-20]. https://www.bis.org/about/bisih/topics/cyber_security/leap.htm.
- [19] Bank for International Settlements. Project Leap: Quantum-proofing payment systems[R/OL]. (2025-12-11) [2026-08-20]. <https://www.bis.org/publ/othp107.pdf>.
- [20] PYMNTS. BIS-Led collaboration completes successful tests of post-quantum cryptography in payment system[EB/OL]. (2025-12-11) [2026-08-20]. <https://www.pymnts.com/digital-payments/2025/bis-led-collaboration-completes-successful-tests-of-post-quantum-cryptography-in-payment-system/>.
- [21] Banca d'Italia. Banca d'Italia joins Phase 2 of BIS Project Leap to test quantum-safe cryptography in payment systems[EB/OL]. (2025-07-09) [2026-08-20]. <https://www.bancaditalia.it/media/notizia/banca-d-italia-joins-phase-2-of-bis-project-leap-to-test-quantum-safe-cryptography-in-payment-systems>.
- [22] Ivezić M. Payments and the race to quantum safety/post-quantum cryptography (PQC)[EB/OL]. (2026-02-23) [2026-08-20]. <https://postquantum.com/post-quantum/payments-quantum-pqc/>.
- [23] Mastercard. Migration to post-quantum cryptography[R/OL]. [2026-08-20]. https://www.mastercard.com/content/dam/mccom/shared/news-and-trends/stories/2025/quantum-explainer-and-white-paper/Migration-to-post-quantum-cryptography-WhitePaper_2025.pdf.
- [24] Amazon Science. Latency from post-quantum cryptography shrinks as data increases[EB/OL]. (2024-03-05) [2026-08-20]. <https://www.amazon.science/blog/delays-from-post-quantum-cryptography-may-not-be-so-bad>.
- [25] NXP Semiconductors. Post-quantum cryptography: Migration challenges for embedded devices[R/OL]. [2026-08-20]. <https://www.nxp.com/docs/en/white-paper/POSTQUANCOMPWPA4.pdf>.
- [26] International Organization for Standardization. ISO 20022-1: 2013 Financial services—Universal financial industry message scheme—Part 1: Metamodel[S]. Geneva: ISO, 2013.
- [27] Enterprise migration to post-quantum cryptography: Timeline analysis and strategic frameworks[J]. Computers, 2026, 15(1): 9.
- [28] Applied Quantum. Post-quantum financial infrastructure framework (PQFIF): A roadmap for the quantum-safe transition of global financial infrastructure[R/OL]. (2025-09-04) [2026-08-20]. https://business.cch.com/srd/20250904-Post-QuantumFinancialInfrastructure_ARoadmapforthe-Quantum-SafeTransitionofGlobalFinancial.pdf.
- [29] PQC Framework. The applied quantum PQC migration framework: Financial services extension v1.1[R/OL]. (2026-03-01) [2026-08-20]. <https://pqcframework.com/wp-content/uploads/2026/03/The-Applied-Quantum-PQC-Migration-Framework-Financial-Services-Extension-v.1.1-Mar2026.pdf>.
- [30] JPMorgan Chase. JPMorgan chase establishes quantum-secured crypto-agile network[EB/OL]. (2024-05-08) [2026-08-20]. <https://www.jpmorgan.com/technology/news/firm-establishes-quantum-secured-crypto-agile-network>.
- [31] HSBC. HSBC pilots quantum-safe technology for tokenised gold[EB/OL]. (2024-09-19) [2026-08-20]. <https://www.hsbc.com/news-and-views/news/media-releases/2024/hsbc>

- pilots-quantum-safe-technology-for-tokenised-gold.
- [32] Monetary Authority of Singapore. MAS and industry partners publish technical report on proof-of-concept sandbox for quantum-safe communications within the financial sector[EB/OL]. (2025-09-01) [2026-08-20]. <https://www.mas.gov.sg/news/media-releases/2025/mas-and-industry-partners-publish-technical-report-on-proof-of-concept-sandbox>.
- [33] McKinsey & Company. Quantum communication and computing: Elevating the banking sector[EB/OL]. [2026-08-20]. <https://www.mckinsey.com/industries/financial-services/our-insights/quantum-communication-and-computing-elevating-the-banking-sector>.
- [34] McKinsey & Company. The quantum leap in banking: Redefining financial performance[EB/OL]. (2025-11-21) [2026-08-20]. <https://www.chattanoogaquantum.com/resources/mckinsey-the-quantum-leap-in-banking-redefining-financial-performance>.
- [35] Abidin A. Post-quantum cryptography: Migration timelines & strategies[EB/OL]. Cybersecurity Industry Day. (2025-11-01) [2026-08-20]. https://cybersecurity-industry-day.be/wp-content/uploads/sites/13/2025/11/Abidin_pqc.pdf.
- [36] Lohrmann D. Post-quantum cryptography: Moving from awareness to execution[EB/OL]. GovTech. (2026-04-05) [2026-08-20]. <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/post-quantum-cryptography-moving-from-awareness-to-execution>.
- [37] Joseph D, Misoczki R, Manzano M, et al. Transitioning organizations to post-quantum cryptography[J]. Nature, 2022, 605(7909): 237-243.

Global financial infrastructure and the SWIFT network: Strategy and technological evolution for post-quantum cryptography (PQC) migration

LIANG Bei¹, MENG Shengzhe², CHANG Da¹, QIN Yue¹, ZHOU Xu¹, LI Rui³

1. Beijing Institute of Mathematical Sciences and Applications, Beijing 101408, China

2. Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China

3. Research Institute of the People's Bank of China, Beijing 100800, China

Abstract Post-quantum cryptography (PQC) is emerging as a critical technology for protecting financial systems against the threats posed by quantum computing and is expected to gradually replace conventional public-key cryptography. This paper systematically examines the systemic quantum threats facing the financial sector, the evolution of global PQC regulatory frameworks and standardization efforts, and the critical role of crypto-agility in facilitating a secure and timely transition. With major economies targeting the 2030–2035 period for phasing out vulnerable public-key cryptographic schemes, crypto-agility is becoming essential for financial institutions to meet emerging regulatory and compliance requirements. We further examine PQC migration across critical financial infrastructures, including central-bank payment systems, the SWIFT network, and major commercial banks, with particular attention to key technical challenges such as message-size expansion, computational overhead under hybrid cryptographic schemes, and out-of-band certificate distribution. The BIS Project Leap experiments demonstrate the functional feasibility of integrating PQC into central-bank payment infrastructures. However, the substantial message expansion caused by post-quantum signatures such as ML-DSA, along with the additional verification overhead of hybrid schemes, poses significant constraints for high-throughput clearing and settlement systems. SWIFT, meanwhile, has laid out a migration plan with SwiftNet 8.0 as its key transition node. Finally, we analyze enterprise-level migration strategies, timelines, and broader implications, showing that a comprehensive PQC transition may require 5–15 years. The analysis highlights crypto-agility and effective cross-institutional and cross-jurisdictional coordination as key factors for successful migration, providing insights into the evolution of financial infrastructures and digital trust systems in the post-quantum era.

Keywords post-quantum cryptography; financial infrastructure; SWIFT network; crypto-agility; digital signature ●



(责任编辑 王志敏)