

特色专题

金融银行业抗量子计算密码迁移路径

向宏^{1,2}, 丁津泰^{3,4}, 梁蓓⁵, 张琼露⁶

摘要 对当前国内外金融银行业抗量子计算密码(post-quantum cryptography, PQC)迁移工作进行了研究,概述了美国 PQC 算法征集与制标活动,介绍了美国 PQC 迁移的相关指南、PQC 迁移的框架设计,重点介绍了一个适用于中国银行业的 PQC 迁移框架。在此基础上,梳理了抗量子计算密码概念的产生与算法标准化进程,以及以美国国家网络安全卓越中心(National Cybersecurity Center of Excellence, NCCoE)为代表的国际 PQC 迁移工作现状;分析了 NCCoE 基于网络安全框架(CSF2.0)的 PQC 迁移框架,包括量子安全治理、数据资产梳理、管理工具、风险管理和密码敏捷迁移 5 个关键板块;基于国家重点研发计划“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”(055 项目),提出了“数据驱动的银行业抗量子敏捷迁移框架”(DEPATURE,“启航”)。该框架由密码模块识别、密码资产清单汇编、量子安全风险评估、PQC 敏捷迁移和安全效果检验 5 个环环相扣的环节构成逻辑闭环,并最终输出量子安全治理状态。最后对国际金融银行业 PQC 迁移工作的发展趋势进行了展望。

关键词 抗量子计算密码;抗量子迁移框架;金融银行业关键基础设施

1 抗量子计算密码迁移概述

1.1 抗量子计算密码概念的产生与标准化工作

1994 年, Peter W. Shor^[1]采用量子傅里叶变换证明了一旦拥有“大规模量子比特”的量子计算机研发成功,以离散对数和大数分解困难问题为根基的现代公钥密码 DH(Diffie-Hellman)、RSA(Rivest-Shamir-

Adleman)、ECC(elliptic curve cryptography)等^[2-4]将被破解。中国商用密码算法标准 SM2 采用了与 ECC 相同的设计原理,因此也面临同样的威胁。Shor 算法是目前人们所知极少数公开的量子算法之一。另一个公开且常用的量子算法是 Grover 算法,主要用于穷举搜索,对现代对称加密算法(例如中国的 SM4 或其他密钥长度小于 128 比特(bit)的对称加密算法)具有较大威胁。

2001 年, Vandersypen 等^[5-6]搭建了一个拥有 7 个物理量子比特的量子设备,实现了 Shor 算法的简要演示: $15=3\times 5$, 且该系统由室温液态可控核磁共振技术实现,可进一步扩展至其他量子系统。此举意味着作为全球计算机网络信任锚的第一代公钥密码算法所面临的量子计算威胁从理论走向了现实,引起了学术界、工业界和各国政府的高度重视。需要指出的是,当前无论是美欧等国政府,还是标准界、产业界、

1. 重庆大学信息物理社会可信服务计算教育部重点实验室(CPS-DSC), 重庆 400044
2. 江苏金融量子安全先进技术实验室(FAST-Q), 南京 210031
3. 西交利物浦大学后量子迁移交叉实验室(PQC-X), 苏州 215123
4. 江苏省金融学会抗量子计算迁移专业委员会, 苏州 215123
5. 北京雁栖湖应用数学研究院, 北京 101408
6. 中国科学院信息工程研究所, 北京 100093

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: 向宏, 教授, 研究方向为网络空间安全与抗量子计算密码迁移, 电子信箱: xianghong@cqu.edu.cn

引用格式: 向宏, 丁津泰, 梁蓓, 等. 金融银行业抗量子计算密码迁移路径[J]. 科技导报, 2026, 44(16): 64-72; doi:10.3981/j.issn.1000-7857.2026.05.00052

学术界,当谈论量子计算机带来的威胁时,人们更为关注的是“密码分析相关量子计算机”(cryptographically-relevant quantum computer, CRQC)。CRQC 与目前国际上竞争激烈的“量子优越性”(quantum supremacy)不同:后者是使用量子设备来模拟基本粒子的规律(例如玻色采样这一物理计算难题),这也是费曼(Richard Feynman)在 20 世纪 80 年代提出通用量子计算机的初衷。CRQC 是目前唯一已知的能够采用计算机程序运行的特定算法,例如 Shor 算法的量子计算机。它类似于第二次世界大战期间图灵等研发的破译德军 Enigma 密码的人类历史上第一台专用电子计算机 Bombe。CRQC 不仅需要进行物理实现,即制备大量的高保真物理量子比特的同时,还需要执行破解 DH/RSA/ECC/SM2 的 Shor 算法。换言之,CRQC 是密码破译专用量子计算机。由于 CRQC 具备破坏现代大型计算机网络安全基石的功能,因此就如同图灵发明的密码破译专用电子计算机被英美两国严加保密了近 40 年一样,世界各国政府对 CRQC 的研发进展一直守口如瓶。学术界至今也未看到公开、严谨、权威的已经能够破译 DH/RSA/ECC/SM2 等第一代公钥密码算法的 CRQC 研发成功的报告。

为了应对 CRQC 的潜在威胁,进入 21 世纪后学术界开始研究能够抵御 CRQC 的新一代公钥密码算法。2003 年 Bernstein^[7]引入了后量子密码(post-quantum cryptography, PQC)的概念,随后 Buchmann 等^[8]也使用了类似术语,以此来囊括能够抵御量子计算攻击的新一代公钥密码算法簇,以期在未来替换现有的公钥密码,用 PQC 重新锚定网络安全基石。美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)一直采用 PQC 这一术语。美国其他政府部门,如美国国家安全局(National Security Agency, NSA)则经常混用“抗量子算法”(quantum-resistant algorithm)或 PQC。中国近年来使用“抗量子计算密码”这一更为准确的术语,其内涵与 PQC、抗量子算法相同。为了简洁和统一,本文使用 PQC 这一术语。

2008 年,在美国 Cincinnati 召开了后量子密码国际研讨会(PQCrypto 2008),会议论文由 Springer 正式出版^[9],标志着 PQC 正式纳入了国际密码学界的视野。2019 年, PQCrypto 年会在重庆举办,这也是

这类 PQC 顶级学术会议首次来华举办。

2009 年 NIST 发布了对 PQC 的调研报告^[10]。该报告综述了当时已有的一些 PQC 算法,并简要讨论了 PQC 算法迁移到现有安全通信协议中需要考虑的因素。算法方面,该报告认为没有充分的证据证明 CRQC 对经典对称加密算法和安全哈希算法产生致命威胁。因此,在大规模量子计算机面世前,对于现存密码学的研究都应当集中在公钥密码学上,特别是对于现有公钥密码的抗量子替代方案研究及 PQC 迁移。PQC 迁移在今天已经成为计算机网络抵御量子计算机攻击时非常重要的核心概念。

NIST 从 2017 年开始正式启动 PQC 全球算法征集活动,历经 3 轮筛选,于 2022 年锁定了标准算法的候选者。2024 年正式推出了第一批 PQC 算法标准,即 ML-KEM(module-lattice-based key-encapsulation mechanism)、ML-DSA(module-lattice-based digital signature algorithm)、SLH-DSA(stateless Hash-based digital signature algorithm)、HQC(Hamming quasi-cyclic)等,初步解决了采用 PQC 算法来替换第一代公钥密码,以满足大型计算机网络密钥分发和数字签名这 2 个基本功能。目前 NIST 仍在继续组织新的 PQC 签名算法征集工作。

1.2 国际 PQC 迁移现状

几乎与 NIST 组织的 PQC 算法征集活动同步,从 2018 年开始 NIST 下属的国家网络安全卓越中心(National Cybersecurity Center of Excellence, NCCoE)启动了 PQC 迁移的准备工作。随着 NIST 的标准算法逐步成型,NCCoE 加大了对 PQC 迁移的相关指南标准的制定。目前,NCCoE 在 PQC 迁移的指南标准制定方面走在全球前列,并对其他国家的迁移工作产生了很大影响。欧盟和日本等地区或国家也纷纷启动了 PQC 迁移的研究工作。总体而言,欧盟 PQC 迁移工作与美国基本保持一致。受篇幅所限,本文重点介绍美国 NCCoE 在 PQC 迁移方面的主要进展。

1.2.1 NCCoE 关于 PQC 迁移的相关工作概述

2021 年 8 月,NCCoE 发布了《向 PQC 迁移》(Migration to post-quantum cryptography)的指导性文件^[11]。在该份 16 页的文件当中,NCCoE 指出它正在推动一系列工作,以简化从当前的公钥密码算法向 PQC 算法的迁移。该文件给出了 5 大类演示场景,以

便让各界认识到 PQC 迁移的各个关键环节。场景 1: 根据 NIST 特别出版物 (special publication, SP) 140 (NIST 发布的涉及密码模块的计算机安全标准) 对面临量子威胁的公钥密码模块的软硬件模块进行检验 (validate)。场景 2: 识别具有量子脆弱性的密码库。场景 3: 具有量子脆弱性的密码应用领域。场景 4: 在计算平台当中识别那些具有量子脆弱性的代码。场景 5: 广泛应用于各个工业领域但具有量子脆弱性的通信协议。该指导性文件的核心思想是引起社会各界对现有信息系统“量子脆弱性”的意识。

1.2.2 后量子密码迁移中应考虑的因素

2023 年 4 月, NCCoE 出版了《PQC 迁移中应考虑的因素》(Migration to post-quantum cryptography quantum readiness: preparation for considering the implementation and adoption of quantum safe cryptography)(SP 1800-38A)^[12]。这是 NCCoE 3 份系列文件的第 1 份。这份 5 页的指南首先指出, 由于 NIST 的首批 PQC 标准化工作正在向前推进, 为了配合这一工作, NCCoE 推出了该份指南, 用于指导各机构开始启动 PQC 迁移工作。指南的主要内容如下。

1) 面临的主要挑战。当前使用的许多加密产品、协议和服务, 特别是那些使用公共加密算法的产品、协议或服务, 如 RSA、ECDH(elliptic curve Diffie-Hellman)和 ECDSA(elliptic curve digital signature algorithm), 均需要更新、替换或更改以使用 PQC 算法, 否则许多公钥算法和使用它们的协议将容易受到 CRQC 的攻击。现今大多数 IT(information technology)系统都不是为了在不对系统组件进行重大更改的情况下支持新密码算法的快速自适应而设计的。换言之, 是对“密码敏捷性”(crypto-agility)极不友好的静态系统。

2) NCCoE 的 PQC 迁移计划目标。针对上述挑战, NCCoE 的 PQC 迁移项目将首先开发典型示例、指导和推荐实践。接下来, 该项目将展示这些支持各种用例场景的示例。演示结果将发表在该实践指南中, 该指南是 NIST 1800 系列 SP, 由多卷组成。

3) NCCoE 将提供解决方案。这份 PQC 迁移项目的相关指南, 将展示在以下用例场景中发现量子脆弱算法的工具: 在连续集成/连续交付开发渠道过程中, 密码或依赖关系中使用的易受 CRQC 攻击的算

法; 网络协议中使用的易受 CRQC 攻击的算法, 使用主动扫描和历史流量捕获实现对特定系统的可追溯性; 最终用户系统和服务器上的加密资产中使用的易受 CRQC 攻击的算法, 包括应用程序和相关工具库。

上述解决方案的结果将是一系列技术和工具的实际演示, 这些技术和工具可以支持各组织机构在使用基于风险的方法规划迁移路线图时明确易受攻击的公钥密码。同时, 行业合作者将以额外的实践指南、白皮书或 NIST 内部报告(internal reports, IRs)的形式发布互操作性和性能工作流的结果/观察结果/发现, 以缩小差距, 并加快 PQC 在产品、协议和服务中的采用。

该份指南明确了 PQC 迁移工作中密码模块自动化识别工具扮演的重要角色, 并计划在接下来的试验验证环境中对不同的典型场景进行检验。密码模块自动化识别工具是任何组织机构成功启动 PQC 迁移第一步要考虑的, 它直接牵涉组织机构现有加密资产清单汇编科学、准确的梳理, 为组织机构信息系统中进行 PQC 密码模块精确定位替换、绘制量子脆弱性攻击面提供实证依据。

1.2.3 后量子密码迁移中的密码模块发现

2023 年 12 月, NCCoE 出版了《PQC 迁移中的密码模块发现》(Migration to post-quantum cryptography quantum readiness: cryptographic discovery)(SP 1800-38B)^[13]。该指南共 68 页, 文件强调“公钥密码应用发现工具的方法、体系结构和安全特性”。

该指南分享了关于使用密码模块发现工具创建加密清单的经验。它是 NIST 首批关注创建、扩展或使用密码资产清单以支持向 PQC 迁移的实践之一。它提供了: (1) 1 个功能测试计划, 该计划使用密码模块发现工具来确定基线的能力; (2) 1 个用例场景, 为 NCCoE 组织的演示提供背景和范围; (3) 应对这些量子脆弱性密码威胁的思路; (4) 大多数组织机构马上可以开始的密码模块发现过程的多种方法; (5) 基于 NCCoE 给出的用例的抽象架构, 在 NCCoE 组织的实验室中集成了多个参与单位(包括 IBM、Microsoft、Amazon 等大企业, 以及众多中小企业)研发的密码模块发现工具。

该指南首先阐述了密码模块自动化工具识别开发的方法论, 明确指出要遵循统一的软件开发过程来

进行统一规划和设计。同时明确了 S/BOMS(软件数据清单, software bill of materials)和 C/BOMS(密码数据清单, cryptography bill of materials)之间的相关关系。需要指出的是,针对 PQC 迁移的 C/BOMS 目前仍在不断探索之中,但它的规范性又决定了现有密码模块识别与后续 PQC 迁移的质量。此外,密码模块自动化识别与整个系统环境密切相关,因此需要开发一整套测试基准/基线来验证自动化识别工具的准确性和全面覆盖性。

1.2.4 后量子密码迁移的测试标准

2023 年 12 月, NCCoE 出版了《PQC 迁移的测试标准(草案)》(Migration to post-quantum cryptography quantum readiness: testing draft standards)(SP 1800-38C)^[14]。这份 87 页的指南草案给出了迁移的测试方法和指标,是对信息系统进行 PQC 迁移的前提。

NIST 正在进行的 PQC 算法标准化的互操作性测试被确定为一个核心重点领域,以支持技术供应商和标准机构的迁移,开发利用 PQC 的新产品。采购实施 PQC 的系统和软件的组织将能够了解他们已经使用的技术并做好抗量子的准备工作。

从 NCCoE 实验室的测试中对性能指标进行基准测试,将帮助 NCCoE 的联盟成员和任何技术供应商优化其系统,帮助它们走向企业级 PQC 迁移的实现。了解 PQC 算法的性能指标将在激励 PQC 产品和服务提供商方面发挥至关重要的作用。这些技术链、产品链将促使各行业开始启动 PQC 迁移,并将提供 PQC 算法最适合特定用例的初始数据。

从上述 3 份系列文件可以看出美国 NCCoE 组织实施的 PQC 迁移的工作流程。SP 1800-38A 首先给出迁移的挑战、迁移准备工作所需要的框架性设计、主要的迁移功能点,以及预期的成果。SP 1800-38B 重点考虑迁移工作的第一步:密码模块自动化识别,包括工具的种类、预期的输出成果等,从开发识别工具的方法论(如风险评估)、现有软件开发标准的遵从、代码规范(SBOM/CBOM)、密码模块二进制编码的识别,到协议层的密码模块识别和最终预期成果输出与衔接——自动化识别的结果将直接决定系统资产清单汇编的完整性。这对于中国开展相应的 PQC 迁移工具研发具有重要参考价值。最后是 SP 1800-38C,重点关注迁移工程的科学评估——测试基准/基

线的研发。这也是该系列指南草案篇幅最大的部分。该文档中的各种列表展示了 NCCoE 组织在测试验证环境所获得的测试结果,具有很好的参考价值。

在上述基础上,目前 NCCoE 正在凝练总结 PQC 的迁移框架,其核心要素是在 NIST 的网络安全框架的基础上,融入 PQC 迁移的要素。下面对此进行简介。

2 NCCoE 的 PQC 迁移框架

2.1 NIST 的网络安全框架概述

2024 年 5 月,在欧洲电信标准化协会量子安全密码年会上(European Telecommunications Standards Institute/Quantum-Safe Cryptography, ETSI/QSC; 新加坡),来自 NCCoE 的代表做了题为“NCCoE 后量子密码迁移”进展的报告,给出了关于美方整体 PQC 迁移框架的技术路线,即采用 NIST 最新制定的“网络安全框架”(Cybersecurity Framework 2.0, CSF2.0)^[15]。

2025 年 2 月,在国际清算银行(Bank for International Settlements, BIS)巴塞尔(Basel)总部召开的全球央行“量子安全准备”(quantum readiness)会议上, NCCoE 的代表再次重申了该迁移框架。由此看出美国 PQC 迁移的基本框架已经比较成熟。而整个迁移框架的底层逻辑是依据 NIST 的网络安全框架 CSF2.0 细化的。

NCCoE 采用 CSF2.0 的主要原因是 PQC 迁移需要与美国整体网络安全框架相适配,以便于从整体网络安全的角度评估 PQC 子系统所发挥的作用。这一思路值得借鉴。

CSF2.0 沿袭了 NIST 对信息系统实施安全风险的一贯思路,并与之前发布的系列网络安全风险管理标准保持一致。

NIST 网络安全框架(CSF2.0)为行业、政府机构和其他组织机构管理自身的网络安全风险提供了指导。它提供了一个网络安全建设成果的分类,任何组织机构无论其规模、行业领域或成熟度如何都可以使用它,以更好地理解、评估、考虑优先事项和与各方沟通其网络安全工作。该文档介绍了 CSF 2.0、其组件以及如何使用它的方法。

该框架以 NIST 网络安全风险管理为基础,以网

络安全治理为宗旨,对信息系统的安全风险进行“识别”“防护”“检验”“响应”,直到“恢复”形成闭环。

与以往 NIST 的类似标准相比,CSF2.0 的创新性在于为信息系统建设过程中所面临的各阶段网络安全风险的科学评估提供了更为详细且可操作的工具箱。

CSF2.0 包括以下组成部分:(1) CSF 核心组件(CSF Core)。该组件是 CSF 的核心,可以帮助任何组织机构管理其网络安全风险。CSF 核心组件是功能、类别和子类别的层次结构,详细说明了每个分类结果。(2) CSF Core 是一组网络安全判定结果,按功能、类别和子类别排列。为实现结果而采取的具体行动将因组织机构和网络安全用例而异,负责这些行动的个人也会有所不同。此外,功能、类别和子类别的顺序和大小并不意味着实现它们的顺序或重要性。CSF Core 的结构旨在与组织机构内实施风险管理的人产生共识。

CSF2.0 除了上述 CSF Core 之外,还包括以下 2 个组件:(1) CSF 组织机构概况,这是一种根据 CSF 核心的结果描述组织机构当前和/或目标网络安全状况的机制;(2) CSF 级别,可应用于 CSF 组织机构的概况,以描述组织机构网络安全风险治理和管理实践活动。

2.2 NCCoE 的 PQC 迁移框架概述

基于 CSF2.0,NCCoE 开发了一个冗长的名为“以数据为中心的聚焦密码敏捷性优先的迁移风险管理”(data centric risk management to prioritize mitigation and migration with crypto agility)的框架。该框架的特点如下。

1) PQC 迁移框架与 CSF2.0 相融合。NCCoE 的 PQC 迁移框架整体嵌入到 CSF2.0 框架当中,即上述 CSF2.0 的各个环节均与 PQC 迁移框架相结合。可以简单地理解为 CSF2.0+PQC。首先,NCCoE 的 PQC 迁移框架分为 5 个关键板块:第 1 个板块是达到 PQC 迁移的终极目标——量子安全治理,与 CSF2.0 的核心目标——网络空间安全治理目标一致。为此,NCCoE 的 PQC 迁移的第 2 个板块是数据资产梳理,包括代码、各类函数库(例如密码库)、应用程序、各类与之相关的文档、协议和信息系统等。这个环节既指向 CSF2.0 的“识别”环节,也包括 PQC 迁移过程中最重要的现有密码模块识别,以及在此基础上形成的

数据资产清单。第 3 个板块是管理工具,针对数据、密码、脆弱性、资产、日志、零信任等进行的有效管理。第 4 个板块是风险管理,包括数据清单、风险管理引擎(风险监控、对应的可视化仪表盘、风险评估报告、基于量子安全风险评估的基准/基线等)。第 5 个板块是最具挑战性的密码敏捷迁移。需要指出的是,这 5 大板块是否能够与 CSF2.0 的 5 个环节一一对应,在目前 NCCoE 的 PQC 迁移框架当中尚未做到严丝合缝的衔接。但鉴于 NIST 基于风险管理的标准、指南、工具等已经非常丰富和成熟,所以在 NCCoE 的 PQC 迁移框架中将关注的焦点放在了密码敏捷性迁移当中。

2) NCCoE 关注的密码敏捷性迁移要素。按照 NCCoE 的观点,密码敏捷性分为多个维度:敏捷迁移的指导原则包括独立于应用(场景)、简单易懂、足够抽象(以便可扩展)、可交换性、可管理性和便于执行。具体环节包括:(1) 安全性。包括攻击面、降级攻击等。(2) 成熟度模型。包括测评与验证。(3) 合规性。与美国现有法律法规等的一致性。(4) 敏捷迁移框架。包括模块化和抽象性、动态配置管理、算法适配性和相关标准。(5) 敏捷迁移技术机制。包括协议层的协商机制、应用层的 API(application programming interface)抽象、算法库、硬件加速机制等。(6) 资源需求与性能。包括硬件、固件、软件,通信协议,以及对云服务的微控制器等。(7) 用例。场景驱动的 PQC 迁移演示以及对实用指南开发的反馈等。

截至目前,NCCoE 仍在对上述 PQC 迁移框架不断进行细化完善。需要指出的是,NCCoE 这个 PQC 迁移框架是针对一般信息系统 PQC 迁移的,并非针对特定应用场景。与此同时,中国科技工作者也针对金融银行业 PQC 迁移框架提出了自己的见解,并在 2024 年 ETSI/QSC 新加坡年会、2025 年 BIS 组织的各国央行“量子安全准备”闭门会议和 2025 年 ETSI/QSC 西班牙年会上与包括 NCCoE 在内的各国代表进行了交流。

3 中国银行业 PQC 迁移框架研究

中国在 2023 年 11 月启动了科技部“平安中国”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”(简称 055 项目)。055 项目属于在全球范围内最早启动的金融银行业 PQC 迁移项目之一。另外一个涉及金融银行业 PQC 迁移的项目,是由国际清算银行(Bank for International Settlements, BIS)、德意志联邦银行(Deutsche Bundesbank, 德国央行)和法兰西银行(Banque de France, 法国央行)联合组织实施的“跃迁计划”(Project Leap)。该计划与 055 项目同期启动,主要是在德国央行、法国央行之间通过 VPN(virtual private network)/IPSec(internet protocol security)专网进行 PQC 迁移试验;055 项目则注重商业银行典型应用场景,如手机银行、网上银行和跨行交易的 PQC 迁移技术验证。因此,从场景的丰富程度和潜在用户数等指标而言,055 项目领先于“跃迁计划”。

055 项目的成果之一是提出了“数据驱动的银行业抗量子敏捷迁移框架”(a Data-driven Pqc-Agility migration framework in bank industries, DEPARTURE),即“启航”。该迁移框架包括了密码模块识别、密码资产清单汇编、量子安全风险评估、PQC 敏捷迁移,以及安全效果检验这 5 个环环相扣的环节,并形成不断循环迭代的逻辑闭环。最后输出量子安全治理状态结果。以下对“启航”框架的各个环节进行简要介绍(图 1)。



图 1 “启航”——数据驱动的银行业抗量子敏捷迁移框架概念

3.1 密码模块识别

密码模块识别环节的主要任务是辨识组织机构当前信息系统中所采用的密码模块及其相关业务关联(如加密模块支持的数据等)。了解组织机构信息

系统当中的密码模块部署情况、开发商信息与供应链,为组织机构下一步制定重要信息资产清单提供支撑。这一状态是目前国际上 PQC 迁移工作的第一个环节,也是一大难点,其中既涉及各类操作系统、数据库、中间件和应用软件,也涉及硬件设备所使用的密码库。其难点在于对使用的第一代公钥密码模块(RSA/ECC/SM2 等)进行代码级的精确定位。这些密码模块均无法抵御 CRQC 的攻击。因此从网络安全漏洞检测的角度,这些密码模块都极大地扩展了对手的攻击面。055 项目针对国际上开源代码库,如 GitHub 等平台,以及鸿蒙、红旗 Linux、龙蜥等操作系统进行基于大模型的密码模块代码级识别,取得较好效果。

3.2 密码资产清单汇编

在密码模块识别的基础上,需要对组织机构下一步准备开展 PQC 迁移的重要信息资产(数据、信息系统与公钥密码模块相关的软硬件资产、通信协议、业务数据、业务流程甚至组织架构)进行梳理并形成清单,并在组织机构企业风险管理(enterprise risk management, ERM)战略的指导下,制定需要进行迁移的清单优先顺序。

以银行业为例,核心信息系统,如客户账户管理、存款计息、贷款台账与还款核算、总账记账、资金清算、汇率利率管理、账务统一核算均为支撑所有前台业务的数据与账务底层。支撑这些核心业务的信息系统中采用了哪些与密码模块相关的软硬件系统,均需要进行梳理并形成清单。在 055 项目选择的 3 大典型应用场景,即手机银行、网上银行和跨行交易等均涉及上述核心业务。

3.3 量子安全风险评估

该状态对“密码资产清单汇编”的输出结果进行 PQC 迁移的风险评估。该环节的主要目的是在进行迁移之前,结合拟采用的 PQC 密码模块(安全参数、性能)是否能够顺利替换原有的密码模块,并能支撑组织机构原有的业务重要性、连续性进行量子安全风险评估。评估结果还将包括迁移的风险排序,并与密码资产清单相结合形成迁移的优先顺序。该状态的输出结果将直接决定是否采用、采用什么以及何时采用 PQC 密码模块。

特别需要指出的是,在这个环节当中,“启航”迁

移框架与美国的 PQC 迁移框架有本质区别。中国银行业 PQC 迁移的风险评估需要遵循中国的相关法律法规(如《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等)、国家标准和行业标准,遵从中国网络信息安全管理的基本制度,例如等级保护、风险评估相关标准。另一方面,量子安全风险评估极大地依赖对目前国际上量子计算研发进展的风险预警。055 项目的成果之一是对国际量子计算安全风险进行了系统性研究,包括预警模型等^[16]。

3.4 PQC 敏捷迁移

该环节将现有密码模块更换为 PQC,从而提升组织机构的量子安全能力。该环节将在风险评估的基础上,根据密码资产清单,针对已经识别出来的无法抵御 CRQC 攻击的密码模块,采用敏捷迁移/混合模式进行抗量子密码的迁移实现。该环节需要根据信息系统现有的密码模块、通信协议等进行算法适配性迁移,包括考虑对原有公钥算法模块的筛选(国际商用密码标准或中国商用密码标准)与 PQC 算法的适配(密钥交换或数字签名)等要素。

敏捷迁移是目前国际上 PQC 迁移工作的重中之重。它不仅是将具有“量子安全漏洞”的密码模块更换为现有的 PQC 算法模块,还需要考虑未来 PQC 算法的不断更新、迭代。即使是当前主流的 PQC 算法,各界仍在对其安全性进行不断地探索。因此要从系统工程的角度对敏捷迁移进行统筹规划。

在 PQC 算法研究方面,055 项目取得了突破性成果,首次刻画了国际主流的格密码安全分析边界^[17],引起了国际 PQC 各界的高度重视。该成果对 055 项目的目标之一“与银行信息系统相适配的 PQC 算法研究”起到了关键作用。同时,055 项目在抗量子密码安全通信协议方面的研究也取得了一系列成果^[18-19],对抗量子安全协议的敏捷性迁移极为重要。这些研究成果均对今后中国银行业 PQC 迁移具有重要的借鉴作用。

3.5 安全效果检验

安全效果检验包括如下 2 个层面。

1) 技术层面的效果检验。它能够及时发现和分析 PQC 迁移后的异常情况(例如 PQC 模块在实现过程中的漏洞、部署错误等),以及可能带来整体信息系

统网络安全攻击和事件的潜在不利事件。需要着重指出的是,安全效果检验需要新的检测工具与原有的网络安全检测工具相结合,但该环节不要求使用量子计算机进行攻击检测。一方面是因为现有的量子计算机尚不具备对第一代公钥密码的破解能力,另一方面任何组织机构(国家)现阶段如果已经拥有了 CRQC,均不会公开。还需强调的是,对于重要基础设施信息系统的量子安全状态的检验,国际上的惯例是搭建高仿真环境进行离线(off-line)验证。在安全性和性能均达到要求后,再分阶段、分规模、分业务进行迁移切换。这一点对于银行业及其重要基础设施信息系统尤为重要。

2) 政策层面的效果检验。在技术层面效果检验的基础上,检验银行信息系统量子安全敏捷迁移对现有的银行监管政策是否存在冲突或需要补充完善等。

055 项目在实施过程中,一方面针对手机银行、网上银行和跨行交易搭建了高仿真的试验平台,对迁移效果进行检验。与此同时,江苏银行还专门针对网上银行进行了 B 产线(即全银行业务生态环境,但使用白名单机制进行风险控制)环境下的测试工作,这一测试具有国际先进水平。该技术验证无论是场景丰富性、全栈技术链验证、国密算法+PQC 算法混合模式,还是即插即用的抗量子 UKey 等方面,均领先于 BIS 的“跃迁计划”。值得指出的是,055 项目还率先在政策合规性方面迈出了全球第一步。

3.6 量子安全治理状态

这是“启航”框架的最终目标。该状态代表一个组织机构的量子安全风险战略,期望和政策得以建立、沟通和监控。第三方权威机构提供评估结果,以告知组织机构可以做些什么来实现 PQC 迁移的目标,并确定迁移优先顺序。量子安全治理状态对于将量子安全纳入组织机构更广泛的 ERM 战略至关重要。它阐述了对组织机构背景的理解;制定量子安全战略和量子安全供应链风险管理;角色、职责、权限、政策,以及量子安全战略的监督。其治理效果由以上 5 个环节汇聚而成,并对每个环节进行定性/定量刻画,使得重要网络和信息系统的管理人员、工程技术人员、服务提供商,以及用户对系统的量子安全状态有一个总体认识。量子安全治理的能力/水平类似于信息系统安全能力成熟度。

4 结论

国际 PQC 迁移工作已经从标准成熟、技术成熟走向面向应用领域的工程化迁移阶段,急需合规性指导,例如七国集团(Group of Seven, G7)2026 年 1 月发布公告^[20],要求在 2035 年之前完成成员国之间金融系统的抗量子计算密码迁移工程,但目前仍未出台相关的合规性指南。而 055 项目发布的《银行业抗量子计算密码迁移管理指南》团体标准^[21],不仅是国内首创,也是国际率先示范,为国际金融行业抗量子计算密码迁移提供了中国合规方案。

当前,国内外 PQC 迁移工作聚焦 2 个方向。一个是迁移路径与框架。它决定了一个国家 PQC 迁移的整体一致性和迁移质量的保障。另一个是 PQC 敏捷性迁移。这是一个不断演变的动态过程,不仅涉及算法敏捷性、协议敏捷性,还涉及整个信息系统安全敏捷性的设计与实现。对于中国而言,既是挑战,更是机遇。通过 PQC 迁移这个网络空间的大迁徙,有可能从标准链、技术链、产品链和生态圈等方面在新的安全赛道上闯出一条中国道路。

参考文献(References)

- [1] Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring[C]//Proceedings of 35th Annual Symposium on the Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society Press, 1994: 124–134.
- [2] Diffie W, Hellman M. New directions in cryptography[J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644–654.
- [3] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. *Communications of the ACM*, 1978, 21(2): 120–126.
- [4] Miller V S. Use of elliptic curves in cryptography[C]//Advances in Cryptology—CRYPTO'85 Proceedings. Berlin, Heidelberg: Springer, 1986: 417–426.
- [5] Vandersypen L M K, Steffen M, Breyta G, et al. Experimental realization of an order-finding algorithm with an NMR quantum computer[J]. *Physical Review Letters*, 2000, 85(25): 5452–5455.
- [6] Vandersypen L M K, Steffen M, Breyta G, et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance[J]. *Nature*, 2001, 414(6866): 883–887.
- [7] Bernstein D J. Has anyone really cracked anything recently [EB/OL]. (2003–09–19) [2026–08–24]. <https://archive.ph/BHGOM>.
- [8] Buchmann J, Coronado García L C, Döring M, et al. Post-quantum signatures[EB/OL]. (2004–11–24) [2026–08–24]. <https://eprint.iacr.org/2004/297>.
- [9] Buchmann J, Ding J. Post-quantum cryptography[C]//Proceedings of the 2nd international workshop on post-quantum cryptography (PQCrypto 2008). Berlin, Heidelberg: Springer, 2008.
- [10] Perlner R A, Cooper D A. Quantum resistant public key cryptography: A survey[C]//Proceedings of the 8th Symposium on Identity and Trust on the Internet. New York: ACM, 2009: 85–93.
- [11] National Cybersecurity Center of Excellence. Migration to post-quantum cryptography: Project description[EB/OL]. (2021–08–01) [2026–08–24]. <https://www.nccoe.nist.gov/sites/default/files/2022-07/pqc-migration-project-description-final.pdf>.
- [12] National Cybersecurity Center of Excellence. Migration to post-quantum cryptography quantum readiness: Preparation for considering the implementation and adoption of quantum safe cryptography: NIST SP 1800–38A (preliminary draft)[EB/OL]. (2023–04–01) [2026–08–24]. <https://www.nccoe.nist.gov/sites/default/files/2023-04/pqc-migration-nist-sp-1800-38a-preliminary-draft.pdf>.
- [13] National Cybersecurity Center of Excellence. Migration to post-quantum cryptography quantum readiness: Cryptographic discovery: NIST SP 1800–38B (preliminary draft) [EB/OL]. (2023–12–01) [2026–08–24]. <https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf>.
- [14] National Cybersecurity Center of Excellence. Migration to post-quantum cryptography quantum readiness: Testing draft standards: NIST SP 1800–38C (preliminary draft) [EB/OL]. (2023–12–01) [2026–08–24]. <https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf>.
- [15] National Institute of Standards and Technology. The NIST cybersecurity framework (CSF) 2.0[EB/OL]. (2024–02–26) [2026–08–24]. <https://www.nist.gov/cyberframework>.
- [16] 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.
- [17] Zhao Z Y, Ding J T. Towards large-scale lattice attack: New lattice records by disk-based sieving[C/OL]//Advances in

- Cryptology—EUROCRYPT 2026. [2026-08-24]. <https://eurocrypt.iacr.org/2026/acceptedpapers.php>.
- [18] Liu K B, Gu X Z, Ren P X, et al. Speedy error reconciliation[C]//Information Security and Cryptology. Singapore: Springer Nature Singapore, 2026: 166-186.
- [19] Liu K, Lu X. Enhancing TLS protocol security: A hybrid cryptographic approach for post-quantum migration[C]//Proceedings of the International Conference on Cryptography, Security and Privacy (CSP 2026). Piscataway, NJ: IEEE, 2026.
- [20] G7 Cyber Expert Group. Planning for the opportunities and risks of quantum computing[EB/OL]. [2026-08-24]. <https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf>.
- [21] 江苏省金融学会. 银行业抗量子计算密码迁移管理指南[S]. 南京: 江苏省金融学会, 2026.

Migration path of post-quantum cryptography for the financial and banking industry

XIANG Hong^{1,2}, DING Jintai^{3,4}, LIANG Bei⁵, ZHANG Qionglu⁶

1. Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University), Ministry of Education, Chongqing 400044, China
2. Jiangsu Financial Advanced Security Technology for Quantum Laboratory (FAST-Q), Nanjing 210031, China
3. Post-Quantum Migration Interdisciplinary Laboratory (PQC-X), Xi'an Jiaotong-Liverpool University, Suzhou 215123, China
4. Special Committee on Post-Quantum Cryptography Migration, Jiangsu Provincial Society for Finance and Banking, Suzhou 215123, China
5. Beijing Institute of Mathematical Sciences and Applications, Beijing 101408, China
6. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract This article studies the current work on post-quantum cryptography (PQC) migration in the financial and banking industry both domestically and internationally. It provides an overview of the PQC algorithm solicitation and standardization activities in the United States, introduces the relevant guidelines for PQC migration in the United States, and presents the framework design for PQC migration. Finally, a PQC migration framework applicable to China's banking industry was highlighted. On this basis, this paper reviews the origin of the PQC concept and the algorithm standardization process, as well as the current status of international PQC migration led by the National Cybersecurity Center of Excellence (NCCoE) of the United States. It then analyzes the NCCoE PQC migration framework built upon the Cybersecurity Framework (CSF) 2.0, which covers five key building blocks: quantum-safe governance, data asset inventory, management tools, risk management, and crypto-agile migration. Based on the National Key R&D Program project "Research on PQC Migration Technology for the Banking Industry and Its Critical Infrastructure Information Systems" (Project 055), a Data-driven Pqc-Agility migration framework in banking indUstRiEs (DEPARTURE) is proposed, which forms a closed loop consisting of five interlocking phases: cryptographic module discovery, cryptographic asset inventory compilation, quantum-safe risk assessment, PQC agile migration, and security effectiveness verification, and finally outputs the quantum-safe governance status. The development trend of PQC migration in the international financial and banking industry is also discussed.

Keywords post-quantum cryptography (PQC); quantum-resistant migration framework; critical infrastructure of the financial and banking industry ●



(责任编辑 王志敏)