后量子密码迁移策略研究

Research on Post-Quantum Cryptography Migration Strategies

韩　浩，鲁华伟，邹艳鹏（联通数字科技有限公司，北京 100037）
Han Hao，Lu Huawei，Zou Yanpeng（China Unicom Digital Technology Co.，Ltd.，Beijing 100037，China）

摘　要：
密码是保障网络与信息安全的核心技术和基础支撑，是数字经济高质量发展的安全基石。然而随着量子计算的发展，传统的密码技术面临严峻挑战。当前各国高度重视量子安全技术的研究，相继发布后量子密码迁移路线图。分析了传统密码技术面临的量子威胁，给出了后量子密码技术路线，最后提出了后量子密码迁移技术发展建议，以期为量子安全技术发展提供参考。

关键词：
密码学；后量子密码；公钥密码；后量子迁移
doi：10.12045/j.issn.1007-3043.2025.10.003
文章编号：1007-3043（2025）10-0013-05
中图分类号：TN914
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Cryptography is the core technology and basic support to ensure network and information security，and is the security cornerstone for the high-quality development of the digital economy. However，with the development of quantum computing，traditional cryptography faces serious challenges. At present，countries attach great importance to the research of quantum security technology and have successively released the roadmap of post-quantum cryptography migration. It analyzes the quantum threats faced by traditional cryptography，give the post-quantum cryptography technology route，and finally puts forward suggestions for the development of post-quantum cryptography migration technology，in order to provide reference for the development of quantum security techniques.

Keywords：
Cryptography；Post-quantum cryptography；Public key cryptography；Post-quantum cryptography migration

引用格式：韩浩，鲁华伟，邹艳鹏. 后量子密码迁移策略研究[J]. 邮电设计技术，2025（10）：13-17.

1 概述

随着量子计算技术的深入发展，传统的密码技术正面临着前所未有的挑战，量子计算带来的安全威胁正在催生着网络安全技术体系新秩序的建立。现代密码学作为网络安全的理论基础，主要分为公钥密码与对称密码两大分支，其中公钥密码因其在密钥协商、数字签名等场景的不可替代性，成为量子计算攻击的主要目标。Peter Shor提出求解整数分解问题的多项式时间量子算法（Shor算法）[1]，首次从理论上证明传统公钥密码的安全基础可被量子计算突破。此后，基于Shor算法框架发展的系列量子算法的飞速发展，使得当前广泛应用的RSA、Diffie-Hellman、Elgamal及SM2等公钥密码算法的安全假设在量子计算模型下失效，此类算法依赖的数学难题均可在量子计算中被多项式时间求解，导致基于此类算法的网络安全协议面临系统性安全风险。受影响的安全协议包括虚拟专用网络的IKEv2协议、传输层安全的SSL/TLS协议、安全邮件的S/MIME协议及远程访问的SSH协议等，直接威胁网络信任体系与身份认证机制的安全性。量子技术攻击对于传统对称密码安全性减半，可

基金项目：国家密码科学基金（2025NCSF01007）
收稿日期：2025-08-28

以通过增加密钥长度来有效抵抗量子计算攻击。

虽然当前量子计算机尚未成熟，但“先存储，后解密（Harvest Now，Decrypt Later）”攻击[2]风险越来越大，攻击者可截获并存储当前加密数据，待量子计算技术成熟后进行解密。2024年，全球风险研究所（Global Risk Institute in Financial Services）发布《量子威胁时间线报告》[3]，报告指出量子计算机的快速发展正在对采用非对称密码算法保护的加密数据造成严重安全威胁。量子计算机正成为全球竞争的焦点，预计未来10年有34%的可能性产生量子计算机，这将会对现有的网络安全体系产生深刻变革。

为应对量子计算攻击带来的威胁，后量子密码（Post-Quantum Cryptography，PQC）正在成为国内外主流的量子安全研究方向。美国国家标准技术局（NIST）相继公布了CRYSTALS-Dilithium、CRYSTALS-Kyber、SPHINCS+、Falcon和HQC等后量子密码标准算法[4-6]。亚马逊、思科、IBM和微软等科技巨头共同发起了开放量子安全（Open Quantum Safe）开源项目，研究基于后量子密码的网络安全协议。2025年2月，国家密码管理局面向全球征集后量子密码算法，用于同时抵抗经典计算攻击和量子计算攻击，标志着我国商用密码算法正式向后量子技术迈进，为我国网络安全新格局提供了量子安全保障。

2 后量子密码技术

如表1所示，当前后量子密码主要包括基于格、基于编码、基于多变量、基于同源映射以及基于哈希的后量子密码方案。

表1　后量子密码算法对比

后量子密码算法		安全可靠性	算法性能
基于格	基于标准格问题	安全性较高	尺寸有待提升 计算效率一般
	基于代数结构格问题	有待研究	尺寸较好 计算效率较好
基于编码	基于标准编码问题	安全性较高	尺寸较差 计算效率一般
	基于代数结构编码问题	有待研究	尺寸一般 计算效率较好
基于多变量		多个代表性算法被攻破	签名尺寸具有优势 整体尺寸大 计算效率一般
基于同源映射		代表性算法被攻破	尺寸好 计算效率很低
基于哈希		高	公钥尺寸具有优势 签名尺寸大 计算效率低

2.1 基于格

格密码是目前研究最成功的一类后量子公钥密码，在美国NIST首批4个后量子密码标准算法中，基于格的后量子密码独占3席。基于格的后量子密码的安全性基于高维格理论数学难题最短向量问题（SVP）和最近向量问题（CVP）的计算复杂性。SVP和CVP已被证明是NP-hard问题，这是基于格的后量子密码被认为能抵抗量子计算机攻击的理论依据[7-8]。在后量子密码的推进过程中，基于格的后量子密码的安全性和实用性得到了验证，在公钥加密、密钥协商和数字签名等方面已经能够支持多数应用场景，谷歌、苹果等IT龙头企业已率先在其产品中部署相关算法。

2.2 基于编码

基于编码的后量子密码是第二大类后量子密码算法，其安全性基于编码数学难题的计算复杂性。McEliece提出了首个基于编码的公钥加密方案[9]，其核心在于将一定数量的错误码引入编码中，纠正错误码或计算校验矩阵的伴随式是困难的。McEliece使用随机二进制的不可约Goppa码作为私钥，公钥是对私钥进行变换后的一般线性码。由于基于编码的后量子密码通常具有公钥大、密钥生成慢的特点，在实用化方面有待提升。

2.3 基于多变量

基于多变量的后量子密码是后量子密码算法最早的类别之一，这类密码算法基于求解高次多变量方程组NP问题。通常基于多变量的后量子密码采用二次多项式，并将有限域上一组二次多项式作为公钥映射。基于多变量的后量子密码与其他后量子密码算法相比，具有签名验签速度快、消耗资源少的优势，其缺点是公钥尺寸大，因此适用于无需频繁进行公钥传输的应用场景，例如计算和存储能力受限的物联网设备等。

2.4 基于同源映射

同源是指2条椭圆曲线之间存在一个映射，这个映射能够保持它们的群结构同态。基于同源的后量子密码是基于椭圆曲线同源问题的后量子密码技术。基于同源的密码继承了椭圆曲线密码的底层运算，公钥和密文尺寸都非常小，可以在通信量受限的环境下运行，但是其运行效率非常低，其密钥生成、加密和解密速度几乎比基于格大2个数量级，这使其不易在一些计算性能不足的设备上实现。

2.5 基于哈希

基于哈希的签名算法安全性仅依赖于哈希函数的安全性，是安全性假设最保守的签名算法，美国NIST首批后量子密码标准中的SPHINCS+属于此类算法。哈希函数的困难性可直接假设等同于理想的通用攻击的复杂度，其安全性并不会随着设计的优化而减弱，在后量子时代，基于哈希函数的签名算法具有巨大的潜力。

3 迁移规划与推进

在全球范围内，多国已积极发布后量子密码迁移相关规划与指南，明确路线图和时间表以推进加密算法的升级换代。

美国NIST发布了《过渡到后量子密码学标准》公开草案，提出逐步淘汰传统加密算法、采用后量子密码算法的路线图和时间表。建议联邦机构识别和评估现有加密资产，分阶段推进迁移，计划到2030年弃用安全强度低的传统算法，在2035年前全面采用后量子密码。

英国国家网络安全中心（NCSC）发布了《迁移到后量子密码学的时间表》，为英国各组织未来数年安全迁移到后量子密码学提供清晰路线图和关键时间节点，助力技术决策者、风险负责人及关键基础设施运营者规划实施这一复杂技术变革。

加拿大发布了后量子密码迁移路线图，要求联邦各部门在2026年4月前提交初步后量子密码迁移计划，并每年持续报告。高优先级系统在2031年底之前完成迁移，所有剩余系统在2035年前完成迁移。

韩国国家情报局和科学技术信息通信部（MSIT）发布了后量子密码总体规划，计划在2035年之前将相关密码系统转变为后量子密码。

我国尚未发布后量子迁移规划，但相关机构已开展后量子密码迁移的相关研究工作。赛迪智库在《应对量子计算挑战需积极推进后量子密码研发和迁移》中提出国家层面应统筹开展为期10~15年的后量子密码研发和迁移计划。信通院发布的《后量子密码应用研究报告》系统梳理了当前阶段后量子密码的发展情况。

4 后量子密码应用方向

4.1 后量子数字证书

PKI/CA是一种利用公钥密码体制建立起来的具有普适性的安全基础设施，身份认证系统通过密码协议验证用户或设备的身份，用以安全地访问资源。此类系统通常使用非对称密码机制（如数字签名或密钥协商）来实现安全的身份确认。PKI/CA的核心是数字证书，证书采用的签名算法以及证书中包含的签名算法大多为RSA、ECDSA、SM2等非对称密码算法，难以抵抗量子计算攻击。为抵抗量子计算攻击，可在保留原有数字证书格式的基础上，兼容后量子签名算法，构建支持经典算法和后量子算法的混合证书。与传统的数字证书相比，后量子数字证书与传统数字证书格式完全相同，只是对数字证书的长度进行了扩展。与简单的后量子算法替换相比，混合数字证书模式可以更好地支持PKI/CA系统向后量子方向平滑过渡，并且兼顾了经典安全和量子安全。

4.2 后量子安全传输协议

SSL、IPsec、SSH等是实际中应用最为广泛的网络传输协议，为开放网络上的数据通信提供安全保障。在量子计算攻击背景下，采用非对称密码算法的网络传输协议会遭受严重的安全威胁，可采用基于后量子密码的网络安全传输替代方案（见图1），通过替换通信双方的双向认证算法、密钥协商算法以及会话密钥加密算法，实现SSL、IPsec、SSH等具备抵抗量子计算攻击的能力。在密钥协商阶段，采用后量子密码算法代替传统的RSA、ECDSA、SM2等非对称密码算法，通过后量子密钥封装机制实现共享密钥交换。在保证网络传输协议框架兼容性的前提下实现向后量子平滑过渡。

4.3 后量子密码服务

基于后量子密码服务平台提供统一的后量子密码服务，采用具备后量子密码算法的密码设备构建后量子密码资源池，通过密码资源统一接入接口实现对各类后量子密码设备服务能力的接入（见图2）。在业务系统进行后量子密码迁移时，能够通过灵活的密码算法调度，实现传统密码与后量子密码的混合模式，在对现有业务系统密码改造的基础上，完成传统密码服务向后量子密码服务的平滑切换，助力企业快速实现后量子密码技术的安全集成与应用，提升企业系统抵抗量子计算攻击的能力。

5 后量子密码迁移策略和建议

后量子密码迁移的核心任务是公钥密码算法的安全替换，主要涉及数字签名、门限密码等公钥密码

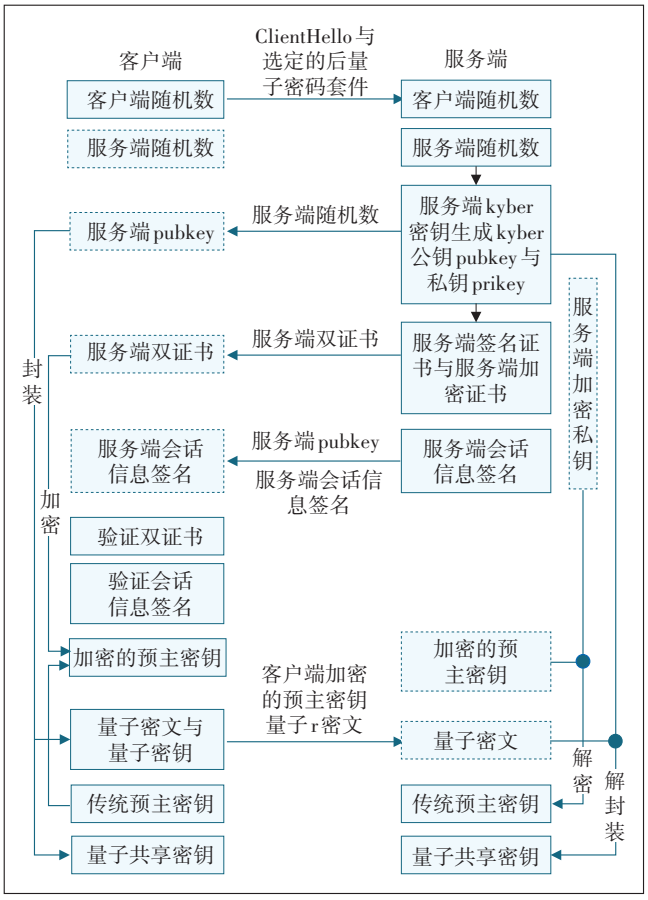

图1　基于后量子密码的安全传输过程

机制的后量子密码迁移。然而，这一迁移面临多重挑战，包括签名长度显著增加导致的存储开销上升、计算复杂度提高引发的处理延迟增加、网络传输数据量增大带来的通信成本上升，可能造成系统吞吐量下降，影响存储效率与数据同步性能。后量子密码迁移是一项系统性工程，需综合评估对系统软硬件架构、安全协议兼容性及安全合规性的影响，制定科学严谨的迁移计划，确保在不影响业务连续性与稳定性的前提下实现系统的量子安全保障。

5.1 加快推进后量子密码标准化进程

后量子密码标准体系的构建不仅是技术问题，更是国家网络空间安全战略竞争的核心环节，对国家安全、技术自主可控、产业经济合作及全球治理话语权具有深远影响。目前西方国家已建立相对完善的后量子密码标准体系，计划在2035年前完成全行业后量子密码迁移。但我国今年刚启动后量子密码算法标准征集工作，而从算法征集到标准发布再到产业落地需经历较长时间。若我国在标准完善后再启动迁移部署，可能加剧中美在后量子密码领域的技术代差，带来严峻的网络安全风险挑战。近10年来，我国在后量子密码领域已取得显著进展，在格密码关键科学问题研究上实现突破，初步形成国际领先优势，国内高校与科研机构已设计出多款性能指标国际领先的后量子密码算法。因此，加快我国主导设计的后量子密码算法，持续推进其标准化进程具有重要意义。在国内后量子密码算法标准研制过程中，企业应积极开展混合后量子密码技术验证，提前布局后量子密码迁移工程。

5.2 制定后量子密码实施路线图

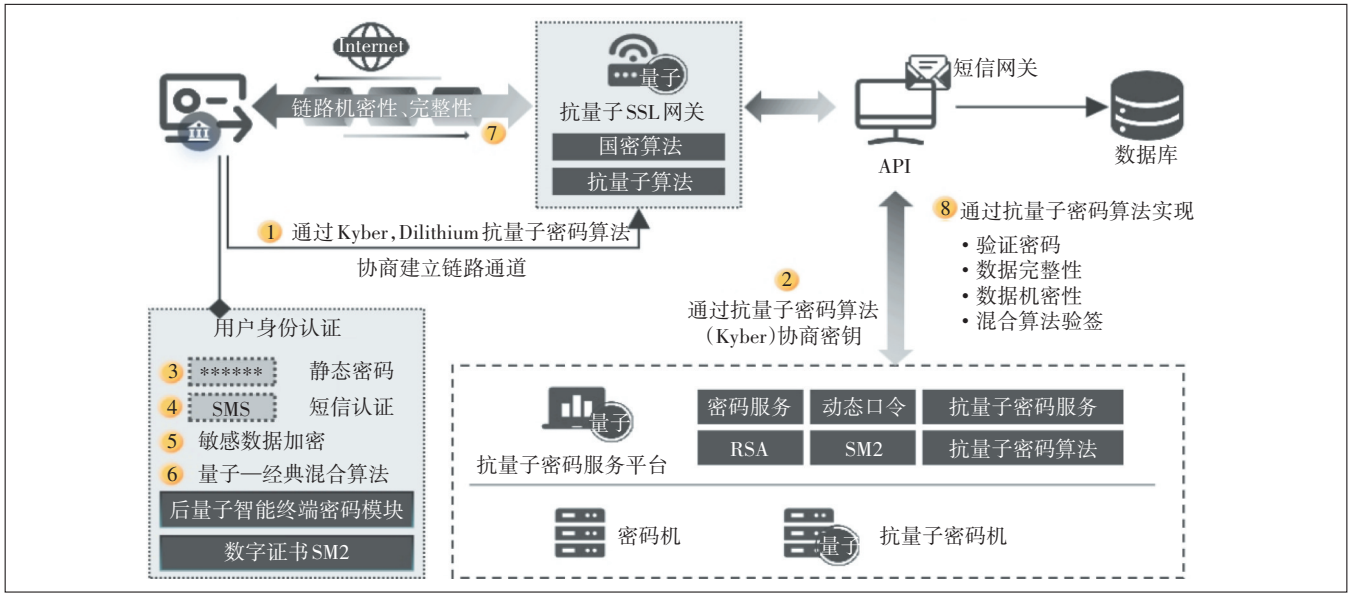

图2　后量子密码服务过程

a）精准识别迁移对象。在开展业务系统后量子密码迁移时，需结合业务系统建设现状确定后量子密码应用范围，基于量子计算攻击带来的潜在威胁，识别易受到量子计算攻击的风险暴露面。对广泛使用RSA、ECDSA、SM2等非对称密码算法用于保护数据机密性和完整性的业务系统，因其在量子计算环境下风险等级高，应优先纳入迁移范围。

b）科学制定迁移策略。需构建多维度的后量子密码迁移实施策略，根据业务场景特性选择合适的后量子密码算法，采用模块化的密码组件替换方案，在不改变现有架构的基础上逐步提升业务系统的抵抗量子攻击能力。由于业务系统的复杂性和多样性，全系统同步完成后量子迁移不具备可行性，应优先针对高风险、核心业务系统开展迁移，持续优化方案和积累实战经验，为全面迁移制定明确的阶段化时间表。

c）开展全面可行性论证。迁移实施前需进行系统的技术可行性验证，对现有业务系统的密码算法应用、安全协议设计及密钥管理机制进行全面评估，分析密码组件替换为后量子组件后的平滑迁移可行性。在迁移过程中，需建立常态化测试验证机制，持续对后量子技术应用效果进行评估，确保全面迁移后业务系统的稳定运行。

d）动态优化迁移方案。基于可行性论证过程中的测试和验证结果，形成后量子密码迁移分析报告，并给出改进方案，进一步指导企业细化后量子迁移实施计划，持续改进后量子密码迁移的实施策略，建立动态调整的迁移策略优化机制。

5.3 加强密码应用技术创新

在抵御量子计算攻击的战略背景下，应大力鼓励后量子密码技术创新，持续加大对基于格、多变量及编码的后量子密码技术应用落地的资源投入，推动后量子密码技术与实际业务场景的深度融合创新，提升业务系统的量子安全保障能力。通过政策引导、资金倾斜与产学研用协同机制，鼓励产业链各方加大后量子密码应用研究力度。电信运营商作为通信领域技术应用创新的主体，应积极参与后量子密码技术研发与试点验证，加快迁移技术的工程化落地，带动产业向量子安全能力升级方向发展，筑牢数字经济高质量发展的安全基石。

6 结束语

随着量子计算技术的持续演进，量子计算攻击将对网络空间安全乃至国家安全构成重大潜在影响，特别对基础通信网络、云基础设施等新一代信息基础设施的安全运行带来严峻挑战。后量子迁移技术的突破将深刻重塑网络安全防护体系的新格局，本文提出的后量子密码迁移实施策略，结合业务系统抵御量子攻击的实际需求，精准识别量子计算攻击风险并制定科学的后量子实施计划，可为提升企业量子安全防护能力提供参考。展望未来，发展自主、可控、可用的后量子密码技术，对于持续应对国内外网络安全威胁，保障国家网络空间安全，具有重要的现实意义与战略紧迫性。

参考文献：

[1] SHOR P W. Algorithms for quantum computation：discrete logarithms and factoring[C]//Proceedings 35th annual symposium on foundations of computer science. Santa Fe：IEEE，1994：124-134.

[2] JOSEPH D，MISOCZKI R，MANZANO M，et al. Transitioning organizations to post-quantum cryptography[J]. Nature，2022，605(7909)：237-243.

[3] MOSCA M，PIANI M. Quantum threat timeline report 2024[R/OL]. [2025-02-17]. https://globalriskinstitute. org/publication/2024-quantum-threat-timeline-report/.

[4] National Institute of Standards and Technology. Module-lattice-based key-encapsulation mechanism standard：FIPS 203[S/OL]. [2025-02-17]. https://csrc.nist.gov/pubs/fips/203/ipd.

[5] National Institute of Standards and Technology. Module-lattice-based digital signature standard：FIPS 204[S/OL]. [2025-02-17]. https://csrc.nist.gov/pubs/fips/204/ipd.

[6] National Institute of Standards and Technology. Stateless hash-based digital signature standard：FIPS 205[S/OL]. [2025-02-17]. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.205.pdf.

[7] LENSTRA A K，LENSTRA H W，Jr，LOVÁSZ L. Factoring polynomials with rational coefficients[J]. Mathematische Annalen，1982，261(4)：515-534.

[8] LYUBASHEVSKY V，SEILER G. NTTRU：truly fast NTRU using NTT[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems，2019，2019(3)：180-201.

[9] MCELIECE R J. A public-key cryptosystem based on algebraic coding theory[R/OL]. [2025-02-17]. https://home.cs.colorado.edu/~jrblack/class/csci7000/f03/papers/mceliece.pdf?origin=publication_detail.

作者简介：

韩浩，毕业于北京大学，高级工程师，博士，主要从事网络空间安全、密码安全、量子安全相关工作；鲁华伟，毕业于郑州大学，正高级工程师，学士，主要从事数据通信咨询与设计、IP网络规划、网络空间安全相关工作；邹艳鹏，毕业于哈尔滨理工大学，学士，主要从事网络空间安全、密码安全、零信任等相关工作。