2025 中国联通后量子密码白皮书

中国联通研究院

2025 年 7 月

版权声明

本白皮书中所涉行业规模、市场预测及趋势分析，系基于公开资料、专家访谈与样本调研所得，因方法和样本范围所限，仅反映撰写时间点的综合判断，不对其准确性与完整性作出任何保证。读者应结合自身实际需求，审慎评估报告内容的适用性。因使用本报告或其任何部分而产生的直接或间接损失，本公司不承担任何责任。本白皮书不构成任何形式的投资建议或交易指引，读者对其决策及后果应自行负责。

目　录

前 言

随着量子计算技术的快速发展，传统公钥密码体系面临前所未有的安全威胁。为应对这一挑战，后量子密码（Post Quantum Cryptography,PQC）成为全球密码学研究与产业化的战略方向。本白皮书系统梳理了后量子密码的技术路线、标准化进程、产业化应用及通信系统的迁移路径，结合国内外研究进展与实践案例，提出了面向未来的密码体系重构策略。

白皮书首先分析了量子计算对传统密码体系的颠覆性影响，明确后量子密码的必要性与紧迫性。通过对比国际主流技术路线（如基于格、编码、哈希等），结合 NIST、欧盟及中国标准化进程，提出了技术选型与兼容性评估框架。随后，白皮书聚焦产业化落地，展示了后量子密码在通信终端、网络设备、数据中心等场景的融合应用，揭示了国产芯片、开源库及云平台的技术突破与生态布局。针对通信系统迁移的复杂性，白皮书提出了分阶段实施路径，强调混合模式与密码敏捷性在保障安全过渡中的核心作用。

白皮书进一步指出，后量子密码的规模化部署需依托政策引导、技术攻关与产业协同。中国在 PQC 领域已取得算法设计、芯片研发、标准预研等阶段性成果，但需加快标准化进程、突破硬件性能瓶颈，并构建覆盖全生命周期的密码治理能力。通过产学研用深度融合，推动后量子密码从实验室走向规模化商用，将为中国在全球量子安全竞争中抢占技术制高点提供关键支撑。

核心编写组成员：

中国联通研究院：王光全、王泽林、赵春旭、周彦韬、屈文秀、马铮

武汉二进制半导体有限公司：陈帅、蔡敏、刘皖熠、陈怡霄

河海大学：曹元、赵海坤、殷子，冯子寒

中科鉴芯（北京）科技有限责任公司：叶靖

南京大学：王中风，田静，李明昊，魏耀东

中国科学院计算技术研究所：穆嘉楠，李华伟，李晓维

南京航空航天大学:刘伟强，崔益军，王辈

中山大学：戴望辰，刘垚

中国船舶集团有限公司第七二二研究所：李杨、陈义涛、吴涵

中汽芯（深圳）科技有限公司：夏显昭

浙江九州量子信息技术股份有限公司：钱懿

北师香港浸会大学:陈东龙，黄军浩

中国科学院大学：沈海华，刘艳

北京普安信科技有限公司：闫淑辉、邓晓辉

一、概述

（一）密码是信息安全体系的基础

习近平总书记强调，“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”国家在宪法、经济法、民法、商法、行政法等多个层级和方面的法律中都对“网络安全”提出了要求。在总体国家安全观引领下，密码技术通过法律保障、标准规范与产业实践的协同，持续为数字时代提供不可替代的安全基座。

其中，《中华人民共和国密码法》旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，提升密码管理科学化、规范化、法治化水平，是我国密码领域的综合性、基础性法律。密码工作需坚持总体国家安全观，遵循统一领导、分级负责，创新发展、服务大局，依法管理、保障安全的原则。坚持中国共产党对密码工作的领导。中央密码工作领导机构对全国密码工作实行统一领导，制定国家密码工作重大方针政策，统筹协调国家密码重大事项和重要工作，推进国家密码法治建设。

（二）现有密码体系的发展与应用

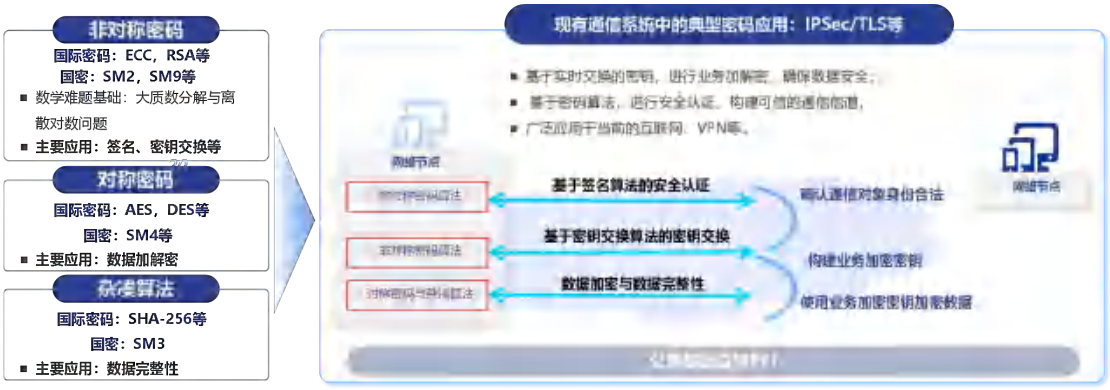

图 1-1 现有密码体系与典型通信应用

传统密码技术作为信息安全的基础，涵盖了对称密码算法、非对称密码算法和哈希算法等多种技术手段。这些密码学算法已被标准化，并广泛应用于各种安全协议和系统设计中，以确保信息的机密性、完整性和真实性。

1. 对称密码算法

对称密码算法，也称为私钥密码算法，依赖于发送方和接收方共享相同的密钥，用于数据加密和解密。由于其加解密效率高，对称密码广泛应用于数据传输加密和数据库存储加密等场景，确保数据的机密性。例如，AES、ZUC、SM4 等经典对称密码算法通过多轮迭代的混淆和扩散机制，保证了密文的不可预测性和安全性。在现代密码学中，对称密码仍然是大多数实际应用中的首选方案，尤其是在高性能要求的场景中。

2. 非对称密码算法

非对称密码算法，又称公钥密码算法，使用一对不同的密钥（公钥和私钥）来实现加密和解密操作。公钥用于加密信息，私钥用于解

密信息，且私钥不需要共享。这种密钥结构解决了对称密码算法中的密钥分发问题，并为身份认证、数字签名等功能提供了安全保障。RSA、ECC、SM2 等算法都是常见的非对称密码算法，它们基于数论中的难解问题，如大整数分解和离散对数问题，具有较高的安全性和广泛的应用场景。

3. 哈希算法

哈希算法用于将任意长度的数据映射为固定长度的散列值。常见的应用包括密码存储和数据完整性校验。SHA、SM3 等哈希算法通过生成唯一的消息摘要，确保数据未被篡改，并为数字签名、认证协议等提供基础支持。哈希算法在保证数据完整性和不可篡改性方面具有重要作用，是现代密码学体系中的关键组成部分。

4. 密码协议

综合运用对称密码、非对称密码和哈希算法，可以构建多种安全协议，这些协议在保证数据机密性、完整性、认证性和不可否认性等方面提供了必要的支持。典型的密码协议如 SSL/TLS、SSH 和 PKI，为互联网通信和电子交易提供了坚实的安全保障[1]。

- **TLS/SSL 协议**：通过加密算法、哈希算法和数字签名技术，确保客户端与服务器之间的安全通信。其核心机制包括握手协议（用于身份认证与密钥协商）和记录协议（用于确保数据传输的机密性与完整性）。在实际应用中，TLS 协议为 HTTPS 提供了安全支持，是万维网数据安全传输的基石。
- **SSH 协议**：则主要用于在不安全的网络环境中提供安全的远

程登录和数据传输。SSH 通过多种身份验证方式（如密码认证和公钥认证）和加密技术，保障了远程通信的机密性与完整性，广泛应用于系统管理和安全文件传输领域。

- **PKI（公钥基础设施）**：通过证书颁发机构（CA）签发的数字证书，提供公钥的可信分发和管理，支撑电子商务和互联网通信中的身份认证与数据保密功能。X.509 证书作为公钥证书的标准格式，已被广泛应用于 TLS/SSL 等网络协议以及电子签名等非在线应用中。

5. 我国商用密码产品及分类

商用密码是指商用密码技术、商用密码产品和商用密码服务的总称，主要用于“不涉及国家秘密内容的信息”领域，即非涉密信息领域。商用密码产业是指采用密码技术，为不涉及国家秘密的信息提供加密保护、安全认证相关技术、产品和服务行业的总称。商用密码产品目前按形态划分为 6 类，分别为密码软件、密码芯片、密码模块、密码板卡、密码整机、密码系统。

表 1-1 我国商用密码分类情况

分类	简介	典型产品
密码软件类	提供纯软件形态出现的密码产品	信息加密软件、密码算法实现软件等产品
密码芯片类	指以集成电路芯片形态出现的密码产品	密码算法芯片、密码 SOC 芯片等产品
密码模块类	指以多芯片组装的背板形态出现，具备专用密码功能，但本身不能完成完整的密码功能的产品	加解密模块、安全控制模块等产品
密码板卡类	指以板卡形态出现，具备完整密码功能的产品，作为密码产品的核心组件	USB 密码钥匙、PCI 密码板卡等产品
密码整机类	指以整机形态出现，具备完整密码功能的产品，以密码板卡为核心组建	VPN、网络密码机、服务器密码机、签名验证服务器等产品
密码系统类	指以系统形态出现，由密码功能支撑的产品，一般由多个密码整机组成	安全认证系统、密钥管理系统等产品

总之，传统密码技术通过对称加密、非对称加密和哈希算法的有机结合，构建了现代信息系统中的核心安全机制。随着技术的不断发

展，这些传统密码学技术将在未来继续演化，提供更为广泛和深入的安全保障。

（三）经典计算机与量子计算机下的密码体系安全性

1949 年，C.E.香农在贝尔实验室技术杂志（Bell Systems Technical Journal）上，发表了一篇题为“Communication Theory of Secrecy Systems（保密系统的通信理论）”的论文。该论文[2]对密码学的研究产生了巨大的影响，并由此开辟了密码技术科学化的先驱。在实际中，无条件安全的系统是不存在的。我们通常所说的算法安全性，就是指算法的计算安全性（Computational Security）。

1．经典计算机下的密码体系安全性

传统计算机，通常指的是现代使用通用的数字计算机，其心脏依赖于硅芯片。传统计算机系统由硬件系统和软件系统两大部分组成。硬件系统是进行信息处理的实际物理装置，主要由中央处理器（CPU）、存储器、输入输出控制系统和各种外部设备组成。

在传统计算机体系下，对称密码（如 AES、ZUC、SM3/SM4 等）的安全性基于密钥长度。攻击的复杂度与密钥空间呈指数关系，如 AES-256 的经典安全强度为 256 位。早期的对称加密算法如 DES（Data Encryption Standard）已被更安全的算法如 AES（Advanced Encryption Standard）所取代。AES 提供 128、192 和 256 位密钥长度、SM2 提供 128 位密钥长度，能够有效抵抗经典计算机的暴力破解等攻击手段。

非对称加密算法如 RSA、ECC（Elliptic Curve Cryptography）等基于复杂的数学难题（如大数因子分解、椭圆曲线离散对数问题等），这些难题在目前的计算能力下难以被破解。

2. 量子计算机下的密码体系的安全性

量子计算机是一种利用量子力学原理进行信息处理与计算的物理装置，具有运行速度快、处置信息能力强、应用范围广等特点。随着技术的不断发展，量子计算机将在更多领域展现出其独特的优势和价值。

量子计算对对称密码存在一定威胁，主要得益于 Grover 算法和 Simon 算法。Grover 算法能够针对穷尽搜索的时间复杂度提供平方加速[3]，而 Simon 算法则可在多项式时间内解决特定周期性问题，并对特定密码结构提供指数级加速[4]。尽管如此，这些量子攻击对对称密码的影响有限，通过增加密钥长度即可抵抗量子攻击。例如，增加哈希函数输出长度能够有效对抗量子原像攻击。因此，量子计算对对称密码的威胁相对较小，主要的安全风险集中在公钥密码领域。

Shor 算法在 1994 年提出，能够以多项式时间复杂度解决大整数分解和离散对数问题[5]，直接威胁到以数论难题为基础的公钥密码系统，包括 RSA、Diffie-Hellman、ElGamal、Schnorr 签名、椭圆曲线加密与签名（如 ECDSA、ED25519、SM2）等。若大规模容错量子计算机成为现实，这些公钥密码将失去安全性。

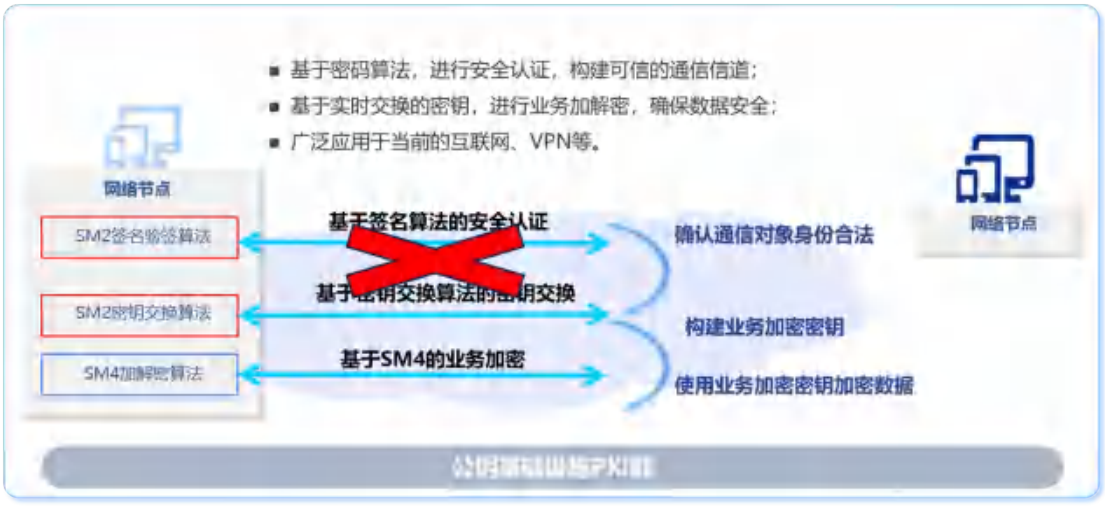

图 1-2 量子计算机对现有密码体系的威胁

此外，"现存后解"（Store-now-decrypt-later，SNDL）攻击也加剧了这一威胁。如图 1-3 所示，攻击者可存储当前无法破解的密文，待量子计算能力足够强大后再行破解[6]。尽管当前的量子计算能力仍不足以破解大规模密钥，但随着量子技术的快速发展，预计 2035 年左右，百万级量子比特的计算机可能问世，届时现有的公钥密码系统将面临巨大挑战[7]。因此，对未来保密期超过 10 年的敏感信息，使用现有公钥密码已不再安全，必须尽早转向后量子密码方案。

图 1-3 后量子密码迁移的阶段性挑战与长期威胁应对

基于图 1-3 所示的迁移挑战与威胁应对框架，量子计算对信息

安全的威胁已形成系统性风险链。表 1-2 进一步揭示该风险链如何通过四类攻击路径（先存储后解密攻击、代码签名破解、历史数据篡改、密钥基础设施崩溃）从技术漏洞渗透至业务场景，最终引发隐私泄露、关键业务中断乃至国家安全危机等三层级灾难——这种从"量子计算能力演进"到"系统性安全崩塌"的传导逻辑，正是迁移必须优先阻断的核心威胁路径。

表 1-2 量子计算安全隐患分析表

针对数据安全，实施先存储后解密	代码签名与数字签名	篡改历史数据	密钥管理攻击
在量子计算机可用之前，攻击者会收集数据并进行存储，在量子计算能力成熟时再解密这些数据。该攻击会对需要长期保密的数据安全性形成威胁，例如企业核心数据、国家机密或个人生物数据等。目前普遍认为一些攻击者已经在进行这种类型的攻击。	如果加密算法在量子计算的威胁下变得脆弱，针对代码的身份认证服务可能会受到攻击（例如汽车 OTA 等），从而导致软件更新中出现漏洞。	如果数字签名算法量子计算的威胁下变得脆弱，数字签名数据的完整性可能会受到破坏，例如审计记录、通话记录、合同和其他数据。	密钥基础设施使用非对称密码来存储对称密钥。因此，用于长期存储的密钥有可能因为非对称密码遭到量子计算机的攻击而变得脆弱。

上述风险可能导致隐私泄露、声誉受损、网络中断甚至国家安全等具有重大影响的后果。

（四）应对量子计算机威胁-不断迭代的密码体系

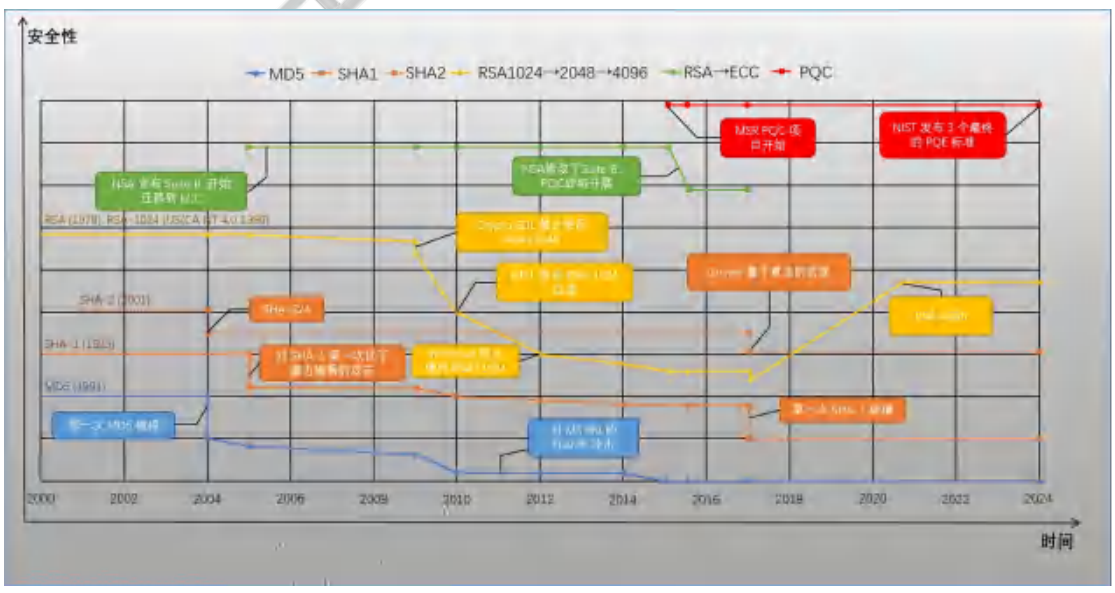

图 1-4 密码算法的发展

为了应对量子计算机威胁，当前主要有两种技术路线，即量子保密通信技术以及后量子密码技术：

1. 量子保密通信技术

量子保密通信也被称为量子密码或量子密钥分发（QKD），是利用量子力学的基本原理（如未知量子态不可克隆定理和海森堡不确定性原理）或量子纠缠等特性，来建立对称密钥，并通过这些密钥实现安全的通信。量子保密通信的安全性基于物理学基本原理，与计算复杂度无关。即使未来出现强大的量子计算机，也无法对其安全性构成威胁。由于量子态的不可克隆性和测量干扰性，任何对量子信息的窃听或篡改都会被通信双方立即察觉，从而确保通信的高安全性。

2. 后量子密码算法

密码学是动态发展的。如图 1-4 所示，随着现代计算机以及密码分析学的发展，密码算法的安全性会随时间而逐渐降低。当密码算法无法满足数据安全需求时，就需要向新的密码算法迁移。

例如，由于碰撞攻击的突破，SHA-1 算法的安全性大幅降低，因此目前应用都迁移至 SHA-2 算法。由于传统计算机及密码分析学的快速发展，RSA-1024 被证明缺乏安全性，目前相关应用向 RSA-2048、RSA-3072，甚至 RSA-4096 迁移。由于迁移过程的复杂性，上述迁移往往需要超过十年时间来完成。

随着量子计算技术的迅速发展，传统密码学的安全性面临前所未有的挑战。现代密码学在保护数据隐私和确保信息安全方面发挥了关键作用，其基础主要建立在计算复杂性理论上。无论是对称密码算法、

非对称密码算法，还是哈希函数，传统密码技术的安全性依赖于现有经典计算机在合理时间内无法破解这些算法。然而，量子计算凭借其强大的并行计算能力，能够在某些情况下显著减少密码算法的破解时间，威胁到现有的安全体系。因此，在密码学领域，探索后量子密码学（Post-Quantum Cryptography，PQC）的技术路线，旨在设计能够抵抗量子计算攻击的新型密码方案。

后量子密码算法的数学原理主要基于量子计算难以解决的数学问题，如基于格的密码学、多变量密码学、编码密码学和哈希密码学等。这些算法在设计时就考虑到了量子计算的威胁，因此能够在量子计算时代保持通信的机密性和完整性。

表 1-3 QKD 与 PQC 技术详情表

技术路线	原理	实现方法	适用场景
QKD	量子力学基本原理，如未知量子态不可克隆定理和海森堡不确定性原理。	量子通信专用设备。	应用于对安全性要求极高的场景，受通信距离和传输媒介的限制，目前难以实现长距离、大规模的密钥分发。
PQC	量子计算难以解决的数学问题，如基于格的密码学。	兼容现有软硬件实现方法。	适用于所有需要密码保护的场景，但是需要与现有密码体系兼容。

量子密钥分发和后量子密码在应对量子计算威胁的密码学领域中各有优势和特点。量子密钥分发提供无条件的安全性保障和实时性优势，但受通信距离和传输媒介的限制；而后量子密码则具有多样性和兼容性优势，适用于更广泛的场景。未来随着技术的不断发展和应用需求的不断增加，两者将在各自的领域发挥重要作用。

二、后量子密码算法及算法实现

（一）后量子密码技术路线

如图 2-1 所示，随着量子计算机的发展，经典密码算法如 RSA 和 ECC（椭圆曲线加密）面临着巨大的安全威胁。为了应对这种潜在威胁，密码学家和研究人员开始开发新一代基于不同数学难题的后量子密码算法（如图 2-1 示）。这些算法旨在抵御量子计算的攻击，确保未来的信息安全。根据其底层数学问题的不同，后量子密码算法的研究主要可以分为五种技术路线：基于格的密码、基于编码的密码、基于多变量的密码、基于哈希函数的密码以及基于同源曲线的密码。

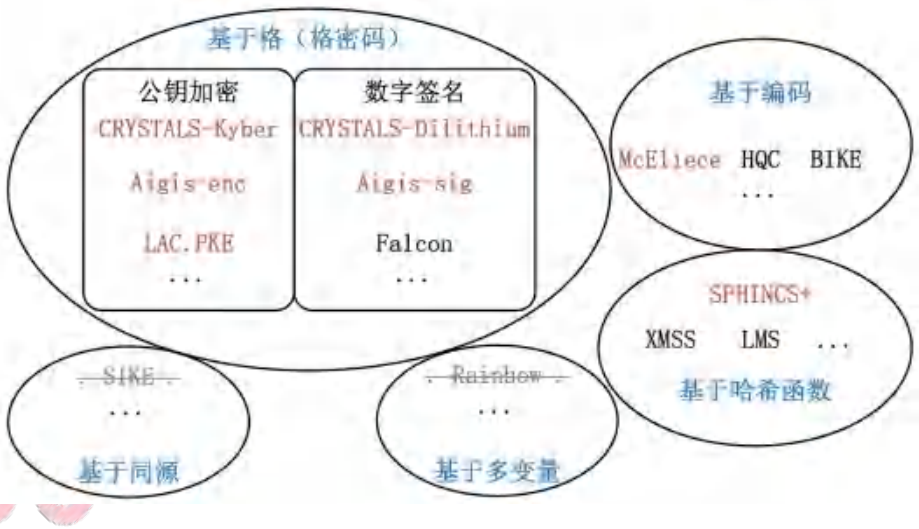

图 2-1 PQC 密码算法的数学基础

1. 基于格的密码

格密码是基于数学中的格（Lattice）结构构造的密码系统，格可以看作是一种离散的加法子群，由一组线性无关的非零向量生成。格密码的安全性依赖于在格上求解某些难解问题的困难性，如最短向量问题（SVP）、最近向量问题（CVP）及其变种。Ajtai 和 Regev

分别引入的小整数解问题（SIS）和容错学习问题（LWE）为实用的格密码研究奠定了基础[8]。

基于格的密码算法因其多功能性和高效性，成为目前后量子密码学研究的主流方向之一。SIS 和 LWE 等问题不仅用于构造加密和数字签名方案，还可用于构建诸如全同态加密、不可区分混淆等高级密码学原语。目前，NIST 后量子密码标准化过程中，多个基于格的算法进入了最终的候选阶段。这类算法通常具有较小的公私钥尺寸和较快的计算速度，非常适合实际应用环境。

2. 基于编码的密码

基于编码的密码依赖于信道编码中的难解问题，其原理是设计高效的冗余编码来纠正传输过程中出现的错误。在密码学领域，研究人员发现某些编码问题在译码时的复杂性可以用于构造安全的加密算法。基于编码的密码算法通常具有较小的密文，但也存在公钥尺寸大的缺点，这在实际应用中带来了挑战。

最著名的基于编码的密码方案是 1978 年由 McEliece 提出的经典 McEliece 加密方案，该方案基于 Goppa 码，具有非常快的加密速度[9]。尽管其公钥尺寸过大，实用性有限，但由于其后量子安全性，McEliece 方案依然被认为是潜在的替代方案，并成功进入了 NIST-PQC 的前三轮评估阶段。

3. 基于多变量的密码

基于多变量的密码算法是最早提出的后量子密码方案之一。这类算法基于求解高次多变量方程组的 NP 难问题，通常采用有限域上的

二次多项式来构造加密或签名方案。代表性的算法包括 HFEv-类型的 GeMSS 签名体制和 UOV 类型的 Rainbow 签名算法。

基于多变量的密码算法在 NIST-PQC 评估过程中表现出色，尤其在签名验签速度方面具有显著优势。尽管这类算法的公钥尺寸较大，但由于其计算效率高、资源消耗少，适用于无需频繁传输公钥的应用场景。

4. 基于哈希函数的密码

基于哈希函数的密码算法通过将任意长度的消息映射到固定长度的输出，来实现加密或签名。哈希函数通常不依赖任何密钥，安全性来自于找到碰撞的困难性。Merkle 提出的数字签名方案（MSS）是基于哈希函数的早期代表性方案，它通过哈希树结构降低了一次性验证密钥的复杂性[10]。

在 NIST 的后量子密码标准化进程中，基于哈希函数的签名方案取得了重要进展。其中，XMSS 是一种有状态签名方案，SPHINCS+ 则是一种无状态的签名方案。这类算法具有理论上的高安全性，但也面临签名体积过大以及有状态签名次数有限的挑战。

5. 基于同源曲线的密码

同源椭圆曲线密码利用椭圆曲线之间的同态映射来构造加密系统，其代表性算法包括超奇异同源 Diffie-Hellman（SIDH）和 CSIDH。这类密码算法的公钥和密文尺寸较小，非常适合在通信量受限的环境下使用。

2011 年，Jao 等人提出了超奇异同源 Diffie-Hellman 问题，并

设计 SIKE（Supersingular Isogeny Key Exchange）公钥加密系统[11]。然而，尽管 SIKE 进入了 NIST-PQC 的第四轮评估，但不久后其遭遇了致命的攻击，这对同源密码的应用带来了挑战。然而，这并不意味着同源密码研究的终结，同源问题本身仍然是后量子密码学中的一个重要研究方向。

（二）后量子密码技术路线评价

迁移至后量子密码需系统性评估候选算法的适用性。本章从安全性强度、经典平台性能及工程化特性三个维度建立评估模型，为机构选型提供技术依据。

1．安全特性评估

后量子密码算法的安全性是评估其有效性的重要指标。为此，各种算法需要满足以下安全特性标准：

（1） 密码学破解难度

NIST 将后量子密码算法的安全等级与传统密码算法对应，提出了五种不同的安全等级，后量子密码算法应具备以下安全标准，并在实际应用中得到验证：

I. 与 AES-128 一样难以破解： 根据研究，使用经典计算机进行 AES-128 的穷举攻击所需的总计算量为2^{128}次运算。而后量子密码算法如基于格的后量子密码算法所需的计算复杂度也必须确保达到或超过这一标准。对于格基算法，当前最强的攻击方法依然保持在多项式时间的复杂度内，反映出其较好的安全性[12]。

II. 与 SHA-256 一样难以破解：SHA-256 的碰撞搜索复杂度为 2^{128}。后量子密码算法如哈希基密码等（例如 XMSS、SPHINCS+）也需在此范围内提供类似的安全性。

III. 与 AES-192 一样难以破解：AES-192 的安全性同样可以转化为 PQC 算法的安全性，需评估后量子密码算法在应对量子计算时的持久安全性。

IV. 与 SHA-384 一样难以破解：在 SHA-384 的层面，相比于 SHA-256，后量子算法需要提供更强的碰撞抵御能力，以保障信息系统的安全性。

V. 与 AES-256 一样难以破解： AES-256 是现阶段最广泛使用的强密码算法，其抗量子攻击的能力应被后量子密码算法充分检验。

（2） 案例与数据

如 Google 和 Microsoft 合作，针对 PQC 算法的安全性进行持续测试。发现大规模量子计算在破解 NTRU 及其他后量子算法时仍需大量的计算资源[13]。

2. 平台兼容性评估

PQC 算法的成功迁移同样与其在不同平台上的兼容性密切相关。为了确保后量子密码算法的迁移顺利进行，各种兼容性指标显得尤为重要。

（1） 现有系统的集成

后量子密码算法应在现有系统中快速部署。实际上，许多企业在融合后量子密码算法时，其集成时间比他们预期的短了 30%至

50%[14]。例如，使用后量子密钥交换协议的系统能够在不更改基础架构的情况下，迅速实现安全性覆盖。

（2） 性能与效率

性能不仅影响用户体验，也直接关系到算法的应用范围。根据对现有后量子算法的性能比较分析[15]，例如 Kyber 和 FALCON 等算法在计算效率上已经与传统算法（如 RSA 或 ECC）接近，且在数据处理传输时延上，后量子算法与它们的差距逐渐缩小。

（3）标准化和相互操作性

通过与 NIST 以及其他行业组织协作，后量子密码算法的标准化过程正在加速，以确保其在全球范围内的互操作性。例如，NIST 在 2022 年发布的后量子密码标准草案，涵盖了多种后量子算法的推荐实现，为企业提供了清晰指导[16]。这种多方支持的标准化进程促进了各类平台的适应能力与兼容性。

3. 其他特性评估

在后量子密码算法的设计和应用中，还必须考虑多种其他特性。这些特性直接影响算法的可用性和安全性。

（1）即插即用替换

PQC 算法的“即插即用”特性使其在现有系统中集成和应用更具可行性。例如，企业在测试新算法时，能够在不影响正常业务流程的情况下进行迭代更新。通过此方式，不少金融机构如 Visa 和 Mastercard 已经成功嵌入后量子密码协议[17]。

（2）抵御侧信道攻击

后量子密码算法抵御侧信道攻击的能力呈现显著分化，其特性高度依赖数学结构与实现优化。格密码（如 Kyber/Dilithium）的多项式运算易受功耗分析攻击，但掩码随机化技术可降低 99%的差分功耗分析（DPA）成功率；哈希签名（如 SPHINCS+）因无复杂运算天然抗时序攻击，但长签名增加了电磁泄露风险；多变量密码的布尔逻辑降低能量指纹，但公钥结构易遭故障注入破解。当前防护核心围绕三重机制：算法层强制恒定时间实现以消除时序泄露；计算层通过掩码扰乱能量轨迹；硬件层采用可信执行环境（TEE）隔离敏感操作。如 NIST 胜出算法（ML-KEM/ML-DSA）通过掩码+随机化+恒定时间三重防护，在软件/硬件层达到实用级侧信道防御

（3）敏捷性

最后，后量子密码算法需具备良好的算法敏捷性，以适应快速变化的网络安全环境。例如，一些公司通过代码库和开源项目，加快了后量子密码的开发速度，使得算法能够在无需完全重新设计的情况下适应新的网络协议[18]。关于密码算法的敏捷想问题，将在本白皮书的第五章展开讨论。

4. 结论

综合上述各项评估，后量子密码算法的成功迁移将不仅依赖于其在各种平台上的兼容性和安全特性，还需考虑其他关键特性如即插即用、抵御侧信道攻击及敏捷性等。随着量子计算的快速发展，组织应充分进行风险评估并采取行动，在密码管理与安全策略上做好面向未

来的准备。

（三）后量子密码算法的特性差异与应用场景

基于“风险分散＋性能多元＋应用匹配＋分阶段推进”的战略考量，NIST 在最终标准中囊括多种算法类别，确保量子时代的密码体系既安全可用，又能灵活适配各行业的差异化需求。在后量子密码算法标准化过程中需要选出多种算法类型，主要基于以下几点考虑：

多样化的安全假设：每一类算法都基于不同的数学难题——格（LWE/SIS）、编码（McEliece）、多变量方程、哈希树和同源映射等——它们各自抵抗量子攻击的机理不同，互为补充。一旦某一难题被新技术或数学突破削弱，其他类型仍能维持安全性。

性能与资源的权衡：算法在公钥 / 私钥大小、签名 / 密文长度、加解密速度、硬件加速潜力、存储开销等方面差异显著。格基算法（Kyber、Dilithium）兼顾了较小密钥与较快运算，适合大规模网络协议和硬件加速。编码算法（Classic McEliece）公钥尺寸大、加解密快，适用于信任与长期保密场景。哈希基签名（SPHINCS+）无需状态维护，安全性能最强，但签名体积大，适于对侧信道强要求的应用。多变量与同源密码（Rainbow、SIKE）则在签名速度、标识大小或交互模式上提供了独特优势。

协议与应用场景需求：不同协议（TLS、SSH、IPsec、固件签名、IoT 设备认证）对密钥交换和签名有各自的延迟、带宽和兼容要求。NIST 推出混合密钥封装（Hybrid KEM）与混合签名模式，允

许根据场景选择最优算法组合。

风险对冲与分阶段迁移：标准化初期先选出四种主干算法（CRYSTALS-Kyber、CRYSTALS-Dilithium、FALCON、SPHINCS+），并保留多种候选方案进入后续评估。这样既能迅速商用，也为未来可能的安全威胁及需求调整保留空间。

国际互操作与合规：多种算法同时标准化，有助于不同国家、行业与产品在兼容性和合规性上对接。运营商、硬件厂商和安全模块能够根据自身合规要求（FIPS、CC、ISO）选择或组合算法，平滑完成经典密码向后量子密码的演进。

表 2-1 NIST 选择的后量子算法列表

算法	CRYSTALS-Kyber（ML-KEM）	CRYSTALS-Dilithium（ML-DSA）	FALCON（FN-DSA）	SPHINCS+（SLH-DSA）	HQC（Hamming
概述	CRYSTALS-Kyber 是一种基于模格的密钥封装机制（ML-KEM）。它基于有结构格上的模格容错学习（MLWE）数学难题。	CRYSTALS-Dilithium 是一种基于模格的数字签名（ML-DSA）方案。它基于有结构格上的模格容错学习（MLWE）和模格短整数解（MSIS）数学难题。	FALCON 是一种基于快速傅立叶正交格构造的基于格的签名方案。它利用格的代数结构来实现非常紧凑的签名。	SPHINCS+是一种无状态哈希签名方案。这意味着它不需要在签名操作之间维护任何内部状态，使其在某些情况下更容易部署。	HQC 是一种基于编码的公钥加密方案，它依赖于随机线性码的解码难度，使用准循环码来提高效率。
用途	通用密钥交换，类似于 RSA 或 Diffie-Hellman，适用于保护传输中数据的机密性。	用于身份验证和不可否认性的数字签名，确保数据的完整性和真实性。	该数字签名算法的签名较小，特别适用于带宽受限或存储签名成本较高的场景。	用于数字签名，尤其适用于在对抵御侧信道攻击有较高要求的场景。另一方面，其基于哈希的底层架构使得更容易在现有系统中完成软硬件实现。	通用密钥交换，类似于 RSA 或 Diffie-Hellman，适用于保护传输中数据的机密性。
替代	用于替代密钥交换算法，如 RSA, Diffie-Hellman, ECC（ECDH 和 X25519/X448）	用于替代数字签名算法，如 RSA, ECDSA, EdDSA（特别是使用 NIST 曲线和 Ed25519/Ed448 曲线的 ECDSA/EdDSA）	特别关注签名的场景下，用于替换数字签名算法 RSA, ECDSA, EdDSA。	在抗侧信道攻击能力是主要关注点的场景下，用于数字签名的 RSA, ECDSA, EdDSA。	用于密钥交换的 RSA, Diffie-Hellman, ECC（ECDH 和 X25519/X448）
技术细节	Kyber 是一种密钥封装机制（KEM）：发送方生成一个随机密钥，使用接收方的公钥将其封装，并将密文发送给接收方。接收方随后使用其私钥解封出该密钥。	Dilithium 采用“Fiat-Shamir-with-Aborts”技术，通过拒绝采样（rejection sampling）保证签名紧凑且抵抗量子计算攻击	FALCON 基于一种基于格上最短整数解（SIS）问题的陷门函数构建。	SPHINCS+基于 Merkle 树结构，并使用哈希函数作为其主要构建模块。	HQC 的公钥从一个随机线性码中提取。通过用随机错误向量编码明文消息生成密文。为确保安全通信，接收方使用其私钥（对应的解码能力）解密密文并恢复原始消息。

如表 2-1 所示，NIST 目前已选取了 5 种算法，它们都提供了多组不同的参数，以达到不同的安全级别，使用者可以专注于选择一组参数，以满足应用程序的独特安全需求，根据平台和实现的不同，这些算法的性能可能会发生变化。国内提出 PQC 算法大多也是基于格问题构造的，其中最为主流的方案 Aigis-enc 和 Aigis-sig 分别在原有 Crystals-Kyber 和 Crystals-Dilithium 方案的框架上进行了改良，充分利用非对称模块 LWE（AMLWE）的困难度，并仔细选择参数，在计算成本、存储开销和安全性之间获得了更好的折衷，具有更短的公钥和密文/签名，相较 NIST 标准有所领先，有望在未来成为国产标准化算法。

（四）通信系统中的软硬件支持

1. 全定制硬件的后量子密码算法实现研究

全定制硬件实现的后量子密码芯片，可以独立实现某个或者某一类数学困难问题密码算法的完整计算过程，这种实现方式适用于计算速度或功耗具有严格要求的应用场景。

由于基于格的密码算法研究相对成熟，一直是 PQC 标准化过程中的主流候选算法，因此无论是针对基于格的密码算法中的核心计算模块（如多项式乘法、采样等），还是完整算法的专用硬件设计都获得了更为广泛持续的关注。Yaman 等人[19]通过代数优化设计了支持双模式（NTT/INTT）的动态可重构处理单元，兼顾轻量化与高性能需求，显著提升 Kyber 中多项式环运算的硬件效率。Alhassani 等人

[20]创新性地采用剩余数系统（RNS），结合快速查找表与子模数分解策略，在 FPGA 平台上构建了适配单/双蝶形架构的高速模乘加速器。Guo 等人[21]则提出一种双模式无冲突内存映射方案，结合混合基 2/4 NTT 算法与“延迟末层”（lazy-last-layer）技术，在无需预处理的前提下提升内存带宽利用率，并通过优化存储访问模式避免采样数据对大型 FIFO 的依赖。Li 等人[22]提出了一种超低复杂度的多项式乘法架构，将参数特性进行充分利用，可以有效提升模格密码算法的速度和面效比，在参数选取合适的情况下，可以实现 50%的面效比提升和 1.86 倍的加速比提升。针对全流程硬件化需求，Xing 等人[23]首次实现 Kyber 的纯硬件架构，集成多模式蝶形运算单元与可配置 Keccak 模块，结合模数定制化算法压缩资源开销，达成全参数支持下的低面积设计。Nguyen 等人[24]提出了专为 Kyber 定制的轻量级 SHA3 哈希模块，显著减少了对 FIFO 等额外硬件资源的需求，并首次提出无存储型迭代 NTT 架构，在 FPGA 上实现了完整算法最小的硬件资源开销。Cui 等人[25]提出了一种基于指令的高性能控制器架构，并设计了多种存储格式和高效的数据调度方案，通过内部和外部指令集协调控制各子模块，提高模块复用性和灵活性，在灵活性、性能和资源效率之间实现了良好平衡。Zhao 等人[26]面向 Dilithium 的高效部署，提出分段流水线处理机制，通过中间数据复用与模块级加速（如 NTT、SampleInBall 及 Decompress 优化），同步降低存储需求与计算延迟。Gupta 等人[27]进一步融合资源共享、预计算查找表等策略，在 FPGA/ASIC 平台实现高面积时间积效率，大幅缩短

Dilithium 密钥生成、签名及验证的时序开销。Li 等人[28]提出多指令并行架构与定制指令集，实现多项式级并行计算，采用 Karatsuba 算法将 23×23 位乘法分解，进一步减小关键路径，实现了 Dilithium 最高性能的硬件设计方案。

除了格密码外，针对基于编码的密码算法，Zhu 等人[29]为解决 Classic McEliece 的密钥生成时间开销过大的问题，提出了高吞吐的密钥生成加速器 Mckeycutter，根据可并行的任务划分和模式配置，在降低 BRAM 的同时提升了计算速度。此外，针对 HQC 和 BIKE 也有一些硬件优化成果，[30]和[31]分别提出了专门针对 HQC 和 BIKE 算法进行全定制人工设计优化，并支持密钥产生、封装和解封装的硬件设计。针对基于哈希的密码算法，[32-35]等工作基于 XMSS、LMS 和 SPHINCS+算法也分别提出了相应的高效定制硬件设计。

随着后量子密码算法标准化的逐步收敛，现有的 PQC 实现研究工作也逐渐从单一算法的硬件优化实现，转向多种后量子密码算法的融合架构设计，以更好地应对未来新一代密码的迁移部署，适配多样复杂的应用场景。Aikata 等人[36]提出了一种统一的架构 KaLi，它可以对 Kyber 和 Dilithium 的所有安全级别执行密钥生成、封装、解封装、签名生成和签名验证，[37]中则为 Kyber 和 Dilithium 的融合硬件加速器提出了一种混合多路径延迟换向器流水线架构（HMDC）。Zhu 等人[38, 39]为进一步提高后量子密码芯片的功能灵活性，研发了两款可重构密码芯片 RePQC 和 PQPU，支持国内外多种主流后量子密码算法。

2. ARM 上的后量子密码算法实现研究

在 NIST 于 2016 年开始征集后量子密码算法以来，已有大量研究人员对后量子密码在专用芯片上展开软件实现优化研究。本章着重介绍四个后量子密码标准算法在物联网和移动设备等专用芯片上的软件实现优化技术，主要针对两种芯片：基于 ARMv7-M 架构的 Cortex-M 系列物联网芯片（其中 Cortex-M4 是 NIST 在物联网设备上评估后量子密码算法的推荐平台）和基于 ARMv8 或 ARMv9 架构的 Coretx-A 系列移动设备芯片。

Cortex-M 系列：在这类平台上的优化一般集中在优化核心算子如模乘算法、NTT 和 Keccak，同时内存优化也是后量子密码能否部署在物联网芯片上重要优化点。现有后量子密码在 Cortex-M4 上的软件实现优化一般都被收集在 pqm4[40]代码库中，该库收集了大量发表在各种会议或者期刊的优化实现代码，能够轻松、快速地评估对比各种后量子密码的实现效率。2019 年，Botros 等人[41]首先在 Cortex-M4 对 Kyber 进行了内存优化和性能提升，他们利用 Seiler[42]于 2018 年提出的有符号 Montgomery 模乘算法实现了有符号 NTT 实现，其 NTT 实现比 Kyber 提交者所提交的 NTT 实现快两倍，他们还提出了多项式矩阵、向量的即时生成策略来降低 Kyber 的内存占用，使其更适用于物联网芯片。Alkim 等人[43]则进一步提出了在 Cortex-M4 上仅需两个时钟周期的最优 16 位 Montgomery 约简算法实现、实现了更优的层合并技术优化 NTT，并利用延迟约简技术优化了 Kyber 的点乘运算。Greconici 等人[44]则提出了在 Cortex-M4

上最优的32位Montgomery约简算法实现，并给出了在Cortex-M3上恒定时间的 32 位 NTT 实现。Abdulrahman 等人[45]则提出了更优的有符号 Barrett 约简算法用于约简 Kyber 的 NTT 中的约简运算，并提出可以利用更快的 16 位 NTT 快速实现 Dilithium 中的部分多项式运算。2022 年，Huang 等人[46]创新性地提出了 Cortex-M4 上仅需两条指令的 16 位 Plantard 模乘算法，比最优的 Montgomery 模乘算法[43]快一条指令。他们[47]将 Plantard 模乘扩展到 Cortex-M3 和 RISC-V 两种低端 32 位物联网平台中，有效地在这些平台上提升 NTT 的实现效率。此外，Huang 等人[48]还对格基密码算法中最耗时的算子 Keccak 在 ARMv7-M 平台上进行内存访问的流水线优化，极大地提升了格基密码算法中 Keccak 的实现效率。除此以外，为探索后量子密码在物联网芯片的部署性，Hülsing[49]、Bos[50]人还专门探索了 SPHINCS、Dilithium 在物联网专用芯片上的内存优化，有效论证了后量子密码在这些平台上的可用性。

Cortex-A 系列：在移动设备芯片上，与物联网芯片相比，由于内存充足，内存优化在这些平台上则没有那么重要，因此，这些平台上的优化通常集中在算法的核心算子模乘算法、NTT 和 Keccak 等。Nguyen 等人[51]和 Sanal 等人[52]分别在 ARMv8-A 上利用 NEON 对 Kyber 后量子密码进行加速实现，其 Kyber 实现效率比参考实现快 3 倍以上。Sanal 等人[52]还指出利用 ARM 的 AES 硬件加速指令可极大地提升 Kyber-90s 的实现效率。Becker 等人[53]指出 Barrett 约简与 Montgomery 模乘算法之间存在关联，首次提出了当前最优的

Barrett 模乘算法，该算法可以利用 NEON 或 AVX2 等 SIMD 指令集进行高效的实现；他们还针对 Kyber 的不完整 NTT 提出了“非对称乘法”优化技术，利用缓存技术提升点乘运算的实现效率。其次，Becker 等人[54]进而提出可以利用 ARM 中的内联 Barrel 移位指令降低旋转指令的使用数量，并利用 Cortex-A 系列芯片的流水线提出混合 Keccak 实现技术，极大地提升了 Keccak 在格基密码算法或基于哈希的后量子密码算法 SPHINCS+的实现效率。除了以上优化技术，Nguyen 等人 和 Kim 等人[55-57]还分别对 Falcon、Kyber、Dilithium 这些后量子密码算法在 Cortex-A 系列芯片的实现进行了更细致的优化研究。下表给出部分参考文献的实现性能和内存占用以供参考。

表 2-2 后量子密码在 ARM 上实现性能与内存占用

	算法	时钟/内存占用（cc/bytes）		
		KeyGen	Encaps/Sign	Decaps/Verify
Cortex-M4[42]	Kyber-512	499k/3136	634k/2720	597k/2744
Cortex-M4[43]	Kyber-512	452k/2392	586k/2344	542k/2360
Cortex-M4[47]	Kyber-512	369k/2292	448k/2348	409k/2332
Cortex-M4[45]	Dilithium2	2267k/7916	3097k/14428	1259k/9004
Cortex-M4[47]	Dilithium2	1595k	4052k	1576k
Cortex-M4[50]	Dilithium2	2927k/4900	18470k/5000	4036k/2700
Cortex-A72[51]	Kyber-768	110k	141k	138k
Cortex-A72[54]	Kyber-768	100k	128k	121k
Cortex-A72[53]	Dilithium3	534k	1188k	454k
Cortex-A78[58]	SPHINCS+-128	5043k	117280k	7949k
Jetson AGX Xavier[53]	Falcon-512	-	498k	29k

3. RISC-V 上的后量子密码算法实现研究

在 RISC-V 平台中，可以使用硬件/软件协同设计技术，开发复杂且高度定制化的 PQC 解决方案。在早期，大家都是将加速器放在处理核心的外面这一松散耦合的加速器设计来实现。Fritzmann 等人[59]是通过协同设计进行后量子加速的首批提出方案之一，其实现了 IEEE-1363.1 标准化版本的 NTRUEncrypt，仅使用松散耦合协处理器来加速多项式乘法。随后 Banerjee 等人[60]提出了一种灵活的加密

处理器，通过加速算法中的多项式乘法和 keccak 内核，能够支持多种格基后量子密码算法，包括 Kyber 和 Dilithium。

虽然松散耦合方案易于集成到系统中,但它通常灵活性较差并且需要较高的通信开销。因此，Fritzmann 等人[61]的研究将后量子加密技术的加速器从松散耦合过渡到紧密耦合，作者将硬件加速器集成到了 RISC-V 内核中，包括一个 SHA-256 内核和二次多项式乘法。在 Alkim 等人[62]中，作者进一步将有限域乘法器集成到 RISC-V 处理器中，以加速 Kyber 中的多项式乘法。随后 Fritzmann 等人[63]提出了一个增强型的 RISQ-V 架构，它不仅支持向量化模运算、NTT 计算和高效生成随机多项式，还增加了 29 条新指令以有效执行格密码学中的原子操作，以达到重用处理器资源并减少内存访问次数。Xin 等人[64]进一步提出了一种向量处理器 VPQC，实现了一个向量 NTT 单元以支持不同维度（从 64 到 2048）数论变换（NTT）的并行计算。此外，还设计了一个向量采样器，同时执行均匀采样和二项式采样。

上述这些工作主要集中在 Ring-LWE 上，而未能充分利用 Module-LWE 独特的矩阵结构，并且大多数基于 ISA 扩展的协同设计工作都属于轻量级实现。因此，Zhao 等人[65]引入了一种自定义矩阵扩展到 ISA，允许动态配置由一个自定义指令处理多项式，还提出了一套完整的模块设计和数据流组织方案进一步满足 PQC 算法的灵活性，同时还实现高计算性能。Nannipieri 等人[66]研究了 RISC-V 中 ISA 的扩展，探讨了性能和复杂度之间的权衡以便于实现 Dilithium

和 Kyber 中的 NTT 操作。Karl 等人[67]了 NTT 变换和逐点乘法以及用于 Dilithium 和 Falcon 的 SHAKE128 和 SHAKE256 函数，并支持 Dilithium 方案的所有参数集和 Falcon 的验证模块。Miteloudi 等人[68]提出了一个支持模数运算以及 NTT 蝴蝶操作的轻量级定制算术逻辑单元（ALU），还引入了十个新指令，来访问自定义 ALU 执行所必需的操作。López-Valdivieso 等人[69]提出了一个针对 SPHINCS+方案的模块化软硬协同 RISC-V 设计，主要集成了 Keccak-1600 和 Haraka 这两个哈希加速模块，支持不同安全等级下的实例。下表给出部分参考文献的实现性能以供参考。

表 2-3 后量子密码在 RISC-V 上实现性能

平台/文献	算法	时钟（kCCs）			面积×时间（kGE×ms）
		KeyGen	Encaps.	Decaps.	
Sapphire SoC[60]	Kyber-512	74.5	131.7	142.3	403.4
VexRiscv Core[62]	Kyber-512	118	181	253	-
RI5CY core[63]	Kyber-512	150.1	193.1	204.8	-
SCR1 core[64]	Kyber-512	18.6	45.9	80.0	410.8
Rocket Core[65]	Kyber-512	9.4	19.0	43.8	81.1
CVA6 SoC[66]	Kyber-512	419.6	438.2	100.8	-
数字签名					
平台/文献	算法	时钟（kCCs）			面积×时间（kGE×ms）
		KeyGen	Sign	Verify	
Sapphire SoC[60]	Dilithium2	167.4	634.8	229.5	403.4
Rocket Core[65]	Dilithium2	45.8	175.1	89.8	81.1
CVA6 SoC[66]	Dilithium2	1592.3	5884.3	1700.7	-
PULPino[67]	Dilithium2	593.4	1905.9	651.2	-
	Falcon-512	-	-	314.6	-
PULPino[68]	Dilithium2	479	782	511	-

（五）后量子密码技术实现与性能分析

1. PQC 与当前密码体系在数学基础上的差异

PQC 与当前密码算法的构建均基于特定的数学难题。其安全性则依赖于该数学难题的安全性。PQC 与当前密码体系具有不同的数学基础。数学基础上的差异使得 PQC 与传统密码在算力、存储、通信需求等方面存在较大差异。

表 2-4 现有公钥密码与 PQC 的数学难题差异

密码算法		类型	数学基础	传统计算机	量子计算机
传统密码	RSA	公钥密码	大质数分解难题	难以破解	可以破解
	ECC	公钥密码	椭圆曲线上的离散对数难题	难以破解	可以破解
PQC 算法	Kyber	公钥密码	格上的数学难题	难以破解	难以破解
	Dilithium	公钥密码	格上的数学难题	难以破解	难以破解
	Spingcs+	公钥密码	哈希难题	难以破解	难以破解

2. PQC 与传统密码算力需求差异

当前的主流传统密码方案包括 RSA、椭圆曲线密码学（Elliptic Curve Cryptography, ECC）等算法，这些算法的安全性通常基于大数分解或椭圆曲线离散对数问题。然而，随着量子计算的发展，这些传统密码可能面临被破解的风险，因此后量子密码方案应运而生。这些方案主要包括基于格密码、编码理论、哈希函数等的算法，如 Kyber、Dilithium、SPHINCS+、FALCON、Classic McEliece 等，旨在抵御量子计算的威胁，确保信息安全。为研究传统密码与 PQC 的算力需求差异，我们以 ECC 和 Kyber 为例进行对比分析，这两者分别代表了当前传统密码和后量子密码的典型方案。ECC 作为一种广泛应用的传统密码算法，以其较高的安全性和效率著称，但在面对量子计算时不再安全；而 Kyber 作为一种基于格理论的后量子密码方案，目前已被 NIST 标准化，设计初衷就是为了抵抗量子计算的威胁，同时保持与现有系统的兼容性和实用性。通过对比这两种算法，我们可以深入理解传统密码和后量子密码在安全性、效率和实现复杂度等方面的差异，帮助我们为未来的密码设计提供指导。

在实际应用中，椭圆曲线密码系统需要实现各种功能，如数字签名、公钥加密等。所有这些函数的主要组成部分是标量乘法，定义为

$KP = \sum_1^K P = P + P + \cdots + P$ ，其中 P 为椭圆曲线上的一个点，K 为随机整数。它由一系列点加（Point Addition，PA）和倍点（ Point Doubling，PD）计算得到，并进一步分解为一定数量的有限域运算。图 2-2 展示了创建 ECC 加密方案所需的算法集所遵循的层次结构，首先，选择使用的协议类型包括椭圆曲线迪菲-赫尔曼（Elliptic Curve Diffie-Hellman，ECDH）协议，椭圆曲线数字签名算法（Elliptic Curve Diffie-Hellman，ECDSA）协议，其次定义执行椭圆曲线点乘法（Elliptic Curve Point Multiplication，ECPM）的算法，然后定义执行有限域的算法。

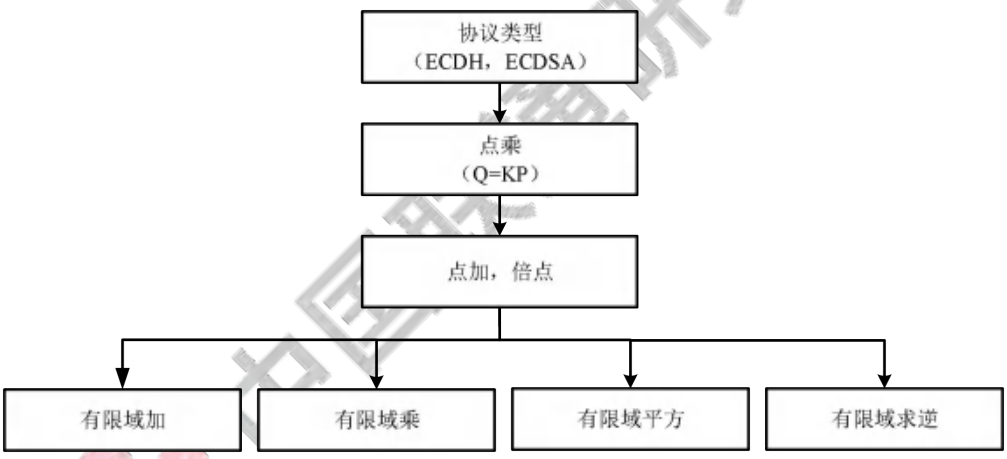

图 2-2 ECC 算法的操作层次结构

在 ECC 中方程的形式、点和运算公式会随坐标的不同而变化。由于模除是最复杂、最昂贵的有限域运算，通常所以通常会选择投影坐标、雅可比坐标、混合坐标或其他坐标来避免模除，对应的计算复杂度如表 2-5 所示，表中 M 代表模乘，I 代表模逆。

表 2-5 PA 和 PD 的计算成本[70]

	倍点	点加
Affine	1I, 4M	1I, 3M

Projective	10M	14M
Jacobi	8M	16M
Mixed Jacobi-Affine	--	11M

ECC 的安全性基于椭圆曲线离散对数问题，计算复杂度相对较低，主要体现在有限域的运算和点乘运算上。

后量子密码学（PQC）是为应对量子计算机可能带来的威胁而设计的密码体系，其中密钥封装机制（KEM）CRYSTALS-Kyber，又称 Kyber，是一个典型的代表。Kyber 是一种基于格的密码学（LBC）算法，其安全性建立在解决带错误的模块学习（Module - LWEs）问题的困难度假设上。模块格中的基本代数运算形式为 As + e，其中 s 和 e 为 k 维多项式向量，A 为 k×k 维多项式矩阵，其元素在多项式环 Rq 中。Kyber 的安全级别可以通过改变模块维度 k 来轻松调整，例如，Kyber512、Kyber768 和 Kyber1024 三个参数集的 k 分别为 2、3 和 4，分别相当于 NIST 的安全级别 1、3 和 5，同时，多项式乘法的参数集保持不变，具体的参数设置如表 2-6 所示。

表 2-6 Kyber 中的参数设置

参数	NIST-LEVEL	n（多项式的度数）	k（安全级别参数）	q（模数）
Kyber512	1	256	2	3329
Kyber768	3	256	3	3329
Kyber1024	5	256	4	3329

为了促进 Kyber 的实际应用，许多研究者致力于降低多项式乘法在硬件平台上的计算复杂度和延迟，数论变换（NTT）被广泛应用于 Kyber 优化多项式乘法的实现中，具有拟线性复杂性的优点。图 2-3 展示了 Kyber 算法的操作层次结构，其中，NTT 运算在整个 Kyber 算法中是一个关键的性能瓶颈，主要因为其计算复杂度较高，

实现难度大。因此，如何优化 NTT 运算的执行效率，成为提升 Kyber 算法整体性能的一个重要研究方向。

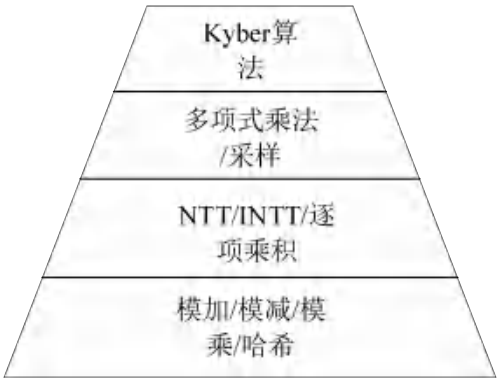

图 2-3　Kyber 算法的操作层次结构

以 Kyber512 为例，我们可以通过对 Kyber 计算流程的具体分析，统计出底层算子的数量，如表 2-7 所示。通过优化这些底层算子，尤其是 NTT 运算，可以显著提升 Kyber 的密钥生成、加密和解密的效率，从而使其在后量子时代成为一种更加实用和高效的加密方案。

表 2-7 Kyber 的计算成本

Kyber512	密钥生成	加密	解密
NTT/INTT 数量	2NTT	1NTT+2INTT	1NTT+1INTT
模乘总数	2944	4416	1920
模加/减总数	1793	2691	1922
哈希总数	10	14	3

由于 NTT 运算在 PQC 中是一个关键的性能瓶颈，为了实现高效的 NTT，需要在软件和硬件上进行大量的优化工作，[22]采用了一种新颖的 Barrett 约减技术和紧凑的模乘器，通过实现一种可重构的 Kyber 多项式乘法加速器来优化 NTT。表 2-8 中显示了我们在 FPGA

上实现模乘、模逆、PA、PD 模块的资源消耗和延时，同时评估了现有研究中点乘[71]和 NTT 模块[22, 24]的实现。

表 2-8 模乘、模逆、PA、PD、点乘和 NTT 模块的性能评估

		LUT	FF	DSP	BRAM	周期数	时钟频率/MHZ	总延时/ns
模逆	--	5025	2837	--	--	347	250	1388
模乘	--	12823	--	81	--	6	115	51.9
倍点（PD）	RAM	13613	--	81	15.5	55	--	475.75
	Register	30332	11995	162	0	34	--	294.1
点加（PA）	RAM	13823	--	81	15.5	66	--	564.96
	Register	30432	12105	162	0	49	--	423.85
点乘（ECPM）[71]	GF（2^{163}）	16345	4590	--	--	--	279	2930
	GF（2^{571}）	54470	13275	--	--	--	218	28800
NTT	低延迟设计[22]	4619	4166	16	8	84	273	310
	轻量化设计[24]	1005	599	2	0	448	227	1970

其中，模逆采用二进制的 EEA（Extended Euclidean Algorithm）算法，PA，PD 采用 Jacobian 坐标方案，并且评估了采用 RAM 和寄存器两种不同控制方案的性能，表 2-9 中所有工作均在 FPGA 上进行评估。由表中可以看出，NTT 的轻量化设计相比于 PA，PD 所消耗的 LUT 和 DSP 数量分别有明显降低，低延迟设计的延时相比于采用 RAM 控制的 PA，PD 也有所减少。优化后的 NTT 模块性能明显优于 ECC 中的底层 PA，PD 算法模块。

表 2-9 ECC core 和 Kyber 协议硬件实现

	Platform		LUT	FF	Slice	Time（ms）	Cycles（K Clock）	时钟频率/MHZ
ECC core[72]	Virtex-5	GF（2^{163}）	6959	7244	2475	0.0447	13	290.9
		GF（2^{571}）	22529	24808	7876	0.2181	49.5	227.06
	Virtex-7	GF（2^{163}）	6169	7176	2201	0.0405	13	320.8
Kyber-512 [24]	Artix-7	--	5500	3400	1500	0.0751	14.2	182

表 2-9 对比了[72]中所提出的基于 Lopez-Dahab 投影系统的 ECC 新架构和 Kyber 协议硬件实现的性能指标。从表中可以明显看出，在硬件资源方面，Kyber-512 在硬件资源占用（LUTs、FFs、Slices）方面明显优于 ECC，资源消耗较少，更适合在资源受限的硬

件平台上部署。在性能方面，Kyber-512 相比于 ECC（GF（2571））不仅在延时上表现更优（更快），而且所需的时钟周期数更少。整体来看 Kyber-512 在 FPGA 实现上比 ECC 更具优势，特别是在资源受限或需要高性能的应用场景中。故 Kyber 可能更适合用于现代嵌入式系统和物联网设备中。

总体而言，PQC 与传统密码学在算力需求上的差异主要体现在密钥大小和计算复杂度上。尽管 PQC 算法如 Kyber 在理论上复杂度较高，但通过优化底层算子和硬件支持，其性能在实际应用中可以与传统密码学算法相当，甚至更优。

3. PQC 与传统密码的通信与存储需求差异

表 2-10 PQC 与传统密码的密钥/密文大小差异

密码算法		私钥长度（byte）	公钥长度（byte）	签名/密文长度（byte）
传统密码	RSA-2048	256	256	256
	ECC-256	32	64	64
PQC 算法	Kyber-512	1632	800	768
	Dilithium	2528	1312	2420
	Spingcs+	64	32	7856

后量子密码的核心目标在于抵御未来量子计算机的攻击，这迫使其放弃传统密码学所依赖的整数分解和离散对数难题（如 RSA、ECC），转而采用基于格理论、哈希函数、编码理论或多变量方程等新型数学难题。这种数学基础的转变带来了一个不可避免的代价：为了实现同等级别的安全性，PQC 算法所需的密钥、签名、密文等数据结构的尺寸普遍远大于当前广泛使用的传统密码算法。这种尺寸上的膨胀，直接转化为通信带宽和存储空间需求的显著增加。

具体来看，公钥在 PQC 体系中的尺寸增长尤为明显。例如，传

统 ECC 算法（如 secp256r1）的公钥通常只需约 32 字节，而 NIST 选定的 PQC 标准算法如 CRYSTALS-Kyber 的公钥则达到 800 至 1500 字节，CRYSTALS-Dilithium 的公钥甚至达到 1300 至 2500 字节。这意味着 PQC 公钥比 ECC 公钥大出 30 到 80 倍，相比 RSA-2048 的约 256 字节公钥也大了 3 到 10 倍。这种增长源于支撑 PQC 安全性的数学结构需要更大的参数空间。

在加密通信中，用于密钥交换的密文尺寸的膨胀同样显著。传统非对称加密（如 RSA）的密文长度大致等同于其密钥长度（如 2048 位即 256 字节）。相比之下，PQC 的密钥封装机制（KEM）如 Kyber-768 产生的密文长度可达约 1000 字节，NTRU-HPS 的密文也在 700 到 1200 字节范围。这意味着 PQC 加密产生的密文比 AES 等对称加密大数十倍，也比 RSA 加密大 4 到 5 倍，显著增加了每次加密通信传输的数据量。

数字签名是另一个尺寸激增的关键领域。传统 ECDSA 签名非常紧凑，通常仅 64 字节，RSA-2048 签名约为 256 字节。而 PQC 签名算法的尺寸则大幅跃升：Dilithium-III 签名可达约 2500 字节，Falcon-1024 签名在 700 至 1300 字节之间，基于哈希的签名方案 SPHINCS+的签名甚至可能高达 10 到 50KB。因此，PQC 签名比 ECDSA 签名大 10 到 100 倍，比 RSA 签名也要大 5 到 10 倍。这直接影响了需要频繁进行签名操作的场景，如软件更新分发、文档签署和交易认证。

数字证书作为承载公钥和身份信息并由权威机构签名的核心信

任载体，其尺寸受到公钥和签名双重膨胀的叠加影响。传统 X.509 证书，若包含 ECC 公钥，大小通常在 500 到 800 字节，包含 RSA 公钥的证书约为 1 到 1.5KB。而一个包含 Dilithium 公钥（约 2.5KB）和 Dilithium 签名（约 2.5KB）的 PQC 证书，仅核心密码学元素就达 5KB 左右，加上其他标准字段（如主体、颁发者、有效期等），整个证书很容易膨胀到 10KB 甚至 50KB 级别。这意味着 PQC 证书的体积可能是传统 ECC 证书的 10 到 50 倍，是 RSA 证书的数倍到数十倍。

这种关键密码学元素尺寸的剧增对实际系统产生了深远的通信与存储影响。在通信层面，协议握手过程（如 TLS 1.3）需要交换证书和签名，PQC 带来的巨大数据量会显著增加单次握手所需传输的字节数（可能增加 10-100KB），在高延迟网络（如卫星链路）中导致握手时间明显延长。对于带宽极其受限的物联网设备或低功耗广域网，传输如此庞大的证书或签名可能超出其能力范围，导致连接失败或耗尽电池。此外，大尺寸数据包可能超过网络的最大传输单元限制，需要额外的分片处理，增加了复杂性和开销。在存储层面，终端设备（如浏览器、操作系统）需要存储信任锚（根证书库），PQC 根证书库的集体膨胀可能使其从 MB 级跃升至 GB 级，占用大量宝贵资源。对存储空间通常只有 KB 级别的嵌入式设备（如智能卡、传感器）而言，存储单个 PQC 密钥或证书都可能变得极其困难甚至不可能。对于服务器端和证书颁发机构，存储海量用户证书（如在企业邮件加密系统或 PKI 中）的数据库需要扩容数十倍，显著增加了硬件成

本和维护负担。内容分发网络缓存大尺寸证书的效率也会降低，增加回源流量。

综上所述，后量子密码算法在提供抵御量子攻击能力的同时，其公钥、密文、签名和证书等元素的尺寸相比传统密码算法呈现数量级上的增长。这种增长是支撑其安全性的数学基础所决定的必然代价。它直接转化为对通信带宽的更高要求和存储资源的更大消耗，尤其对资源受限环境、高频次握手协议和大规模证书管理系统构成了严峻挑战。应对这一挑战需要算法层面的持续优化（如选择更紧凑的 PQC 方案）、协议层面的改进（如证书压缩、会话重用）以及硬件层面的升级（如扩展安全模块存储）。认识到并妥善处理这些显著增大的通信与存储需求，是成功向后量子密码时代迁移的关键环节之一。

三、后量子密码标准与政策

（一）后量子密码算法的标准发展

后量子密码的标准化进程正在全球范围内迅速推进，随着量子计算机对传统加密技术的潜在威胁逐渐成为现实，世界各国和组织纷纷加紧布局，以确保未来的数字安全。

1. 美国的标准化进程

量子计算机能够利用其强大的并行计算能力破解传统计算机无法在合理时间内解决的复杂数学问题，从而威胁到现代加密系统的安全性。为应对此种威胁，美国国家标准与技术研究所（National Institute of Standards and Technology，NIST）自 2015 年起启动了后量子密码的算法筛选和标准化工作。这项工作旨在开发和推广能够抵御量子计算攻击的密码算法，以保障电子通信和数据交换的安全性。

（1）初步启动阶段（2015-2017 年）

2015 年，NIST 发起了全球性的后量子密码学项目，旨在通过公开征集和评估新的加密算法，寻找能够抵御量子计算威胁的解决方案。全球超过 25 个国家的研究机构和企业提交了 82 种候选算法，涵盖了不同的数学问题和密码设计。

NIST 还组织了多个国际研讨会和技术交流会议，旨在集结全球密码学专家的力量，共同推动这一领域的进展。研究人员对这些候选算法进行了深入的理论分析和实用评估，筛选出在安全性、性能、资

源消耗等方面具有优越表现的算法。

（2） 筛选与测试阶段（2017-2022 年）

在候选算法提交后，NIST 与全球的密码学专家密切合作，对这些算法进行了系统的测试和评估。这一过程涉及到密码学家们对每一种算法的安全性和性能进行深入的数学分析和计算机模拟测试，以确保其在量子计算威胁下的抗攻击能力。

2017 年，NIST 启动了第一轮算法评估，直至 2022 年，经过了三轮严格评估，将 82 种候选算法缩减为 15 种算法。评估工作不仅考察了这些算法在抵御量子计算攻击方面的潜力，还考虑了它们在计算效率、资源消耗、易用性等方面的表现。这些算法被分为两类：入围算法和备选算法，并进入进一步的深入分析阶段。

（3） 标准草案的发布与验证阶段（2022-2023 年）

2022 年，NIST 宣布选定四种后量子密码算法，包括用于公钥加密的 CRYSTALS-Kyber 算法和用于数字签名的 CRYSTALS-Dilithium、Sphincs+以及 FALCON 算法。这四种算法代表了后量子密码学领域的最前沿，基于不同的数学基础和密码设计理念。

NIST 在 2023 年发布了基于这四个算法的 FIPS 系列标准草案版本，并鼓励网络安全从业者开始在其系统中采用这些新标准。NIST 标准不仅涵盖了这些算法的具体实现，还包括了如何在不同应用场景中部署和使用这些算法的详细指导。

- FIPS 203：基于 CRYSTALS-Kyber 算法，旨在作为通用加

密的主要标准。其优点在于加密密钥相对较小，方便双方交换且具有较快的运行速度。

- FIPS 204：基于 CRYSTALS-Dilithium 算法，旨在作为数字签名的主要标准。
- FIPS 205：基于 Sphincs+算法，提供无状态的哈希签名方式，作为 CRYSTALS-Dilithium 的备选方案。
- FIPS 206：基于 FALCON 算法，该算法采用 NTRU 晶格基础，并计划于 2024 年发布为标准草案。

（4） 正式发布标准（2024 年 8 月）

2024 年 8 月 13 日，NIST 正式发布了首批三项后量子密码学（PQC）标准，进一步为全球网络安全设定了新的基准。这三项新标准分别是：

- FIPS 203：基于模块格的密钥封装机制标准。
- FIPS 204：基于模块格的数字签名标准。
- FIPS 205：基于无状态哈希的数字签名标准。

这些标准草案规定了用于密钥建立和数字签名的具体算法，旨在抵御量子计算机对当前加密标准的安全性威胁。NIST 强烈建议全球范围内的系统管理员开始向这些新标准过渡，以确保未来网络安全的稳固性。这一发布标志着 NIST 在后量子密码标准化工作中的一个重要里程碑。

（5）未来发展与补充标准

尽管 NIST 已经选定了前三种主要算法，但其标准化工作并未结

束。于 2025 年初，NIST 在三种基于编码的候选方案里面选择了 HQC 进入到最终名单。此外，NIST 也在评估另一组为数字签名设计的算法，并计划对 15 种候选算法进行进一步测试与分析。

NIST 强调，当前已发布的标准应被优先采用，各系统管理员应立即着手集成这些算法。与此同时，NIST 将继续制定备份计划，以确保未来有能力应对新出现的威胁。

NIST 的后量子密码标准化项目标志着全球密码学领域的一次重要变革。这些新标准不仅为未来量子计算环境下的安全提供了基础保障，还为全球范围内的加密系统升级提供了明确方向。通过与国际密码学界的紧密合作，NIST 确保其标准在全球范围内具有高度的兼容性和适用性。

作为全球标准的制定者，NIST 的后量子密码标准化进程对于全球信息安全的发展具有深远的影响。未来，随着量子计算技术的不断进步，后量子密码学将成为保护数字社会安全的核心技术之一。

2. 欧盟的标准化进程

欧盟在后量子密码标准化的推动过程中，采用了一种开放的态度，既尊重国际标准化机构的成果，同时也致力于自主探索适合欧洲需求的密码方案。与美国 NIST 通过明确的标准化流程直接制定后量子密码标准不同，欧盟并没有设立单独的 PQC 标准化计划，而是结合其内部需求，借鉴并评估 NIST 的候选标准和其他潜在的方案。

（1）欧盟的后量子密码战略框架

欧盟通过其“地平线 2020”项目积极参与全球后量子密码学的

研究，并且与美国 NIST 的 PQC 标准化工作形成了良好的互动关系。地平线 2020 项目作为欧盟的主要科研创新计划，支持多个密码学研究项目，涵盖了量子密码学、后量子密码学和与网络安全相关的其他领域。这些研究成果为欧盟在后量子时代应对全球网络安全威胁奠定了坚实的基础。

虽然欧盟尚未发布独立的后量子密码标准，但欧盟各国通过不同的国家机构和技术委员会积极参与了 NIST 的后量子密码标准化过程。事实上，NIST 选定的第一批四个标准算法中，其主要提交人均来自欧洲，这表明欧洲在全球后量子密码学领域占据了重要地位。

（2） 欧盟主要国家的后量子密码策略

欧盟各成员国在后量子密码标准化方面的策略存在一定差异，且各国的监管机构也有着不同的技术偏好和应用实践。以德国、法国和荷兰为例：

- 德国：德国联邦信息安全办公室（BSI）在其发布的后量子密码白皮书中，强调了基于安全性而非性能的算法选择原则。BSI 推荐使用基于无结构格的加密方案 FrodoKEM 和基于编码的加密方案 Classic McEliece。尽管这两个算法在 NIST 的标准化项目中并未进入最终标准，其中 FrodoKEM 已被淘汰，而 Classic McEliece 仍处于备选阶段，德国仍然信任这两种算法，认为它们适用于需要长期保密的高安全性场景。BSI 在其技术规范（BSITR-02102-1）中推荐了这些算法，特别是在与 ISO 的合作标准化（PWI19541）过程中，BSI

曾试图推动 FrodoKEM 和 Classic McEliece 的标准化工作，尽管目前这些努力暂时中断。

- 法国：法国国家信息系统安全局（ANSSI）在后量子密码的选型上表现出更加灵活的态度。ANSSI 明确表示，将严格遵循 NIST-PQC 流程的结果，但也认识到其他算法的潜在价值。因此，ANSSI 并不打算将其推荐的后量子密码算法仅限于 NIST 获胜者，并可能考虑其他替代方案。ANSSI 的这种开放态度表明，法国在后量子密码标准化过程中注重多样性，并希望在未来保持技术选择的灵活性。
- 荷兰：荷兰内政王国关系部情报安全总局（AIVD）也发布了自己的后量子密码白皮书。在推荐算法上，AIVD 侧重于数字签名的安全性，推荐使用无状态数字签名方案 SPHINCS-256，以及有状态数字签名方案 XMSS。这种选择反映了荷兰对在量子计算威胁下的签名技术的关注，特别是在保护数字身份和认证方面。

（3）欧洲对 NIST 标准的借鉴与发展

尽管欧洲没有制定独立的 PQC 标准化流程，但其通过不同的国家监管机构和标准化组织，参考并借鉴了 NIST 的标准评估结果。例如，德国、法国和荷兰等国家在各自的技术规范中，或多或少都表明会将 NIST 的 PQC 标准作为主要参考依据。这一合作态势不仅促进了跨大西洋的网络安全合作，还为未来全球密码学标准的兼容性打下了基础。

然而，欧盟也意识到，后量子密码学的发展不仅仅局限于 NIST 的标准化流程。不同的应用场景和安全需求，特别是在政府、军方和关键基础设施中，可能需要更加多样化的密码解决方案。因此，欧洲各国在评估 NIST 标准的同时，也在探讨其他可能的候选算法，以应对不同的安全挑战。

随着量子计算技术的逐步成熟，欧洲在后量子密码标准化方面的战略预计将更加明晰。欧盟作为一个整体，可能会在未来的网络安全策略中加强对后量子密码的统筹管理，并通过与国际标准化机构的合作，制定出更加完善的技术框架。同时，欧洲各国将继续保持开放的技术选择态度，确保在未来的量子计算环境中，能够灵活应对各类安全威胁。

总的来说，欧洲在后量子密码标准化进程中扮演着至关重要的角色，其策略既有对 NIST 标准的借鉴，也有对自主创新的坚持。这种平衡策略将确保欧洲在未来的量子安全时代中占据有利地位，同时促进全球后量子密码学标准的进一步融合。

3. 我国的标准化进程

中国在后量子密码标准化方面的探索虽然起步较晚，但近年来已经取得了显著的进展。中国的后量子密码标准化工作由多个机构协同推进，涵盖了从算法设计竞赛到前瞻性研究布局的多个方面。以下将从历史背景、标准化进程及未来展望三个方面阐述中国后量子密码的标准化发展路径：

（1）历史背景：算法设计竞赛与遴选

中国在后量子密码领域的标准化准备工作始于 2018 年。当年 6 月，中国密码学会（Chinese Association for Cryptologic Research，CACR）启动了全面密钥算法设计竞赛，旨在推动国内研究人员积极参与后量子密码算法的设计和开发。该竞赛历时一年半，吸引了国内众多研究机构和学术单位的参与，并于 2019 年 12 月遴选出了 14 个后量子公钥密码算法。

这些算法涵盖了多种基于不同数学难题的后量子密码技术路线，包括基于格、基于编码、基于多变量、基于等价函数和基于椭圆曲线同源问题的密码技术。这些技术路线在国际后量子密码学研究中也具有重要地位。中国的研究人员通过这一算法竞赛，积累了丰富的研究成果，并为后续的标准化进程奠定了基础。

（2） 标准化进程：前瞻性研究与技术立项

尽管中国尚未正式启动后量子密码标准算法的公开征集工作，但相关的研究和规划已取得实质性进展。2023 年，国家标准化管理委员会发布的《2023 年全国标准化工作要点》明确提出要开展后量子密码标准的前瞻性研究和规划布局。这一政策指引表明，中国政府已经意识到后量子密码技术在保障国家信息安全中的战略意义，并计划通过标准化工作为未来的量子计算威胁做好准备。

2024 年初，来自密码行业标准化技术委员会的前沿研究透露，中国已经开始针对部分后量子密码方案进行技术立项。这表明，在基础算法的开发和评估之后，标准化的准备工作已经进入了技术选型和

规范制定阶段。通过立项过程，中国可能会进一步筛选出具有高安全性和广泛适用性的后量子密码算法，并逐步推向标准化。

（3） 中国后量子密码学研究的多样性与国际互动

中国的后量子密码学研究涵盖了多种密码技术路线，从基于格的加密到基于编码的加密，再到基于多变量的加密。尤其是在格密码和多变量密码方面，中国的研究机构已经取得了诸多创新性成果。例如，基于格的算法由于其在抵御量子攻击方面的高效性和安全性，已经成为中国后量子密码研究的重点方向之一。

中国在后量子密码领域也与国际社会保持互动。在 NIST 发起的全球后量子密码标准化过程中，中国的研究人员提交了多个候选算法，并参与了国际学术会议和密码算法评估工作。通过这些国际合作，中国在全球后量子密码研究中占据了一席之地，并为国内标准的制定提供了宝贵的参考。

（二）世界各国的 PQC 迁移进展

量子危机逐渐逼近的当下，国内外研究机构和学者们正在推进密码算法和安全协议的标准化进程，以应对量子计算带来的威胁。同时，各国逐步开始针对后量子密码迁移发布指导意见。此外，芯片、终端、通信、数据中心等领域也对后量子迁移展开部署计划。本小节将介绍国内外后量子密码迁移研究进展。

表 3-1 各国的 PQC 迁移进展

国家	纳入考虑的 PQC 算法	已发布的指导文件	简略时间表
澳大利亚	NIST	CTPCO（2023）	开始规划; 2025-2026 年早期实施
加拿大	NIST	Cyber Centre（2021）	开始规划; 2025 开始实施
中国	中国特定	CACR（2020）	开始规划

欧盟委员会	NIST	ENISA（2022）	开始规划和放缓
法国	NIST（但不限于）	ANSSI（2022, 2023）	开始规划；2024 年开始迁移
德国	NIST（但不限于）	BSI（2022）	开始规划
日本	参考 NIST	CRYPTREC	开始规划；初步时间表
荷兰	AES,参考 NIST、SPHINCS-256、XMSS	NCSC（2023）	带有时间表的行动计划草案
新西兰	NIST	NZISM（2022）	开始规划
新加坡	参考 NIST	MCI（2022）	无时间节点
韩国	KpqC	MSIT（2022）	2022-2023 第一轮算法筛选
英国	NIST	NCSC（2023）	开始规划; 2024 开始实施
美国	NIST	CISA（2021，2022，2023） NIST（2023） NSA（2022，2023） White House（2022）	2023-2033 实施
捷克共和国	NIST 算法（不限于此）	NÚKIB-2023	2027 年前完成迁移（密钥协商、加密）；尽快实施固件/软件签名
以色列	（未明确）	IL-2022, IL-2025	开始规划，建立密码资产清单；合同中纳入 PQC 要求；金融机构需管理量子风险并制定计划
意大利	NIST 算法	IT-2024	（未明确）
西班牙	NIST 算法及 FrodoKEM	CCN.ES-2022	四阶段推进（当前至 2030 年后）
印度	NIST	IT-2024	无时间节点
瑞士	NIST + QKD 融合架构	瑞士量子中心《混合密钥分发协议》（2024）	金融交易试点中（2024 年启动）
巴西	NIST 算法为主	国家电信局《5G 量子安全要求》（2025） 《数字盾牌计划》	5G 网络部署 ML-KEM-768（2026）
俄罗斯	GOST 标准 + 抗量子扩展	量子安全国标草案（GOST R 2025）	能源/军工系统优先迁移（2027）

1. 国际后量子密码迁移研究

在后量子密码领域，相较于我国，欧美等国家无论是迁移方案准备还是后量子密码领域研究成果均走在发展的前列。随着 PQC 标准初具雏形，各国先后提出后量子迁移规划及指南，同时在 PQC 产业化方面也加快推进，抢占先机。2022 年 5 月，拜登政府发布行政令，提出在 2035 年前，由国家安全局（NSA）和 NIST 负责及时完成美国国家信息系统的 PQC 升级迁移，为应用推广扣响了“发令枪”。2023 年 1 月，互联网工程任务组（IETF）成立后量子应用协议工作组（PQUIP），开始从加密技术标准和网络协议升级等方面开展研究与推动。10 月，PQUIP 发布《面向工程师的后量子密码》报，分析 PQC 标准算法特性、过渡时间表、算法替换升级方案等具体技术问题。7 月，NIST 联合国家网络安全卓越中心（NCCoE）发起“向 PQC 迁移”计划，提出升级项目工作流程，推荐 28 家 PQC 技术产

品供应商，包含 IBM、亚马逊、思科等科技巨头和 SandboxAQ、PQShield 等初创企业。8 月，美国网络安全与基础设施安全局（CISA）、NSA 和 NIST 三部门联合发布为《量子准备：迁移到后量子密码学》文件，为机构和企业开展 PQC 升级应用，提出制定升级路线图、编制密码清单、测试验证 PQC 技术产品等指导意见。9 月，IBM、微软、MITRE、PQShield、SandboxAQ 和滑铁卢大学成立 PQC 联盟，推动 PQC 迁移标准研究，创建技术材料，组织测试验证等活动。PQC 算法标准的推出，拉开了全球 PQC 技术产业化序幕。除此之外，自 NIST 提出关于后量子标准化进程以来，欧美各高校在后量子密码芯片领域表现也比较亮眼，美国麻省理工学院研究团队于 2019 年首次提出一种用于量子安全物联网的节能可配置格密码处理器，并完成 40nm 流片及测试。该处理器通过架构优化实现了高达 2 个数量级的功耗降低 124K 门电路的减少，可以支持 NIST 后量子标准化过程的第一轮中的多个基于格的后量子密码算法。普渡大学 Ghosh 团队采用优化的紧凑 Toom-Cook 乘法器完成多项式运算，实现更低的资源开下。基于交互式指令集的架构重用构建减少了面积开销，并使其与在 SoC 中运行的处理器兼容。耶鲁大学 Mohan 等人将后量子密码数字签名方案 XMSS（与 SPHINCS+算法同源）在 28nm 下进行 ASIC 实现，通过新型流水线 XMSS Leaf 结构加速算法中计算最密集的步骤。澳大利亚团队 Aikata 等通过设计兼容不同位宽多项式乘法器与高效存储管理机制，结合快速哈希伪随机数生成器，实现首 Kyber 和 Dilithium 结合的硬件设计，能够在 28nm ASIC 评估中达

到 2GHz 时钟频率。

2. 我国的后量子密码迁移研究与进展

面对欧美等国家在后量子密码（PQC）领域起步早、推进快的局面，我国亟需加快相关算法研究、评估与标准化进程，推进技术产品研发和应用部署，培育具有国际竞争力的领军企业，力争在量子时代的信息安全竞争中占据一席之地，构建自主可控的信息安全保障体系。

2019 年，中国密码学会组织发起“全国密码算法设计竞赛”，共有 22 个分组算法、38 个公钥算法参与评选。最终，Aigis-sig（数字签名方案）、LAC-PKE（密钥封装方案）、Aigis-enc（密钥封装方案）三种算法获得竞赛的一等奖。

表 3-2 2019 年全国密码算法设计竞赛获奖算法汇总表

	算法	功能	安全问题
一等奖	Aigis-sig	数字签名	MLWE
	LAC.PKE	公钥加密/密钥封装	RLWE
	Aigis-enc	公钥加密/密钥封装	MLWE
二等奖	Scloud	公钥加密/密钥封装	LWE
	LAC.KEX	密钥交换	RLWE
	SIAKE	密钥交换	超奇异同源
	AKCN	公钥加密/密钥封装	MLWE
三等奖	OKCN、Fatseal、木兰、AKCN-E8、TALE、PKP-DSS、Piglet-I		

由表 3-2 可见，国内提出 PQC 算法大多也是基于格问题构造的，其中最为主流的方案 Aigis-enc 和 Aigis-sig 分别在原有 Crystals-Kyber 和 Crystals-Dilithium 方案的框架上进行了改良，充分利用非对称模块 LWE（AMLWE）的困难度，并仔细选择参数，在计算成本、存储开销和安全性之间获得了更好的折衷，具有更短的公钥和密文/签名，相较 NIST 标准有所领先，有望在未来成为国产标准化算法。

此外，基于无结构的 LWE 问题构造的 Scloud 方案因其在安

全性上更有保障（能够避免利用代数结构的攻击方法）而备受关注，Scloud+在其基础上利用格编码技术和三元秘密分布来提升计算和通信性能，在同技术路线下性能最优，与国际同类型算法 FrodoKEM 相比，在效率及尺寸方面取得了显著改进。但和传统非结构算法相比，运算效率低，公私钥、密文长度大仍是其瓶颈所在。Tian 等人[73]充分利用参数特点和三元计算优势，首次提出了高效的硬件加速方案，极大改善了 Scloud+的效率低下问题，为解决其性能瓶颈问题提供了有效路径，有望推动 Scloud+算法纳入国产密码标准化体系。

2023 年 4 月，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》报告中提出，应尽快在国家层面统筹开展为期 10—15 年的后量子密码研发与迁移计划。2023 年 11 月，中国信通院发布的《后量子密码应用研究报告》进一步指出，迁移工作应尽早启动，并系统研究了行业迁移策略、迁移时间预测及面临的主要挑战。

在通信及终端应用领域，中国电信安全公司联合北京大学、中国科学院大学、数盾科技等单位，开展了基于后量子密码的产品研发。在其“密评助手”密码服务管理平台上，已完成多个基于 Kyber 算法的密码运算接口适配。2024 年 5 月，该公司发布的新一代安全网关设备集成了后量子密码硬件卡，融合国产 LMS/HSS-SM3 签名算法，并支持 Kyber 与 Dilithium 等国际标准算法，实现了安全密钥协商与端到端身份认证，可灵活切换加密方案，应对量子计算可能带来的安全威胁。

在隐私计算与数字中心等领域，2023 年 11 月发布的《中国电信后量子隐私计算白皮书》提出，通用安全多方计算（MPC）、隐私集合求交（PSI）、隐匿查询（PIR）、联邦学习（FL）等核心隐私计算协议需通过后量子安全算法加以改造。白皮书还介绍了“密流量子盾”平台系统，该平台融合后量子密码算法与隐私增强技术，面向量子计算引发的新型攻击威胁，提供兼容传统与量子计算安全需求的算法迁移方案。

在芯片层面，清华大学与华中科技大学在后量子密码硬件实现方面进展显著。清华大学于 2022 年在 28nm 工艺下完成了 Kyber 与 Dilithium 的 ASIC 实现，兼顾低延迟、高吞吐与低功耗。华中科技大学团队则基于动态可重构算术单元与高性能 NTT 加速器，提出了基于 Kyber 的协处理器架构，支持最新国际算法标准，并在综合性能、功耗和芯片面积之间实现优化平衡。

2025 年 2 月 5 日，我国商用密码标准研究院正式启动新一代密码算法征集，标志着我国后量子密码迁移工作全面启动。结合美国 NIST 的标准化经验，通信系统等关键基础设施将成为我国迁移工作的重点方向。

在工业界，后量子密码的融合应用也在加速推进。当前主要集中在终端侧的集成应用。国内方面，武汉二进制半导体与东风汽车合作，在车载 ECU 中集成了 XMSS 签名算法加速器，为汽车通信系统提供抗量子能力[74]。

在光通信领域，由于后量子密码在签名长度、计算资源等方面的

特殊要求，迁移难度更高。美国 Cisco、德国 ADVA 及微软等企业已推出支持 PQC 的交换机、OTN 和高速 VPN 设备，推动示范应用。国内相关工作仍处于起步阶段。中国联通研究院与武汉二进制半导体合作，尝试在光接入设备上引入后量子密码探索在光通信种的应用可行性[75]。

总体来看，随着量子计算技术的发展，信息产业对量子安全升级的需求日益迫切。当前亟需加强后量子密码在算法、协议、电路和系统各层级的协同研发，构建完整、自主可控的后量子密码技术体系，助力科技成果转化与产业应用落地，夯实我国在量子安全时代的信息基础设施安全防线。

综上所述，向后量子密码的过度是一个艰巨的任务，制定完善的后量子密码迁移计划变得尤为重要。该计划的总体目标是确保所有应用中使用的密码算法能够抵抗后量子计算攻击。这一计划是综合性的，涵盖了从评估现有密码体系的脆弱性到实施后量子算法替代方案的整个过程。计划的成功依赖于政 府、学术界和工业界之间的协同合作，以确保系统的高效和安全迁移。

四、后量子密码的产业化应用

对称加密算法（如 AES）和哈希算法（如 SHA-2）在量子计算威胁面前仍相对安全。虽然增加密钥长度曾被普遍认为能有效抵御量子攻击，但即使是 AES-128，在可预见的未来也难以通过 Grover 算法被实际破解。相比之下，非对称加密体系（包括 RSA、ECDSA、

ECDH 等算法）及其衍生的数字签名机制则面临量子计算机的根本性威胁。其中，“现在收集，稍后解密”（Harvest Now, Decrypt Later）攻击是当前对现有密码体系的最大威胁。

（一）PQC 在应用端的融合应用

1. 浏览器生态

在 NIST 正式发布 ML-KEM （FIPS 203） 标准之前，业界广泛采用实验性混合协议 X25519Kyber768。该协议曾部署于 Google Chrome 及 Mozilla Firefox。标准化进程触发浏览器快速迁移：

Firefox 在 132.0 版本（2024 年 10 月 29 日）率先集成 X25519MLKEM768。Firefox:通过设置“security.tls.enable_kyber”（名称虽为 Kyber，但现启用的是 X25519MLKEM768）。

紧随其后于 Chrome 131 稳定版（2024 年 11 月 6 日）完成切换。Chrome/Chromium 通“chrome://flags/ #enable-tls13-kyber”和“chrome:// flags/ #use-ml-kem”（此标志选择 X25519MLKEM768）共同启用。

对于已启动 PQC 迁移的机构，需将 “X25519Kyber768”升级至 “X25519MLKEM768”。尽管核心算法（Kyber/ML-KEM）未变，但标准化带来的参数调整与接口更新仍需开发适配，其迭代速度超出业界预期。

2. 应用程序对 PQC 的支持

Zoom 率先推出基于 Kyber 768 （ML-KEM） 的量子安全端到端加密 （E2EE），覆盖 Zoom Meetings，计划扩展至 Zoom Phone/Rooms。

Meta 在内部服务通信中部署 PQC，并为 Facebook/Instagram/WhatsApp 等平台的 TLS 连接构建量子安全防护体系，核心聚焦用户数据的前瞻性保护。

3. 融合 PQC 的开源密码库

Open Quantum Safe （OQS）：率先提供混合算法 X25519MLKEM768 及纯后量子算法的完整支持。

BoringSSL: 支持 X25519MLKEM768。该库被 Google 服务/Chrome 以及 Cloudflare 使用。这意味着 Google 云平台（GCP）具备 PQC 能力，但在具体组件（如 Google Cloud 负载均衡器）上的启用指南尚不明确。

WolfSSL（轻量级）：于 2024 年 10 月实现对纯后量子算法 ML-KEM 和 ML-DSA 的支持。其混合算法兼容性存疑——官方文档虽提及“Kyber 混合组”，但未明确标注 X25519MLKEM768 支持状态及文档更新时间。

OpenSSL （行业标准）：进展相对滞后，2024 年 9 月宣布基于 OQS-provider 集成 PQC 的计划。2025 年 1 月发布《ML-KEM/ML-DSA 私钥格式技术白皮书》。目前仍处于 IETF 标准讨论阶段，原生支持时间表未定。

Microsoft SymCrypt: 2024 年 9 月实现混合与纯 PQC 算法支持，同年 12 月扩展支持 LMS 签名及 ML-DSA。Azure 平台已通过密码 API （CNG） 开放能力，但负载均衡器等组件的启用细则未公开。

AWS Libcrypto: 于 2024 年 12 月宣布在 FIPS 140-3 验证模式下支持 ML-KEM 密钥封装及 s2n-tls 中的混合密钥交换。

PQMagic（国产首款 FIPS 全支持库）： 由郁昱教授团队（上海交通大学、上海期智研究院）主导开发与维护，聚焦自主可控与高性能实，性能达 liboqs 2 倍，深度国密改造，高性能优化版需定制，支持算法模块化配置(如仅启用 Aigis-Enc 模式 1 或混合 ML-DSA)，适配不同安全场景需求要求，生态扩展中。

4. 融合 PQC 的开发语言生态

OpenJDK （Java）：2025 年 2 月完成 ML-KEM 与 ML-DSA 的技术提案闭环，预计 Java 24（2025 年 3 月发布）将搭载纯后量子算法，混合方案暂未纳入路线图。

Go 语言: 展现出快速迭代特性：Go 1.23 （2024 年 8 月）：支持草案协议 X25519Kyber768。Go 1.24 （2025 年初）：正式集成标准算法包 “crypto/mlkem” （ML-KEM-768/1024），并默认启用 X25519MLKEM768 混合协议。

底层密码库已初步构建 PQC 能力矩阵,而云计算平台的商业化集成进程相对滞后。企业实施路径需兼顾密码库版本选择与云服务适配度，建议优先评估 BoringSSL、AWS Libcrypto 及 Go 语言等

成熟技术栈，同时密切关注 OpenSSL 标准化进程及云平台产品指南更新。

5. 操作系统层面对 PQC 的支持

Microsoft Windows: Insider 预览版已在下一代密码 API（CNG）中支持 ML-KEM（封装）与 ML-DSA（签名），支持构建混合方案。正推进 PQC 证书链研发，计划扩展至 Windows TLS 协议栈（Schannel）及 Active Directory 证书服务（ADCS）。

Linux 生态系统: Red Hat Enterprise Linux 10.0 率先集成 NIST PQC 算法，通过 OpenSSL/GnuTLS/NSS 库实现 ML-KEM TLS。启用“TEST-PQ”策略模块可激活 X25519MLKEM768, SecP256r1MLKEM768 等混合协议。Fedora Linux（技术试验场）基于 liboqs 与 OpenSSL oqsprovider 实现 PQC 支持。Rawhide 版本已预置 ML-DSA/ML-KEM 算法及 Kyber 混合方案，通过全系统加密策略统一配置。Ubuntu 依托 OpenSSL 3.5+ 实现 PQC 能力。安全厂商正为 LTS 版本（如 22.04）提供合规方案。Linux 基金会 PQCA 加速全生态 PQC 技术整合。

（二）网络安全产业对于 PQC 的应用

下一代防火墙（NGFW）如 PAN-OS 11.1+ 可检测 PQC SSL 会话并实现全面可视化，价值在于：（1）识别启用 PQC/混合 PQC 的应用与连接；（2）深度解析 TLS“ClientHello”中的“supported_groups”扩展；（3）基于威胁特征库比对已知

PQC 算法，实现检测、记录及拦截。

Palo Alto Networks 率先实现量子安全 VPN，严格遵循 IETF 标准 （RFC 8784, RFC 9242, RFC 9370）。

1. “云”端的后量子密码应用

服务提供商实施 PQC 需通信双方协议兼容,这要求企业依赖第三方密码库或自研方案，导致当前应用格局分化显著:

Cloudflare: 已率先在其边缘网络部署 X25519MLKEM768 协议，涵盖客户端至边缘节点（33% 流量采用率）及边缘节点至源站的双向通道。但免费服务与企业级产品的协议启用范围、以及是否实现客户端至源站的全链路 PQC 加密尚未明确披露。Cloudflare 给出了 2025 年 6 月 13 日至 2025 年 7 月 7 日基于 PQC 的 HTTP 连接比例，达到了 37%。

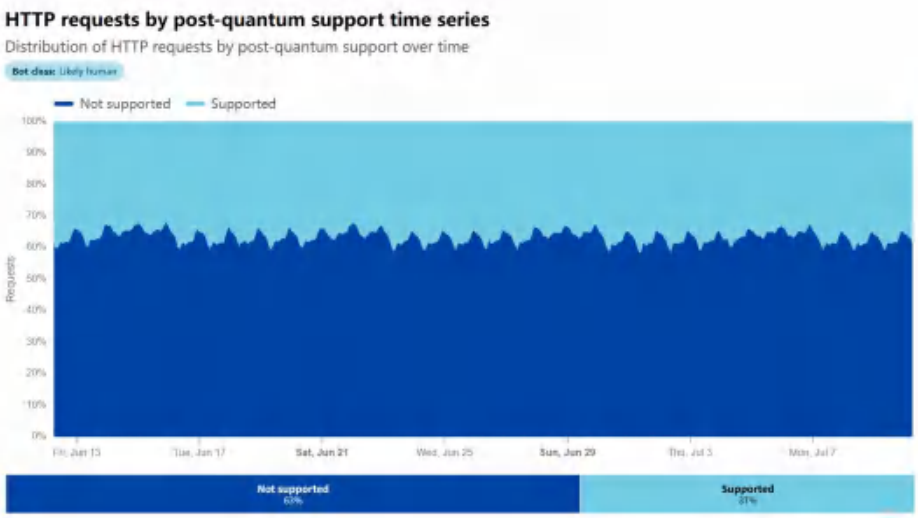

图 4-1 2025 年 6 月 13 日至 2025 年 7 月 7 日基于 PQC 的 HTTP 连接比例（浅色部分）

F5: 2024 年 11 月起，通过使用 OQS 在 F5 NGINX Plus R33 中支持 PQC。2024 年 10 月 30 日宣布在 BIG-IP Next

20.3 中支持 X25519Kyber768Draft00。业界对其未直接采用标准化方案 X25519MLKEM768 持保留态度。

Meta/Facebook: 2024 年 5 月公布 PQC 技术路线图，底层基于 OQS。2024 年 11 月，开源密码库 Fizz 集成 X25519MLKEM768 协议，并发起非标方案 X25519MLKEM512_FB（因 IANA 未分配代码点）。尽管技术储备就绪，Meta 尚未在其公网服务中启用 PQC 加密机制。

Akamai: 在 NIST 标准发布前夕提出边缘至源站的 PQC 部署计划，然实际进程已滞后于初始规划。

2. 抗量子密码芯片

在后量子计算时代来临之际，全球芯片厂商纷纷推出硬件级后量子密码（PQC）解决方案，构建量子威胁防御的核心技术壁垒。以下为四款代表性芯片的技术特性与应用布局：

（1）三星 S3SSE2A：移动终端量子安全的主动防御标杆

三星电子于 2025 年 2 月推出的 S3SSE2A，作为业界首款硬件级后量子密码芯片，专为移动设备打造，旨在抵御量子计算对关键数据的潜在威胁。该芯片通过硬件加速与独立安全架构实现技术突破：后量子密码运算速度较纯软件方案提升 17 倍，同时采用与应用处理器（AP）物理隔离的设计——敏感数据全程在芯片内部处理，仅输出最终结果，大幅降低信息泄露风险。其核心技术集成 Active Shield 实时监控防护与 S-Laser 抗篡改加密，精准覆盖金融支付、身份验证等高敏感场景的量子级安全需求。目前 S3SSE2A 已进入样品发货

阶段，并优先部署于 Galaxy S25 系列旗舰机型，标志着三星在移动安全领域从被动防御转向主动引领量子威胁防御新范式。

（2）英飞凌 OPTIGA™ TPM：跨设备量子安全的标准化基石

英飞凌于 2022 年推出的 OPTIGA™ TPM，是全球首款集成后量子加密（PQC）技术的可信平台模块芯片，致力于为工业控制系统、物联网终端、汽车电子及消费电子产品等各类计算设备提供核心安全保障。该芯片严格遵循可信计算组织（TCG）的全球工业标准，通过内置独立微处理器实现密钥的安全存储与运算，敏感数据仅在芯片内部处理并输出结果，有效抵御固件篡改、旁路攻击等传统安全威胁。在量子防御层面，其除支持传统加密算法外，特别兼容 XMMS 算法以应对量子计算机的潜在威胁，为跨领域设备身份认证、数据加密与完整性保护奠定标准化量子安全基石。

（3）SEALSQ Quantum RootKey：太空级量子安全的突破性应用

SEALSQ 研发的 Quantum RootKey，是首款搭载于卫星的后量子加密芯片，于 2025 年 1 月推出，开创了太空量子安全防护的新领域。该芯片采用抗篡改封装技术，将密钥生成、存储及签名等关键操作隔离在独立安全环境中运行，从物理层抵御旁路攻击与物理入侵；算法层面集成 NIST 标准化的后量子算法（如 CRYSTALS-Kyber 和 CRYSTALS-Dilithium），确保加密通信与身份认证机制在量子计算攻击下保持不可破解性。其技术亮点包括：支持在轨卫星实时密钥管理（已应用于 WISeSat 3.0 卫星）、为物联网设备提供量子抗性数字身份、通过混合密码协议兼容现有系统实现低成本后量子迁移。该

芯片已通过通用准则 EAL5+认证，成为太空通信、国防遥测及智能城市等高敏感领域构建端到端量子安全防线的核心组件，并于 2025 年随欧洲 WISeSat 卫星部署投入实际应用。

（4）Futurex 安全芯片：金融级量子防护的合规性解决方案

Futurex 于 2025 年 6 月 11 日推出的安全芯片是具备 PCI HSM 认证的后量子密码（PQC）硬件安全模块，聚焦金融支付、数据传输等高敏感场景的量子威胁防御。该芯片深度集成 NIST 标准化算法(如 ML-DSA、ML-KEM），并计划支持 SLH-DSA 算法，为用户提供量子威胁下的端到端防护。在技术架构上，其采用硬件级加密引擎与可扩展设计，确保支付系统安全、传输数据机密性及静态数据完整性；合规层面严格符合 FIPS 203/204 标准及 PCI-DSS 等全球合规要求，并通过模块化设计支持混合加密方案，帮助现有系统实现从传统加密向后量子算法的平滑迁移，降低升级成本与风险。

3. 总结

由上述应用可以看出，将经典密码体系迁移至抗量子的后量子密码（PQC）体系已成为必然选择。根据 NIST《后量子密码标准化路线图》，易受量子攻击的算法将分阶段淘汰：ECDSA、EdDSA 及 RSA 算法自 2030 年起进入废止进程，2035 年后将全面禁用。该时间框架看似宽裕，但考虑到企业密码基础设施改造涉及的协议栈重构、硬件兼容性验证及系统迁移复杂度，当前正是制定战略规划的关键节点。尤其需优先关注非对称加密领域，其中密钥交换机制（特别是 TLS 协议中的密钥协商过程）因直面“现在收集，稍后解密”威

胁，已成为密码学社区的研究重点。混合密钥封装机制（Hybrid KEM）作为过渡方案，正加速应用于现代通信协议栈。

随着这些 PQC 算法标准化，纯 PQC 算法实现（如 TLS 1.3 中使用 ML-KEM 进行后量子密钥协商）正在开发中，IANA 已为其分配了标识符（如 MLKEM512:0x0200，MLKEM768:0x0201，MLKEM1024:0x0202）。

然而，业界目前主要致力于实现混合密钥交换。例如在 TLS 1.3 中结合经典算法(如 X25519、ECDH)与 PQC 算法(如 ML-KEM)。这种策略旨在确保：即使 PQC 实现存在未知漏洞，系统也能通过回退到经典算法得到保护，避免单点失效。截至 2025 年 2 月，主流的混合方案是 X25519MLKEM768（该方案在 IETF 文档中与 SecP256r1MLKEM768 和 SecP384r1MLKEM1024 一同定义），已被主流浏览器、密码库以及 CDN 服务商实现。

实施混合密钥交换面临的核心挑战之一是 PQC 密钥尺寸显著增大：这导致一个关键问题：客户端难以高效地向服务器声明其混合算法偏好。若仅在 TLS “ClientHello” 消息中通告支持的密钥组而不附带密钥共享数据，将导致额外的网络往返协商；反之，若同时携带多组密钥共享数据，则会使 “ClientHello” 消息急剧膨胀，可能引发数据分片、性能劣化甚至握手失败。该矛盾在合规性场景下更为突出。由于 FIPS140-2 （2001） 标准未纳入 X25519 与 ML-KEM 算法，混合方案 X25519MLKEM768 被排除在合规体系之外。而基于 secp384r1 与 MLKEM1024 的混合构建虽符合

NIST SP 800-56Ar3 规范，但主流浏览器尚未实现该方案。即使未来实现，服务器端支持的滞后仍可能迫使客户端在“ClientHello”中同时提供多种密钥选项。需注意：NIST 近期声明“拟批准”融合合规算法的混合架构，届时 X25519MLKEM768 可能获准，但政策解读仍存在技术门槛。

迁移至 FIPS 140-3（2019） 能根本解决合规问题，但受监管行业的技术迭代速度较慢。此过渡期内，有提议使用 HTTPS/SVCB DNS 记录来指示服务器支持的密钥交换机制，以减少“ClientHello”膨胀。但这需要网站实际部署 HTTPS/SVCB 记录，目前面临协议支持不足和兼容性挑战。

构建量子安全的互联网是一场马拉松。混合密钥交换作为关键首阶段，其核心使命是抵御“现在收集，稍后解密”威胁，保障数据传输机密性。尽管面临性能优化与设备兼容性等挑战，互联网社区正积极协同攻关。后量子密码学的普及虽常隐于无形，却已悄然提升着数字生活的安全基线——当您下次浏览网页时，那些在后台默默运行的极其复杂且具前瞻性的密码学技术，正在为您的数字未来构筑抗量子防线。

五、后量子密码的通信系统应用迁移实践

（一）量子计算机威胁下的安全风险评估

量子威胁正在推动密码算法和技术的演变。安全风险评估框架使通信基础设施的设计方、生产方和应用方能够合理地评估其设备或数据的安全性，从而制定有效安全规划。米歇尔·莫斯卡（Michele Mosca）阐述了一种基于三个变量的评估方法：

数据和资产的安全生命周期 （x）：指敏感数据和资产需要保持安全的时间段。换句话说，这是需要保护的时间范围，过了这个时间，信息或资产即使被破译，也不会造成重大损害。

迁移到后量子密码 （PQC）的时间 （y）：指企业或组织完成向抗量子密码算法迁移所需的时间。

量子威胁时间 （z）：即有效量子计算机出现并足以破解现有加密技术的时间。如果 x+y>z，则需要立刻考量后量子密码迁移工作。

（二）向后量子密码迁移的时间线

后量子密码迁移时间规划需要综合考虑量子计算的发展和量子威胁。

1. 量子计算加速发展

虽然量子计算攻击的时间表尚不确定，但可以肯定的是，PKI 升级整个网络需要很长时间。因此我们需要关注有关量子攻击时间的更多信息。量子计算已经取得了巨大的进步，并且有大量投资投入到通

用量子计算的竞赛中。基本架构、错误校正和算法改进都推动量子计算效率的大幅提高。物理量子比特数并不是时间表的唯一决定因素，随着逻辑量子比特与物理量子比特比率的增加大量资源和人才涌入，量子计算的进步正在加速。

从过去几年物理量子比特的增长率来看，显然巨额投资开始带来了巨大的能力飞跃。大多数人认为在 2030 年之前破解加密的可能性很大。

2. 立即采取行动的紧迫性

全球国家、机构花了近二十年的时间部署公钥基础设施。2021 年 4 月 NIST 网络安全白皮书指出，“经验表明，在最好的情况下，加密标准发布后需要 5 到 15 年或更长时间才能完全实施这些标准”[76]。算法的替换通常需要更改或替换加密库、实施验证工具、开发实现或加速算法性能的硬件、修改相关操作系统和应用程序代码、更改通信设备和协议以及用户和管理程序。安全标准、程序和最佳实践文档也需要更改或替换，安装、配置和管理流程和文档也需要更改或替换。这项工作只有在选定方向后才开始，这可能还需要 2-4 年的时间。

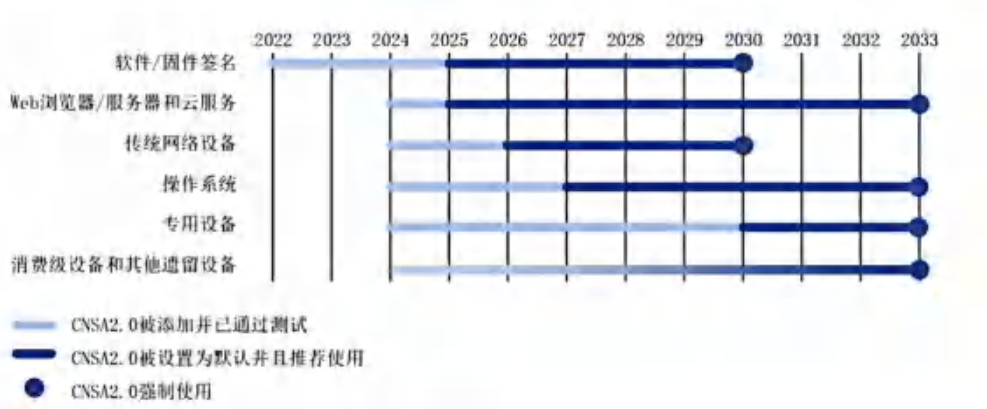

图 5-1 CNSA2.O 针对美国国家安全系统要求的时间线

后量子迁移需要考虑应用生态中的风险，优先考虑迁移保护最有价值资产或支持设备安全的加密技术。迁移过渡时间取决于基于标准的实施的普及程度。由于不同的技术采用后量子算法的进度不同，美国商业国家安全算法套件 2.0（CNSA 2.0）对经 FIPS 认证的产品和设备的迁移截止点设定了严格的限制（17）。

软件签名和固件签名应立即开始迁移工作，在 2025 支持并推荐使用 CNSA 2.0，在 2030 强制使用 CNSA 2.0。Web 浏览器/服务器和云服务在 2025 支持并推荐使用 CNSA 2.0，在 2033 强制使用 CNSA 2.0。传统网络设备（例如虚拟专用网络，路由器等），在 2026 支持并推荐使用 CNSA 2.0，在 2033 强制使用 CNSA 2.0。

操作系统在 2027 支持并推荐使用 CNSA 2.0，在 2033 强制使用 CNSA 2.0。专用设备（例如受限设备、大型公钥基础设施系统）：在 2030 支持并推荐使用 CNSA 2.0，在 2033 强制使用 CNSA 2.0。消费级设备和其他遗留设备在 2033 更新或替换。

（三）通信协议中的融合

应用层	HTTP,**HTTPS**,FPS,**FTPS**,IRC,**DNS**
表示层	**SSL**,**SSH**,MPEG,FTP,JPEG
会话层	**API's , Sockets**
传输层	**TCP**,UDP
网络层	IP , **IPSec** , ICMP , IGMP
数据链路层	**OTNSec**等
物理层	在介质上传输比特流

图 5-2 标红加粗的协议表示可进行后量子密码迁移的协议

开放式系统互联通信参考模型（Open System Interconnection，OSI），定义于 ISO/IEC 7498-1，是国际标准化组织（International Organization for Standardization，ISO）制定的一个用于计算机或通信系统间互联的标准体系，试图使各种计算机在世界范围内互连为网络，一般称为 OSI 参考模型或七层模型。它是一个七层的、抽象的模型体，不仅包括一系列抽象的术语或概念，也包括具体的协议。

OSI 将计算机网络体系结构划分为以下七层：

1.物理层：将数据转换为可通过物理介质传送的电子信号，在介质上传输比特流。

2.数据链路层: 提供介质访问和链路管理，将数据分帧，建立相邻结点之间的数据链路。

3.网络层：定义逻辑地址，供路由器确定路径，实现数据从源到目的的转发过程。

4.传输层：提供可靠的端到端的报文传输和差错控制。

5.会话层：在通信双方之间建立、管理和终止会话，该层的通信由不同设备中的应用程序之间的服务请求和响应完成。

6.表示层：协商数据交换格式，对数据进行转换、加密和压缩，以确保一个系统生成的应用数据能够被另外一个应用所识别和理解。

7.应用层：用户的应用程序和网络之间的接口。

目前，OSI 七层模型中的很多协议都可以实现后量子密码的迁移，如应用层的 HTTP 和 DNS，表示层中的 SSL 和 SSH 协议等，具体如图 5-2 所示。

HTTPS 协议可理解为 HTTP 协议与 SSL 协议的结合，其中 SSL 协议又称为 TLS（Transport Layer Security，传输层安全）协议。TLS 是当今互联网上使用最广泛的协议之一，其为通信双方之间提供机密性、完整性和真实性等安全属性。最新版本 TLS 1.3 使用 ECDH（Elliptic Curve Diffie-Hellman，椭圆曲线 Diffie-Hellman）算法来进行密钥交换，使用 ECDSA（Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法）对服务端和客户端的身份进行验证。鉴于 TLS 1.3 是当今最广泛使用的安全协议，将后量子密码术集成到其中成为了目前的研究热点。

对于 TLS 1.3 的后量子迁移工作，KEMTLS 方案被学界认为是一种新颖且有效的方法。它使用密钥封装机制（KEMs）来保证机密性和进行身份验证，实现后量子安全性的同时避免了昂贵的后量子签名。KEMTLS 使用两种 KEMs 来表述：用于临时密钥交换的 KEMe 和用于隐式身份验证的 KEMs。

以下是 KEMTLS 建立连接，进行握手的通信过程：

（1）建立 TCP 连接后，客户端首先产生自己的公钥和私钥，然后发送一个或多个公钥给服务端，服务端接收后使用公钥进行密钥封装操作，得到共享密钥和密文。

（2）服务端发送密文和一个加密过的公钥证书给服务端，客户端接受到后，使用私钥和密文解封装得到共享密钥。

（3）客户端使用证书公钥进行密钥封装操作，获得另一共享密钥和密文并将得到的密文加密发送给服务端。

（4）服务端使用收到的密文和证书对应的私钥进行解封装操作，得到另一共享密钥。然后利用密钥派生函数（KDF）运算得到多个通信密钥，之后客户端和服务端即可使用通信密钥对数据进行加密并通信。客户端和服务器端建立连接的过程如图 5-3 所示。

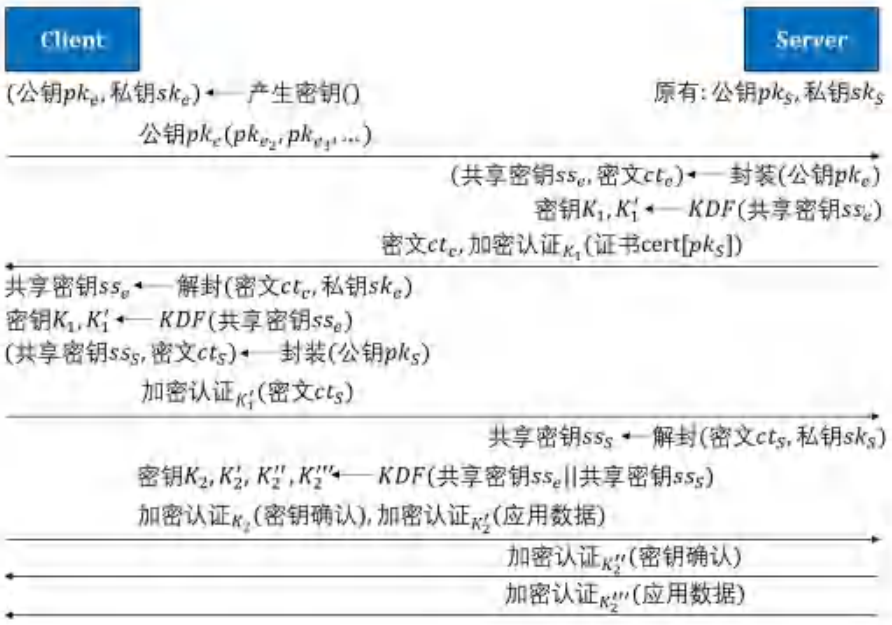

图 5-3 KEMTLS 握手

在后量子加密的迁移指导方针中，部分地区或机构主张采用混合模式，即同时使用传统算法和后量子算法的混合模式。这将有利于后量子加密的迁移，并提供了可实施的回退机制。混合模式中，当新引入的后量子加密算法不适用，或在后续研究中被证明失效时可将其屏蔽，或者回退传统加密结构。但混合模式需要同时部署两套加密算法，这将带来额外的性能开销和系统复杂度的提升，在某些应用场景下显然是不合适的。

1. 传输层安全协议（TLS）1.3

TLS 是一种客户端与服务器之间建立应用层安全通信通道的协

议。TLS 协议使用证书提供单方或相互认证。最新的版本 TLS 1.3 已经作为 IETF RFC 标准化，然而之前的版本如 TLS 1.2 和 TLS 1.1 仍然被广泛使用。许多网络域和浏览器不再支持 TLS 1.1，但是由于许多遗留设备和组件仍在使用，这意味着其他实体如服务器可能需要接受仅使用 1.1 版本的传入连接。 一个 TLS 会话由参与方协商一致的密码套件定义，并通过其组件的名称来描述。

例如， TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 定义了使用（临时的）椭圆曲线 Diffie-Hellman 进行密钥交换，RSA 用于数字签名，AES-GCM 带 128 位密钥用于记录层加密以及 SHA2 带 256 位摘要进行哈希运算。AES 和 SHA2 是对称算法，因此相较于 ECDHE 和 RSA 签名这两种公钥加密算法，它们更不易受到量子计算攻击的影响。

IETF 草案提出了在混合模式下使用 TLS 1.3 的密钥交换组件。本质上，密钥交换阶段会使用标准的 TLS 1.3 密钥交换消息交换流程进行两次或更多次，同时采用不同的底层算法，例如使用传统的 ECDHE 算法和后量子安全的算法如 ML-KEM，并且生成的密钥通过连接的方式组合成一个整体，然后输入到为记录层提供会话密钥的密钥派生函数中。如同所有混合密钥交换设计一样，其目标是只要至少有一个组件算法是安全的，那么整个方案就是安全的。值得注意的是，这种迁移仅限于 TLS 中的密钥交换组件，并不涉及 TLS 的数字签名组件，因此可以防止存储现在以备日后解密的攻击（即会话流量的解密），但并不涵盖认证攻击（例如，对手获取了用于证书的签名

密钥并冒充服务器）。

TLS 1.3 允许使用预共享密钥恢复模式，在该模式下，先前生成的秘密材料被用来加密一个恢复会话中的初始通信。这些恢复使用的预共享密钥可能依赖之前使用了易受量子攻击的非对称加密或密钥交换算法，因此如果先前会话中生成密钥材料所使用的算法不是后量子安全的话，那么它们就容易受到量子攻击。在本文档中，“预共享密钥”一词仅指通过不依赖于易受量子攻击算法的方式预先共享的密钥材料。因此，量子安全讨论中提到的预安装在设备上的秘密密钥，例如 SIM 卡上的秘密密钥，或是通过纸笔方式物理共享的秘密，可以归类为预共享秘密。但是，TLS 1.3 恢复模式中使用的源自易受量子攻击算法的预建立的秘密则不属于此类。

2. 网络层的后量子密码融合

IPSec 作为现代网络的基础加密框架，用于在网络层提供机密性、完整性和认证。在量子威胁背景下，IPSec 需要通过协议扩展、混合模式和产业化落地，来平滑过渡到后量子密码。

IKE 是一种用于两方在互联网层建立安全通信通道的协议，它是 IPsec 套件的一部分。与 TLS 相似，IKE 使用证书来进行认证，并且其核心的密钥交换协议基于 Diffie-Hellman。IKE 版本 1 已被 IKE 版本 2 所取代。IKEv2 在虚拟专用网络（VPN）应用中非常广泛地被使用。IETF RFC 文档描述了一种 IKEv2 的扩展，使其通过使用预共享密钥变得能够抵抗量子计算机的攻击。另一个 IETF 草案于 2023 年 5 月发布，目的是在混合模式下使用 IKEv2 的密钥交换组件。这

一想法与 TLS 的混合模式草案略有不同：首先使用 Diffie-Hellman 密钥交换建立一个初始的安全通道，然后在这个通道内部进行第二次（甚至可能是第三次）密钥交换，使用诸如 ML-KEM 的后量子安全密钥交换机制作为 IKE_INTERMEDIATE 扩展。

当前，StrongSwan、Libreswan 等开源实现已在主干分支中加入 Kyber / Dilithium KEM 和签名支持。Cisco、Fortinet 在企业远程接入 VPN 中开展混合 KEM 测试，验证 NIST L3/L5 算法的性能与互操作性。

通过以上协议扩展、典型应用和产业化实践，IPSec 正在稳步向后量子时代演进，为网络层提供连续可用、向后兼容且安全的量子抗性方案。未来建议在标准组织（IETF、3GPP）与厂商联盟中推进正式 RFC 定稿，并在运营商核心网与云边协同中加速规模部署。

（四）通信系统中设备级集成

后量子密码（PQC）技术正被多家厂商嵌入到光传输、VPN、安全网关等关键设备中，以实现“经典+量子安全”双重保障。以下三类代表性产品展示了产业化落地思路。

ADVA FSP 3000 ConnectGuard™光传输系统 ADVA 在其 FSP 3000 光传输系列中率先引入了混合密钥封装（Hybrid KEM）和后量子算法选项。该平台的 ConnectGuard™ Layer 1 加密模块原生支持 AES-256，同时可插装 CRYSTALS-Kyber、Classic McEliece 等 PQC KEM 算法，并与 CV-QKD 插件无缝共存。设

备无需更换硬件，通过软件升级即可启用后量子密钥封装，并保持端到端 100% 吞吐率和 <10 μs 级加密延迟，经济高效地保护长途和城域网络的光路安全。

Utimaco u.trust GP HSM “Quantum Protect” & PQC VPN 方案 Utimaco 推出的 Quantum Protect 应用包可在其通用型硬件安全模块（HSM）上原位激活，支持 NIST 标准 ML-KEM 与 ML-DSA、LMS/XMSS/Multi-Tree 等格基与哈希型签名方案，无需更换 HSM 即可完成后量子就绪。利用该 HSM 构建的“PQC VPN” 网关将后量子密钥封装、数字签名及常规 IPSec/TLS 协议集成于一体，为企业 VPN 隧道提供量子安全的动态密钥交换和证书签名能力，同时兼容现有网络管理与密钥管理流程。

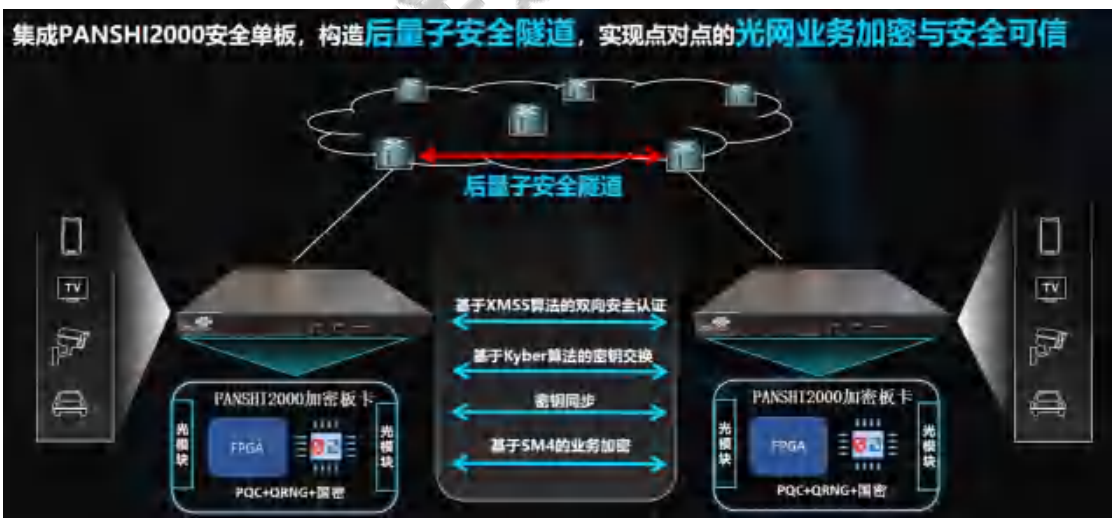

图 5-4 关键技术

中国联通研究院联合武汉二进制半导体有限公司联合打造国内首款后量子密码与国密融合光传输设备，该产品具备安全合规、轻量级、低成本、纳秒级延时等特性，可应用于政务、国防、金融、能源、交通、等领域的数据与信息安全保障。设备首次集成了二进制半导体

自研的后量子密码算法软硬协同加速器。在此基础上构造了一种适用于标准以太网的后量子安全协议，能够高效完成点对点的安全认证以及密钥交换。在此基础上，联通以太网设备能够构造后量子安全隧道，保障光通信网络的安全可信。该协议能够有效兼容现有的以太网数据包结构，易于快速集成以完成现网的安全改造。单次安全认证及密钥交换仅需 10KB 数据传输，对现网带宽无影响，兼具轻量级特性。

设备还集成了二进制半导体自研的国密 SM4 算法全流水硬件加速器。支持双向 10G 同步业务加解密功能，实现纳秒级延时。通过与自研的网络接口进行片内硬件集成与融合，实现了真正的纳秒级加解密延时。通过集成自研的片上密钥管理模块，能够实现针对特定以太网包的高速密钥更新，能够应用于工控、金融、国防等对延时敏感的应用场景。

设备集成了量子随机数发生器及电学随机数生成器，能够高效生成随机数，以保障密钥生成以及安全协议的安全性。同时，还集成了符合国密要求的安全芯片，能够安全的完成板上密钥管理及关键信息存储，具备合规性。安全芯片的可编程功能，使得本设备易于扩展，能够快速兼容新的安全协议与算法。

通过以上关键技术的集成，实现国内首款后量子密码与国密融合光传输设备。通过安全管理界面，能够实时控制安全认证及密钥交换的更新周期，可以监控当前设备的安全功能状态，便于集中化运维。国内首款后量子密码与国密融合光传输设备的发布突出展示了中国联通在后量子密码、国产密码、及其在通信系统中的集成应用方面具

备算法级开发、核心组件、硬件集成等自主研发硬科技实力。为下一代安全通信技术的产业化提供了强大的技术支持。

这三种设备级集成方案，均通过“插拔式”“软件可升级”与“经典+后量子”混合策略，实现了向后量子安全的平滑演进，为通信运营商和大型企业构建了可大规模复制的落地模板。

（五）密码敏捷性：应对加密算法演进的核心战略

1. 密钥敏捷性的定义

密码敏捷性指的是：在不需要重大工程改动的前提下，系统更换算法或参数集的能力。在 TLS、SSH 等主流协议中，算法和参数通常由通信双方通过安全协商动态决定。一方发送自己支持的算法集合，另一方从中选择合适的算法使用。只要交换过程中的每一部分都被身份验证，这种机制就可以有效抵抗降级攻击——即攻击者无法强迫双方使用比原协议更弱的算法，并且此机制也可以自然扩展以支持 PQC 算法。证书签名中也包含算法信息，因此可以支持多种算法共存。

2. 面临的挑战

尽管协议层面提供了敏捷性支持，PQC 迁移过程中仍存在以下核心难点：

- 过度追求敏捷性可能导致极端复杂性。如果过分强调敏捷性，会导致系统协议复杂度激增、维护困难、漏洞频发。例如，明确定义的椭圆曲线就是一个频繁出现安全漏洞的领域，最终被

RFC5480 禁止。该案例不是说密码敏捷性本身有害，而是要恰当使用它。

- 算法协商是同步操作，性能成本高。上述的算法协商本质上是一个同步过程，往返通信是必要的。这对于异步系统或追求最小通信开销的系统（例如 TLS 1.3）来说是一个问题。例如，客户端必须在首次通信中预测正确的密钥交换算法，并发送对应的 keyshare；如果预测错误，服务器会回复 HelloRetryRequest，从而导致额外的握手延迟。虽然 TLS 支持敏捷性，但主动使用这种能力是有成本的，尤其是在 PQC 中更为显著。
- 错误的实现方式可能造成严重安全漏洞。如 JWT（JSON Web Tokens）这样的系统就是典型反例：算法选择直接来源于未验证的令牌字段，攻击者可以设置算法为“none”、将非对称签名变为对称 MAC，或将 PQC 算法降级为经典算法。这个问题促使标准 RFC8725 诞生，它明确规定：实现者不应依据 token 中的算法字段做出选择，而应使用由应用提供的外部配置。对于同步协议，如果密钥派生函数（KDF）未包含整个消息交换内容，攻击者也可篡改协商消息，使通信双方误以为是对方选择了较弱算法，从而引发降级攻击。

3. 密码敏捷性与密钥轮换的关系

为了实现安全的密码敏捷性，特别是在异步协议中（例如证书、令牌等），我们要确保算法信息来源可信。值得注意的是，所有密码操作本质上都依赖一个可信输入：密钥本身。因此，只要将算法或参

数信息与密钥存储在一起，攻击者就无法伪造算法选择。

这也引出了一个关键结论：如果算法由密钥决定，那么更换算法就意味着更换密钥。因此，系统只要具备密钥轮换能力，就具备实现密码敏捷性的基础能力。反过来说，若要支持 PQC 迁移，一个系统必须具备稳定的密钥轮换机制。

4. 实现无中断的密钥轮换

当系统必须执行轮换操作时（例如密钥泄露后），需要保证系统可依赖该流程。同时，在未检测到的密钥泄露场景中，密钥轮换还能提供一定程度的被动恢复能力。然而需要指出的是，密钥轮换虽然在理论上简单，但在实践中存在显著挑战：若密钥在错误时间点被引入或删除，将产生严重的可靠性风险。若系统试图直接替换新旧密钥，将引发严格的分布式一致性问题，这种问题通常极难解决。因此，我们需要采用最终一致性方式实现密钥轮换。

以开源密码库 Tink 为例：在此模型中，需将密钥统一管理而非单密钥作为基础操作单元。因此，密钥集内所有密钥必须支持相同的密码学操作（在 Tink 中称为"基元"）。与混合加密架构不同，集合内的密钥并非协同工作，而是逻辑"或"关系。这意味着每个密钥都被系统完全信任，而整个系统的安全性等同于集合中最弱密钥的安全水平。

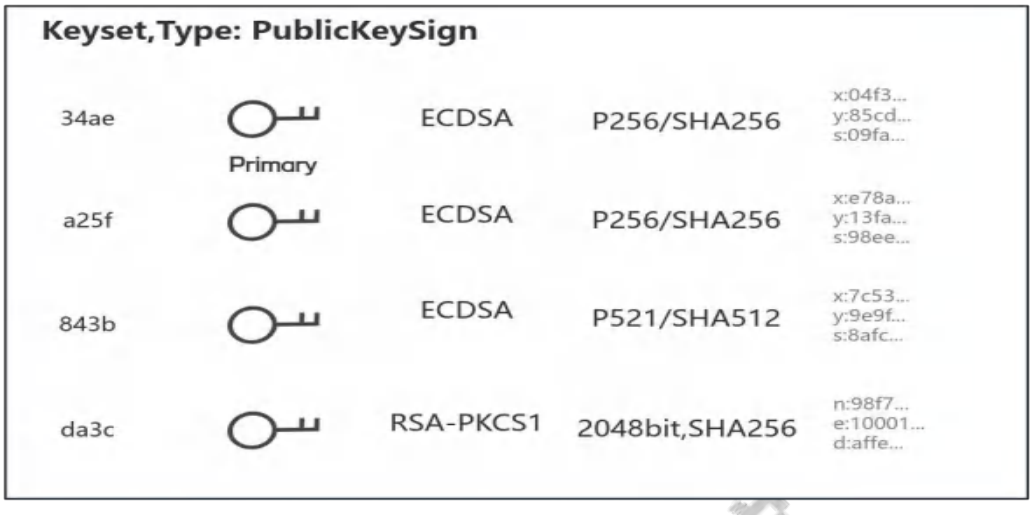

图 5-5 包含算法信息和参数的密钥集

在密钥集中，必须指定一个主密钥（符合 NIST SP 800-57 Part 1 的"active"标准），用于执行主动操作（如签名或加密）。作为性能优化措施，Tink 可在生成密文或签名时，为大多数基元添加主密钥标识符前缀。该标识符使得被动操作（如验证或解密）能直接定位对应密钥。这种密钥集架构可视为独立实现的密码基元，其功能与组成密钥实现的基元相同。

基于此密钥集架构，密钥轮换可通过三个阶段实现：

（1）移除密钥集内最老的密钥（图 5-5 中 ID 为 da3c 的 RSA-PKCS1 密钥）；

（2）将密钥集内最新密钥设为主密钥（图 5-5 中 ID 为 34ae 的 ECDSA 密钥）；

（3）向密钥集注入新生成密钥（图 5-6 中 ID 为 fe71 的 ECDSA+Dilithium 混合密钥），该密钥将在下次轮换时激活。需特别说明：混合密钥在此并无特殊处理逻辑，其与传统签名密钥采用相

同管理机制，且 PQC 组件与传统组件同步生成。

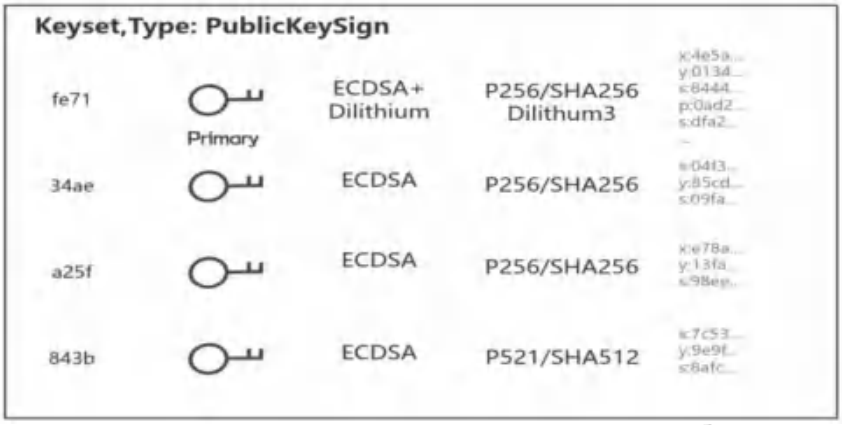

图 5-6 执行密钥轮换后的密钥集

显然，这种轮换方案允许签名方与验证方存在版本差异而不影响系统功能。若签名方持有新密钥集，其使用 ID:34ae 密钥生成的签名，在持有旧版密钥集的验证方仍可正常验证。反之，由于密钥 ID:a25f 尚未被移除，已完成更新的验证方仍能验证未更新签名方产生的签名。

此基础流程可进一步优化：例如通过监控机制，在自动淘汰旧密钥前向密钥管理系统报告仍在使用旧版本解密的密文或验证的签名。在异步环境中，这些密码对象的生命周期可能超过密钥的有效期。此外对于非对称基元，主动操作端无需访问完整密钥材料，仅需保证主密钥可访问即可。

5. 密码敏捷性的核心价值

密码敏捷性不仅仅是一次后量子算法的部署，更是一套持续演进的安全保障机制。拥有敏捷能力的系统可以在发现算法弱点或监管要求变更时，用最小的业务影响完成算法替换，从容应对“先收集后解密”带来的长期风险；同时，它为组织探索新一代轻量级密码、同态

加密、多方计算等前沿技术提供了试验平台，成功与失败都能被快速验证并纳入下一轮迭代。更为重要的是，密码敏捷性助力企业在合规审计中展现快速响应能力，提升整体安全治理的可信度和透明度。

6. 密码敏捷性实现的层级和技术挑战

要实现真正的敏捷能力，需要在协议层、应用层和硬件层构建多层次的支撑。协议层面要保证加密套件协商机制能够动态更新并完整保护协商过程，以防止中间人篡改；应用层面则需通过抽象化的加密接口和统一的配置平台，实现算法替换后业务逻辑“无感知”；硬件层面更需打破传统不可变信任根的局限，设计可插拔或可升级的安全模块，使长期服役的工业设备、智能卡和 HSM 具备同样的灵活性。在这三者之间，如何平衡安全不可变性与灵活更新的矛盾，是最为核心的架构难题。

在协议层面，系统必须具备动态协商算法的能力，并在握手过程中完整传递算法版本与退役时间，以保证协议切换时的安全与可靠。混合模式下，经典算法与后量子算法并行运行，能够在平滑过渡期内维持通信安全，同时为后续切换留足缓冲。

在应用层面，敏捷能力依赖于清晰的架构分离，所有加密功能通过统一的 API 接口暴露给业务逻辑，并由集中化配置平台下发策略，使得算法升级仅需调整配置即可生效，而无需对业务代码做任何修改。此外，为应对硬件受限或不可更新场景，必须在设计之初预留更大内存空间和多种参数适配方案，确保新算法在各种环境中均可兼容运行。

硬件层是实现敏捷的关键瓶颈之一。芯片与 HSM 的信任根设

计固化了特定算法和参数，但长期部署需求却要求在设备寿命周期内不断更新算法。通过在工业控制设备中引入可插拔的加密模块，并为智能卡等短周期设备制定严格的加密功能规范和升级验证流程，可以在不改变整体硬件架构的前提下，实现算法的平滑替换。

企业治理层面需要构建覆盖所有环境的加密资产清单（CBoM），并依据风险优先级制定退役与替换计划。自动化配置管理和策略下发工具能够对弱算法进行快速下线，同时结合定期的演练机制，使组织在真正面对安全事件时能够迅速响应并完成升级，保障业务持续稳定运行。

在 PQC 迁移过程中，组织必须深入考量以下八个关键技术因素，以确保平稳和安全的过渡：

表 5-1 八个关键技术因素及具体要求

技术挑战（Technical Challenge）	具体影响/要求（Specific Impact/Requirement）
带宽	PQC 算法密钥尺寸增大，导致数据流量和延迟增加；需网络升级、优化。
存储	PQC 证书需要更多存储空间；过渡期间需额外存储，并规划扩展。
协议	现有通信协议（TLS, SSH 等）必须更新以支持 PQC 算法的密钥交换和签名。
应用/软件升级	软件和应用程序需大量修改以兼容 PQC 库和新标准；需全面清单和测试。
硬件升级	PQC 对处理能力要求更高，可能需新服务器、处理器、HSM 或专用加速器。
第三方应用和服务	组织依赖的第三方供应商技术需支持 PQC；需与供应商沟通，协调集成。
标准与指南	需遵守新兴 PQC 相关 RFC、标准和指南；需整合和维护最新的 PQC 库。
监管合规性	需符合新的 PQC 监管要求；需更新合规政策、定期审计和维护文档。

7. 关键技术难点与应对策略

在算法和实现并存的情况下，密钥、签名尺寸的剧增往往会给网络带来压力，硬件专用加速器和并行化处理是缓解之道；多算法并行存在时，攻击面会被不经意间放大，必须在设计时坚持“少即是多”的原则，仅保留关键算法并在代码层面进行最小化实现；而经典算法与 PQC 算法在数学结构和参数格式上的差异，也要求在 SDK 或中间件层面预留足够的缓冲与转换能力，才能避免升级过程中出现兼

容性故障。对于云服务商，还需要通过“加密即服务”（EaaS）的方式，将多元化算法以分层模式提供给不同租户，并结合策略引擎与审计日志，确保灵活可控。

表 5-2 总结挑战领域具体问题及解决方案

挑战领域	具体问题	解决方案
资源消耗	PQC 算法大密钥/签名	硬件专用优化
安全性	算法增多扩大攻击面	最小化实现选项
兼容性	经典/PQC 数学结构差异	敏捷意识设计（预留大内存缓冲区）
云服务	客户需求多样化	加密即服务（EaaS）分层提供

协议层面，许多安全协议使用加密算法来提供机密性、完整性、认证和/或不可否认性，通信双方必须就一组通用的加密算法（称为密码套件）达成一致，以使安全协议正常工作。安全协议的这一方面被称为密码套件协商，包括用于完整性保护、认证、密钥导出、密钥建立、加密和数字签名的算法，以提供所需的安全服务。当安全协议可以轻松地从一个密码套件转换到另一更理想的密码套件时，就实现了加密灵活性。NIST 白皮书指出混合加密算法是 PQC 过渡的即时解决方案。这种方法结合了传统公钥密码学（如 ECDSA）和 PQC（如 ML-DSA），旨在为 PQC 方案中不可预见的漏洞提供保障，同时确保系统在整个过渡期内的安全，即如图 5-7 所示。

每个安全协议通常指定一个强制实现算法，以确保支持基本的互操作性，安全协议也应是模块化以增强加密灵活性，并方便插入新的算法或密码套件。同时，加密灵活性意味着安全协议必须支持一个或多个算法或密码套件标识符，并期望强制实现的算法集会随着时间的推移而变化。

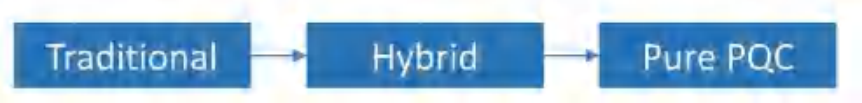

图 5-7 可能从混合模式进行第二次过渡

8. 结论

量子加密标准的不断落地，为密码敏捷提供了实战舞台。2024 年 NIST 正式发布 ML- KEM、ML- DSA、SLH- DSA 等三项 PQC 标准，并于 2025 年 3 月加入备选方案 HQC。企业可提前考量 PQC 应用，一边验证新算法兼容性，一边为大规模部署打下基础。

更宏观的角度来说，密码敏捷应成为行业协作的新共识。Deloitte 提出的“Quantum Trust”以密码敏捷作为零信任架构的一部分，体现跨维度融合的趋势。持续演进的安全基座。

密码敏捷是一项工程与治理并重、标准与实践齐驱的系统工程。需要构建评估路径，以治理整合为基础、资产盘点为起点、模块化设计为中枢、演练/监控为支撑，企业不仅能抵御当前经典加密漏洞，也为未来量子攻击留下主动选择空间。这与“一次性算法升级”形成鲜明对比，而是一个持续优化、可预见、可控制的安全机制。在这个意义上，密码敏捷已成为信息安全战略的主干，也是组织迈向“未来可持续”的必经之路。

（六）中国联通的实践

随着量子计算的飞速发展，支撑现代数字社会安全的经典密码体系正面临前所未有的颠覆性威胁。“先截获，后破译”的风险迫在眉睫，数据的长期安全无法保障。中国联通前瞻性地启动后量子密码迁

移，旨在构建能够抵御未来量子攻击的下一代安全网络，确保国家、企业与个人的信息资产万无一失。

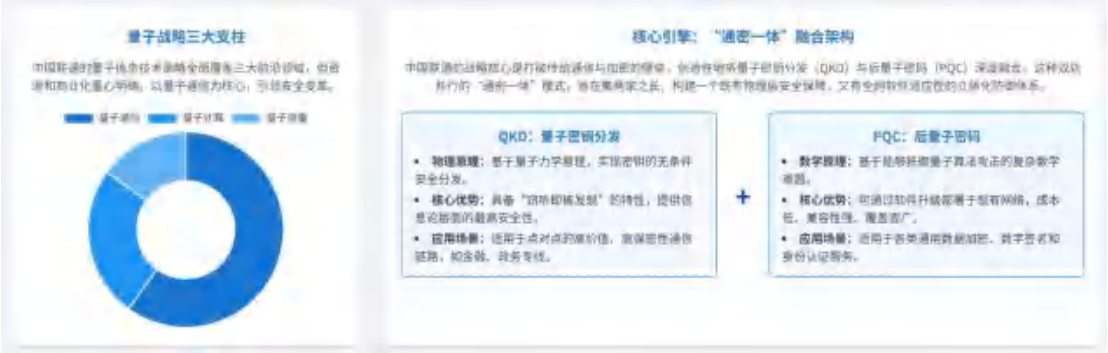

图 5-8 联通量子技术战略全景图

中国联通的策略明确指出将“QKD+PQC 技术并举”，并在其网络中实现“量子经典深度融合”。通过整合这两种技术，中国联通旨在构建一个更健壮、更通用、更具弹性的量子安全解决方案，通过结合最高级别的密钥安全性与广泛的适用性，可能获得竞争优势。这也为单一技术长期可行性的不确定性提供了对冲。

中国联通正通过将其后量子密码策略深度融入现有的量子通信基础设施，以应对后量子时代的挑战。这种前瞻性部署旨在其云、网、端、管各层面构建“量子安全内生服务能力”，确保未来网络安全能够有效抵御量子计算带来的潜在威胁。中国联通的 PQC 策略是其更广泛的量子信息技术路线图的核心组成部分，该路线图同时涵盖了量子计算和量子测量。在 PQC 领域，其核心重点在于开发“通密一体”的融合解决方案，有效利用 PQC 和量子密钥分发（QKD）两种技术。目前，中国联通联合二进制半导体有限公司完成了集成国密与后量子密码的“通密一体”量子融合通信设备研发，并积极探索量子加密通话和量子专线等应用。公司在统一管控平台方面取得了初步进展，并

正合作开发 PQC 加密手机。

图 5-9 联通联合二进制半导体研发的通密一体设备

六、向后量子密码迁移的路线与策略

（一）建立量子迁移路线

密码算法正处于向后量子密码学转变的关键转折点，随着 NIST 宣布了 PQC 算法的标准化结果，以及最近关键算法的最终确定，许多企业和供应商开始制定他们的迁移策略。当组织评估这些变化的潜在影响时，采取积极主动的措施以在不断变化的环境中保持领先至关重要。世界各地的监管机构也强调了在不断发展的数字环境中，立即做好准备以确保合规性和安全性的重要性。制定有效的 PQC 准备计划需要战略远见、技术评估和操作规范的结合。

1. 建立密码资产清单

了解密码技术在当前系统中的应用和使用方式至关重要。因此，有必要对现有的加密技术进行全面细致的盘点，以识别可能容易受到量子攻击的技术及其相关数据的关键性。其具体包括：

发现所有 IT 和 OT 系统中当前使用的算法（RSA， ECC， AES 等），并记录所有依赖密码技术的应用程序、设备、系统和流程。标识所有机器凭证，包括 TLS 证书、SSH 密钥和代码签名凭证，以及它们使用的协议和依赖于它们的应用程序。

上述做法的优势在于：允许对风险评估过程进行规划，以确定向 PQC 迁移的优先级；为向零信任架构的过渡做好准备；通过识别哪些数据可能面临“先存储后解密”的威胁，为未来的分析提供信息。

2. 风险评估

风险评估有助于确定可能受量子计算影响的应用程序和算法列表。需注意的是，并非所有数据和系统面临的风险都是均等的，因此应根据数据敏感性和生命周期、暴露程度、合规性及法律要求，按优先级为资产排序风险。

3. 制定阶段性策略

PQC 的迁移并非一蹴而就，而是一个分阶段的过程。

混合密码学：首先实施 PQC 算法与经典算法并行使用，以保持兼容性并测试有效性，同时不中断现有服务；

算法选择：基于最终确定的国密标准、NIST 标准等标准体系，选择合适的算法（例如，选用 CRYSTALS-Kyber （ML-KEM） 进行加密，选用 CRYSTALS-Dilithium （ML-DSA） 进行签名）；

试点部署：从非关键应用或测试环境开始验证功能、性能影响和互操作性；

供应商和合作伙伴协作：与供应商和服务提供商合作，了解他们的 PQC 支持时间表并协调升级事宜。

4. 更新安全策略和合规框架

企业或组织的安全策略应该随着技术变化而发展，以适应量子计算机时代的安全需求。例如，需要修改加密和密钥管理策略，以纳入后量子密码算法。定义弃用易受攻击的加密算法和应用程序时间表，以监控和适应新兴的与量子相关的监管要求。

5. 持续监测和调整

即使初步过渡可能已完成，但持续关注 PQC 领域的更新和进展至关重要。企业需要留意相关技术进展，追踪 PQC 法规和标准的更新，定期培训员工以保持专业知识和意识，并定期重新评估和更新策略。

（二）当前应用中存在的瓶颈

1. 针对后量子密码体系风险评估困难

现有的密码系统错综复杂，内生安全模块的量子脆弱点位置及使用方式难感知。密码系统通常由多个子系统和模块组成，这些模块之间通过各种接口和协议进行通信。内生安全模块嵌入在这些复杂系统中，负责数据加密、身份验证、权限管理、日志记录等安全功能。多种传统密码算法被广泛使用以保障系统的安全性。底层硬件利用对称密码 AES 和公钥密码 RSA、ECC 等来提供安全服务；在应用层，签名认证则需要用到数字签名技术；而在通信过程中，使用的安全协议则是密码算法的综合运用，如 SSL/TLS 协议。基于场景的差异，即使是同一个系统，其内部的密码算法也需要进行修改和更新，这也是造成系统内部密码算法复杂的原因之一。如何及时准确地发现易受量子计算攻击的密码算法所在位置及使用方式是当前面临的关键挑战。

2. 现有标准化后量子密码算法实现及迁移困难

迁移实施过程中首先面临的挑战是如何在不影响现有系统正常

运行的同时完成密码算法的热迁移。后量子密码算法标准处于初步完成阶段，一些后量子密码的交互逻辑与旧系统不兼容，例如基于哈希函数的 SPHINCS+ 签名算法需要双方维护一个长期存在的密钥，而调用签名算法的旧系统则未必具有维护长期密钥的能力。还有一些后量子密码的性能开销导致无法在旧系统正常运行，Kyber768 在实现 TLS 的三次握手时，过大的 Hello Client 可能会超出旧有底层硬件的处理能力，进而导致协议的异常中断。后量子密码算法与传统密码算法有不同的交互和性能特性，如何在不影响现有系统正常运行的同时完成密码算法的热迁移成为迁移平稳过度的关键挑战。

另外，迁移实现还需要支持不同后量子密码算法的可插拔设计以及互联互通，并且当算法失效时，业务机制还需要支持回滚。这里的算法失效指的是：有可能选用的后量子密码在量子计算机出来之前就已经被经典电子计算机攻破，这种事情也有可能发生，比如 SIKE 算法在刚进入第四轮评估一个月就被攻破，这时，现阶段系统要有能力退回到之前不抗量子的系统，或者迅速切换到其他未被攻破的算法。

3. 如何应对后量子密码在边缘设备中性能和功耗平衡难

通过对各种后量子密码算法进行抽取和分析可以发现，其主要涉及模运算、系数生成等核心算子。后量子密码的核心计算运算涵盖了多项式、矩阵和向量间的模加、模减和模乘等运算。核心算子的硬件实现结果直接影响着整个后量子密码系统 的资源开销和运算性能。针对信息安全领域应用多样性和开发通用性、安全级别的多元化需求问题，在对后量子密码方案中的核心算子进行硬件实现时，需要综合

考虑功耗、性能与面积的折衷关系：在优化硬件资源开销的同时保证一定的运算性能，在追求高性能的同时避免不必要的资源开销，在电路设计的过程中加入低功耗技术，从而最终取得特定应用场景下最高的硬件实现效率。

4. 高效实现后量子密码算法同时兼具抗侧信道攻击技术难

NIST 后量子标准化项目最初的评估标准侧重于提议方案的安全强度和实现难易。不过随着候选过程的推进，也增加了一些其他安全特性要求，其中最重要的一个特性就是实现安全性，即要具有抵挡侧信道攻击的能力，因为近年来的研究表明，侧信道攻击会严重威胁到后量子密码方案的实现安全性。在 NIST 后量子标准化项目第三轮会议后，分析和防范侧信道攻击成为一个亟待探索的重要领域。抗侧信道攻击防御设计已是 NIST 后量子标准化项目的研究重点，对于使用素数模的格密码方案（如 Kyber）来说光是无保护的硬件设计就已经要消耗大量的硬件资源了，因此针对不断优化提出的高效算法实现，在既保证抗攻击结构有效性的同时，又要尽可能的降低硬件资源开销、提高吞吐量性能，是一个需要不断研究探索的重要方向。

5. 技术挑战

从算法性能上考虑，PQC 算法通常需要更多的计算资源、内存、存储和通信能力，因为它们通常具有更大的密钥大小和更复杂的算法，了解和衡量 PQC 算法对于不同部署场景中的性能影响仍需进行深入研究。较大的密钥大小可能会影响安全通信协议（如 TLS）中的分组和延迟模式，从而影响针对当前加密协议优化的网络设备（如路由器、

交换机、防火墙），因此当前大量研究聚焦于优化特定 PQC 算法的性能，包括并行性、更好的内存访问策略和新的数据结构等。

从实现方法上考虑，PQC 算法的核心困难在于如何将数学算法转化为特定平台的优化设计。特别是对于物联网（IoT）等资源受限设备，由于存在功耗、内存和算力等多重限制，如何在保持抗侧信道攻击能力的前提下高效实现 PQC 算法,仍需开展更深入的研究探索。

6. 运营挑战

由于密码技术在系统中的广泛应用，发现和修复漏洞变得愈加复杂。为了实现向 PQC 的迁移，必须明确密码技术的部署位置和使用方式，而这只能通过建立密码资产清单来实现。如果缺乏清晰的资产清单，企业将难以有效开展风险评估，也无法优先识别最容易受到量子威胁影响的系统和流程。在迁移至 PQC 的过程中，企业可能还需同步向零信任架构转型。因此需重新定义访问控制策略和安全协议，现有基础设施和流程可能需全面调整，以适配零信任的“持续验证、最小权限”原则，这直接带来了运营上的挑战。

7. 安全挑战

PQC 由于其新的特性和要求而带来了新的安全挑战。与 RSA 和 ECC 等其他传统算法相比，PQC 算法在密钥大小和计算时间等方面存在不同的权衡，这增加了其安全性评估的难度。为了理解不同使用领域中不同 PQC 算法的安全性权衡，需要进行更多的研究。这包括分析威胁模型、潜在算法缺陷，评估由新型通信模式和内存占用特性可能引发的侧信道漏洞。此外，新型的攻击手段如基于内存的攻击、

时序攻击、差分故障分析等也需要更为详细的研究。

（三）未来的工作中的重点

未来中国后量子密码标准化将围绕多方面展开，为信息安全战略助力。企业需在四大核心领域协同发力推动 PQC 应用，包括标准化、实践转化、自身能力构建及客户迁移。政府则应发挥引导协调作用，运用政策工具激励应用，促进跨行业合作与人才培养，全方位提升国家信息安全水平。

1．未来展望：推动标准化的全面进程

随着量子计算技术的发展，后量子密码学的标准化将在未来几年内成为中国信息安全战略的核心部分。中国在密码学领域具有深厚的技术积累和人才储备，这将为后量子密码的标准化工作提供强有力的支撑。

未来，中国的后量子密码标准化进程可能会围绕以下几个方面展开：

- 标准选型与评估：结合国内外的研究成果，选取具有广泛适用性和高安全性的后量子密码算法，并在标准化过程中引入多方评估机制，以确保其抗量子攻击的能力。
- 国际合作与互认：在标准制定过程中，积极参与国际标准化组织的工作，推动中美欧等国家和地区在后量子密码标准方面的互认，确保中国的后量子密码技术能够在全球范围内推广应用。
- 产业化与应用：推动后量子密码标准在电子政务、金融、国防

和关键基础设施等领域的广泛应用，提升国家整体网络安全水平。

中国的后量子密码标准化进程虽然尚未正式启动，但通过一系列的前瞻性研究、算法竞赛和技术立项，已经为未来的标准化工作奠定了坚实的基础。随着国家层面的政策支持和国际合作的深化，中国有望在未来的量子计算时代，通过标准化进程进一步巩固其信息安全保障能力。这不仅将推动中国在后量子密码领域的技术领先地位，还将为全球后量子密码学的发展做出积极贡献。

2. 企业应该如何开展迁移工作

企业在推进后量子密码落地应用的过程中，需聚焦四大核心领域协同发力，分别为推动行业 PQC 应用标准化、加速 PQC 技术从理论向实践转化、构建企业自身 PQC 能力体系、助力客户完成 PQC 迁移过渡，以此为全球密码体系升级提供系统性支撑。

（1） 推动行业 PQC 应用的标准化

行业 PQC 应用标准化是后量子密码体系迁移进程的基石，其核心目标是通过统一技术规范保障全球范围内的互操作性与安全性。如 NIST 已发布系列算法标准为 PQC 技术提供核心支撑，例如 ML-KEM FIPS 203 用于密钥建立场景，ML-DSA FIPS 204 与 SLH-DSA FIPS 205 用于数字签名场景。这些标准不仅明确了核心技术构建模块，更定义了精细化的参数选择策略，如 ML-KEM-768 与 ML-DSA-65 适用于通用场景的均衡配置，小参数集适配资源受限设备，大参数集则针对高价值数据的长期保护需求。

在协议层面，互联网工程任务组（IETF）正牵头推进 TLS、IPsec 等主流协议的更新工作，预计 2027 年完成标准化，确保 PQC 算法可无缝集成至现有加密框架。其他标准制定组织（SDOs）如 FIDO 联盟、X.509 公钥基础设施（PKI）及 6G 通信协议机构也已启动相关适配工作，但受限于 WebPKI 等领域的分散性特征，工业控制系统协议等特定领域的标准化进程可能面临延迟。

标准化推进过程中需严格规避草案版本依赖，仅基于最终标准实现（如 NIST SP 800-208 中定义的 LMS/XMSS 用于固件签名），以此降低安全风险并保障生态系统一致性。这一标准化体系为行业提供了清晰的技术蓝图，推动全球供应商与监管机构在迁移路径上形成协同对齐。

（2）推动 PQC 应用由理论进入实践

PQC 技术正从理论研究阶段加速向实际应用落地转化，需通过明确迁移时间线、推进产品开发与优化实施策略实现规模化落地。若参考 NIST 的 2035 年时间节点，企业需在 2028 年前完成系统全面发现与评估（识别依赖加密技术的服务、资产及供应商），并制定初始迁移路线图；2031 年前聚焦高优先级任务执行（如关键资产加密升级、基础设施优化）；最终于 2035 年完成全体系迁移。

在产品生态层面，PQC 技术成熟度持续提升：主流浏览器（如 Chrome）已开始支持混合 PQC/TLS 密钥交换机制（尽管相关技术规范尚未完成标准化）；硬件安全模块（HSMs）及安全启动解决方案预计 2025 年实现商业化落地，并计划通过硬件加速技术提升运

行效率（2026-2027 年完成性能优化）。当前行业普遍采用 PQC/传统密码混合方案作为过渡措施，以保障互操作性与安全回退能力。但需明确此为临时方案，最终目标是实现纯 PQC 技术部署。

实践落地过程中需重点应对三大挑战：一是协议兼容性问题（例如工业控制系统（ICS）设备仍依赖老旧协议）；二是测试验证体系不完善（需建立全流程验证机制，确保密码配置准确性，规避回退漏洞）；三是迭代部署周期长（需通过多轮测试验证降低实施风险）。企业应将 PQC 迁移作为系统架构优化的契机，精简冗余架构、降低遗留系统风险，确保 ML-DSA 等理论算法在实际系统中实现高效稳定运行。

（3）构建企业自身的 PQC 能力

构建企业自身 PQC 能力体系是迁移工作的核心支撑。需通过内部评估、策略制定与资源投入的系统性整合，全面提升企业网络韧性。其关键建设阶段包括三大环节：一是明确迁移目标（重点提升密码基础设施健壮性与业务连续性保障能力）；二是执行全维度资产发现（覆盖服务类型、数据流路径、硬件依赖关系及供应商生态）；三是制定差异化迁移策略（如就地升级、平台重构或风险容忍策略）。

针对定制化 IT 或运营技术（OT）系统的企业，需结合场景特性自主选择适配算法（如资源受限设备优先采用 SLH-DSA 算法）；同步规划预算与系统更新周期的协同机制，确保资源投入合理性。能力建设需深度融合风险管理理念，具体包括：量化资产规模（涵盖服务器、物联网（IoT）设备等全类型资产）；建立遗留系统专项处置

机制（针对无法升级的 OT 设备制定风险隔离方案）；构建加密技术柔性适配能力（支持算法快速切换与版本迭代）。

PQC 能力建设需深度嵌入企业网络治理框架，通过强化资产管理、供应链监控等基础环节，确保 PKI 升级等迁移动作不引入新风险。组织应借此契机强化整体网络韧性，通过“PQC 客户端覆盖率”等量化指标追踪建设进度，确保 2028 年前完成初始能力规划，为长达 10 年的迁移周期奠定坚实基础。

（4）帮助客户向 PQC 的过渡

助力客户向 PQC 迁移过渡需聚焦供应链协同与客户支持策略优化，确保迁移过程平滑可控、业务中断最小化。针对不同类型客户需采取差异化支持方案：中小型企业主要通过供应商提供的商品化 IT 组件更新（如操作系统、浏览器等）实现无缝迁移；大型组织及关键基础设施运营商则需强化供应商依赖管理（如云服务提供商的 PQC 兼容性升级进度），通过明确需求传递推动供应商加速适配工作。

系统所有者需主动向客户与利益相关者发布迁移意图声明（包含时间线、目标与实施路径），强化信任传递；针对定制化系统客户（如专有通信系统用户），需提供专属评估服务，协助识别技术更新选项。客户支持体系需重点强化业务连续性保障措施（包括回滚机制、故障容忍设计等），并结合客户场景特性制定定制化方案：面向互联网服务领域（如金融、电信）可推动全球统一迁移节奏；针对物理基础设施客户（如工业控制系统用户）则需协调维护窗口，降低生产中断风

险。

企业应积极参与行业论坛分享最佳实践，同时确保专业咨询资源可及性，通过监管机构联动等渠道协助客户解决传感器升级等具体问题。通过全生态协同，推动行业整体于 2035 年完成 PQC 全面迁移，构建后量子时代的安全保障体系。

3. 政府应发挥的作用

在抗量子密码算法（PQC）的迁移进程中，政府发挥着极为关键的引导与协调作用。

一方面，政府应充分运用财政补贴、税收优惠以及政府采购等政策工具，积极激励企业和各类机构加快推进 PQC 技术的应用步伐。同时，大力推动建立完善的 PQC 产品认证体系，强化供应链安全审查机制，切实保障关键领域的信息安全与可控性。具体而言，可将 PQC 纳入国家级信息安全专项范畴，设立专门的专项资金，用以支持 PQC 的基础研究、产业化落地以及人才培养等方面的工作，从而构建起覆盖“标准—研发—应用”全流程的坚实支撑体系，为 PQC 技术的广泛推广提供全面而系统的保障。

另一方面，政府需着力促进跨行业的协同合作。由行业协会发挥牵头作用，联合高校、科研机构以及龙头企业等各方力量，共同制定行业层面的 PQC 应用指南和最佳实践方案，以加速 PQC 技术在实际场景中的落地应用。此外，加强 PQC 领域的人才培养也是至关重要的一环。政府应积极推动高校开设相关专业课程，为相关专业的学生提供系统的理论学习机会；同时，大力支持在职人员参加专业培

训，提升技术人员对 PQC 新标准的理解深度和实际实施能力，打造一支具备实战经验和专业素养的高素质专业队伍，为 PQC 的广泛应用提供坚实的人力支撑。

总之，政府在 PQC 迁移过程中的作用是全方位且多层次的。通过有效的政策激励、紧密的行业协作以及持续的教育投资，确保 PQC 技术能够顺利实现从研发到产业化的高效过渡，最终全面提升国家信息安全的整体水平，为国家的信息安全和数字化发展筑牢坚实的技术根基。

（四）中国联通的后量子密码布局与规划

作为国家通信基础设施建设国家队，中国联通向 PQC 的迁移不仅仅是技术升级，更是一项战略性任务。其网络中传输和存储着海量的敏感数据，从用户通信到关键基础设施控制，这些数据都可能面临未来量子攻击的威胁。主动部署 PQC 能够确保数据的长期保密性、完整性和真实性，在量子威胁环境中维护信任并符合监管要求。这对于国家安全、金融交易和关键基础设施的保护尤为重要 。

尽管量子计算目前仍处于早期发展阶段，但其快速进步使得“密码敏捷性”成为必要。所谓的“先收集后解密”威胁，即现在收集加密数据，待未来量子计算机足够强大时再进行解密，使得 PQC 的部署变得刻不容缓 。中国联通认识到，对于处理敏感且生命周期较长的数据（例如金融记录、政府通信）的电信运营商而言，在功能完备的量子计算机出现后才采取对策，将使大量已收集的数据面临未来解

密的风险。中国联通在 PQC 标准化和开发方面的早期参与，与 QKD 的努力相结合，表明公司已做出战略决策，旨在领先于“量子危机”而非被动应对。这种前瞻性的立场对于长期维护数据完整性和客户信任至关重要。这表明中国联通认识到大型网络密码转换所需的漫长周期，并旨在减轻未来的风险，而不是应对危机。这将其定位为一家具有前瞻性思维的安全服务提供商，在日益注重安全性的市场中，这可以成为重要的竞争优势。

中国联通的策略明确指出将“QKD+PQC 技术并举”，并在其网络中实现“量子经典深度融合”。通过整合这两种技术，中国联通旨在构建一个更健壮、更通用、更具弹性的量子安全解决方案，通过结合最高级别的密钥安全性与广泛的适用性，可能获得竞争优势。这也为单一技术长期可行性的不确定性提供了对冲。

中国联通多年来一直积极参与量子通信的研究和试验。这包括参与京雄量子干线试验网，以及研发基于 QKD 和 PQC 技术的“通密一体”量子融合通信设备 。联通已开发了量子密钥云平台，这对于支持量子安全加密服务至关重要 。其研究院和智研院均已研发出此类平台，并计划将其与联通云结合，提供量子加密云服务。

图 6-1 中国联通四位一体量子内生服务系统

中国联通的 PQC 规划并非孤立的技术升级，而是系统性地融入“云、网、端、管”四个层面，目标是让量子安全能力像血液一样流淌在整个网络体系中，成为与生俱来的基础能力。在产品开发和试验方面，中国联通取得了初步进展：

量子融合通话： 市场部牵头开发量子融合通话产品，该产品已完成商用局业务测试，并已开展内部试用，该产品旨在提供量子安全的语音通信。

PQC 加密手机： 科创部牵头与合作伙伴签订战略合作协议，并通过政企部推进 PQC 加密手机的开发。该产品于 25 年 5 月对外发布，体现了联通在终端设备安全方面的研究进展。

统一管控平台：联通正在开展量子与传统通信的统一管控研发，“通密一体”设备的统一管控平台已初步完成，并根据新产品开发持续迭代完善。

在网络集成方面，联通研究院已完成“通密一体”QKD 融合光

通信设备的研发，以及 PQC 融合光通信设备的开发。目前正在现网中开展示范“通密一体”设备示范，以形成量子专线业务。这标志着将量子安全直接集成到网络基础设施的实质性进展。

开放共赢构建“产学研”一体化生态：中国联通深知单打独斗无法赢得未来。公司正积极构建开放的“产学研”量子战队，联合顶尖高校、科研院所和产业链合作伙伴，共同推动技术突破、产品商业化和产业孵化，形成创新合力。

七、结论

后量子密码是应对量子计算威胁、保障数字社会长期安全的核心技术基础。本白皮书通过多维度分析，明确了以下关键结论与行动方向：

1. 技术标准化是产业化基石

NIST、欧盟及中国在后量子密码标准化领域的差异与协同，决定了全球密码体系的演进方向。中国需加速推进自主算法的标准化进程，同时积极参与国际标准互认，构建“自主可控+开放兼容”的技术生态。当前，基于模格的密码算法（如 Kyber、Dilithium）因其性能与安全性平衡，已成为国际主流选择，但需进一步优化硬件实现效率，降低资源消耗，以适配物联网、边缘计算等低功耗场景。

2. 产业协同是规模落地的关键

后量子密码的产业化需突破“算法-芯片-协议-系统”的全链条协同瓶颈。国内企业已在抗量子芯片、开源密码库及通信服务集成（如

联通光网络方案）等领域取得突破，但需加强产业链上下游联动，推动算法、硬件、协议与应用场景的深度适配。金融、政务、能源等关键基础设施行业应率先开展试点，形成可复用的迁移模板，带动全行业技术升级。

3. 密码敏捷性是动态防御的核心能力

量子安全威胁的长期性与不确定性要求密码体系具备动态演化能力。密码敏捷性通过算法可替换、密钥可轮换及协议可扩展机制，为后量子迁移提供了灵活路径。企业需构建覆盖算法选型、资产盘点、风险评估、策略执行的全生命周期管理体系，以应对技术迭代与攻击演进的双重挑战。

4. 政策与生态共建是战略保障

政府需通过立法与标准引导，明确 PQC 迁移的时间表与合规要求，推动公钥基础设施（PKI）的量子安全升级。同时，需建立跨行业协作平台，联合科研机构、头部企业与国际组织，形成技术攻关、测试验证、人才培育的闭环生态。中国应发挥“技术+市场”双轮驱动优势，在标准制定、芯片研发、场景验证等领域实现从“跟随者”向“引领者”的角色转变。

5. 未来展望：从技术储备到产业引领

未来 5-10 年，后量子密码将经历从“实验室验证”到“规模化商用”的跃迁。中国需把握技术窗口期，聚焦三大方向：

算法工程化：攻克低功耗设备的高性能实现难题，推动抗侧信道攻击技术与轻量化设计的融合；

标准国际化：基于国产密码体系（如 Scloud+、Aigis 等）探索差异化路径，增强国际话语权；

产业生态化：通过“密码+”模式（如隐私计算、物联网安全），拓展 PQC 在新兴场景的应用边界，构建“算法-芯片-系统-服务”的全栈能力。

后量子密码的迁移不仅是技术革命，更是国家安全与数字经济竞争力的战略抉择。唯有以技术自主、标准主导与产业协同为支点，方能筑牢量子时代的数字安全基座，为全球密码学演进贡献“中国方案”。

参考文献

[1] NIST. Migration to post-quantum cryptography quantum readiness: Testing draft standards: [S]. U.S. Department of Commerce, 2023:

[2] SHANNON C E. Communication theory of secrecy systems [J]. The Bell system technical journal, 1949, 28(4): 656－715.

[3] GRASSL M, LANGENBERG B, ROETTELER M, et al. Applying Grover's algorithm to AES: quantum resource estimates; proceedings of the International Workshop on Post-Quantum Cryptography, F, 2016 [C]. Springer.

[4] SCHROTTENLOHER A. Quantum algorithms for cryptanalysis and quantum-safe symmetric cryptography [D]; Sorbonne université, 2021.

[5] SHOR P W. Algorithms for quantum computation: discrete logarithms and factoring; proceedings of the Proceedings 35th annual symposium on foundations of computer science, F, 1994 [C]. Ieee.

[6] SHARMA S, TRIPATHI M, SAHU H K, et al. A Post-Quantum End-to-End Encryption Protocol; proceedings of the 2023 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), F, 2023 [C]. IEEE.

[7] 西电广研院. 后量子密码迁移白皮书 [Z]. 2024

[8] LYUBASHEVSKY V, PEIKERT C, REGEV O. On ideal lattices and learning with errors over rings; proceedings of the Annual international conference on the theory and applications of cryptographic techniques, F, 2010 [C]. Springer.

[9] MCELIECE R J. A public-key cryptosystem based on algebraic [J]. Coding Thv, 1978, 4244(1978): 114 - 6.

[10] BECKER G. Merkle signature schemes, merkle trees and their cryptanalysis [J]. Ruhr-University Bochum, Tech Rep, 2008, 12: 19.

[11] JAO D, DE FEO L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies; proceedings of the International workshop on post-quantum cryptography, F, 2011 [C]. Springer.

[12] KITAEV A Y. Quantum measurements and the Erlang algorithm [J]. Journal of Experimental and Theoretical Physics, 2002.

[13] AI G Q. Post-Quantum Cryptography: Current Research [Z]. 2021

[14] SURVEYS A C. Evaluating the Performance of Post-Quantum Cryptography [Z]. 2022

[15] ECRYPT. Performance Comparison of Post-Quantum Cryptographic Algorithms [Z]. 2021

[16] NIST. Post-Quantum Cryptography Standardization [Z]. 2022

[17] VISA. Adopting Post-Quantum Cryptography [Z]. 2022

[18] IBM. Accelerating Post-Quantum Development [Z]. 2023

[19] YAMAN F, MERT A C, ÖZTüRK E, et al. A hardware accelerator for polynomial multiplication operation of CRYSTALS-KYBER PQC scheme; proceedings of the 2021 Design, Automation & Test in Europe Conference & Exhibition (DATE), F, 2021 [C]. IEEE.

[20] ALHASSANI A, BENAISSA M. High-speed polynomials multiplication HW accelerator for CRYSTALS-Kyber [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2024.

[21] GUO W, LI S. Highly-efficient hardware architecture for CRYSTALS-Kyber with a novel conflict-free memory access pattern [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2023, 70(11): 4505 – 15.

[22] LI M, TIAN J, HU X, et al. Reconfigurable and high-efficiency polynomial multiplication accelerator for crystals-kyber [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2022, 42(8): 2540 – 51.

[23] XING Y, LI S. A compact hardware implementation of CCA-secure key exchange mechanism CRYSTALS-KYBER on FPGA [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021: 328 – 56.

[24] NGUYEN T-H, DAM D-T, DUONG P-P, et al. Efficient

hardware implementation of the lightweight CRYSTALS-Kyber [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2024.

[25] CUI Y, CHEN J, NI Z, et al. Instruction-Based High-Performance Hardware Controller of CRYSTALS-Kyber With Balanced Resource Utilization [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2025.

[26] ZHAO C, ZHANG N, WANG H, et al. A compact and high-performance hardware architecture for CRYSTALS-Dilithium [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022: 270 – 95.

[27] GUPTA N, JATI A, CHATTOPADHYAY A, et al. Lightweight hardware accelerator for post-quantum digital signature CRYSTALS-Dilithium [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2023, 70(8): 3234 – 43.

[28] LI X, LU J, LIU D, et al. A high speed post-quantum crypto-processor for crystals-dilithium [J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2023, 71(1): 435 – 9.

[29] ZHU Y, ZHU W, CHEN C, et al. Mckeycutter: A high-throughput key generator of classic mceliece on hardware; proceedings of the 2023 60th ACM/IEEE Design Automation Conference (DAC), F, 2023 [C]. IEEE.

[30] DESHPANDE S, XU C, NAWAN M, et al. Fast and efficient

hardware implementation of HQC; proceedings of the International Conference on Selected Areas in Cryptography, F, 2023 [C]. Springer.

[31] RICHTER-BROCKMANN J, CHEN M-S, GHOSH S, et al. Racing BIKE: Improved polynomial multiplication and inversion in hardware [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022: 557 – 88.

[32] THOMA J P, HARTLIEF D, GüNEYSU T. Agile acceleration of stateful hash-based signatures in hardware [J]. ACM Transactions on Embedded Computing Systems, 2024, 23(2): 1 – 29.

[33] CAO Y, WU Y, QIN L, et al. Area, time and energy efficient multicore hardware accelerators for extended merkle signature scheme [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2022, 69(12): 4908 – 18.

[34] MOHAN P, WANG W, JUNGK B, et al. ASIC accelerator in 28 nm for the post-quantum digital signature scheme XMSS; proceedings of the 2020 IEEE 38th International Conference on Computer Design (ICCD), F, 2020 [C]. IEEE.

[35] SAARINEN M-J O. Accelerating SLH-DSA by two orders of magnitude with a single hash unit; proceedings of the Annual International Cryptology Conference, F, 2024 [C]. Springer.

[36] AIKATA A, MERT A C, IMRAN M, et al. KaLi: A crystal for

post-quantum security using Kyber and Dilithium [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2022, 70(2): 747 – 58.

[37] LI Z, TANG J, LU Y. KDA: Kyber and Dilithium Accelerator for CRYSTALS Suite of Post-Quantum Cryptography in Hybrid Multipath Delay Commutator Pipelined Architecture; proceedings of the 2024 IEEE Asian Solid-State Circuits Conference (A-SSCC), F, 2024 [C]. IEEE.

[38] ZHU Y, ZHU W, ZHU M, et al. A 28nm 48KOPS 3.4 μJ/Op Agile Crypto-Processor for Post-Quantum Cryptography on Multi-Mathematical Problems; proceedings of the 2022 IEEE International Solid-State Circuits Conference (ISSCC), F, 2022 [C]. IEEE.

[39] ZHU Y, ZHU W, OUYANG Y, et al. 16.2 A 28nm 69.4 kOPS 4.4 μ J/Op Versatile Post-Quantum Crypto-Processor Across Multiple Mathematical Problems; proceedings of the 2024 IEEE International Solid-State Circuits Conference (ISSCC), F, 2024 [C]. IEEE.

[40] KANNWISCHER M J, RIJNEVELD J, SCHWABE P, et al. pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4 [J]. 2019.

[41] BOTROS L, KANNWISCHER M J, SCHWABE P. Memory-efficient high-speed implementation of Kyber on Cortex-M4; proceedings of the International Conference on Cryptology in Africa,

F, 2019 [C]. Springer.

[42] SEILER G. Faster AVX2 optimized NTT multiplication for Ring-LWE lattice cryptography [J]. Cryptology ePrint Archive, 2018.

[43] ALKIM E, BILGIN Y A, CENK M, et al. Cortex-M4 optimizations for {R, M} LWE schemes [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020: 336 – 57.

[44] GRECONICI D O, KANNWISCHER M J, SPRENKELS A. Compact dilithium implementations on Cortex-M3 and Cortex-M4 [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021: 1 – 24.

[45] ABDULRAHMAN A, HWANG V, KANNWISCHER M J, et al. Faster kyber and dilithium on the cortex-m4; proceedings of the International Conference on Applied Cryptography and Network Security, F, 2022 [C]. Springer.

[46] HUANG J, ZHANG J, ZHAO H, et al. Improved plantard arithmetic for lattice-based cryptography [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022, 2022(4): 614 – 36.

[47] HUANG J, ADOMNICĂI A, ZHANG J, et al. Revisiting keccak and dilithium implementations on armv7-m [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024, 2024(2): 1 – 24.

[48] HUANG J, ZHAO H, ZHANG J, et al. Yet another improvement of Plantard arithmetic for faster Kyber on low-end 32-bit IoT devices [J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 3800 – 13.

[49] HüLSING A, RIJNEVELD J, SCHWABE P. Armed sphincs: Computing a 41 kb signature in 16 kb of ram; proceedings of the Public-Key Cryptography – PKC 2016: 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I, F, 2016 [C]. Springer.

[50] BOS J W, RENES J, SPRENKELS A. Dilithium for memory constrained devices; proceedings of the International Conference on Cryptology in Africa, F, 2022 [C]. Springer.

[51] NGUYEN D T, GAJ K. Fast NEON-based multiplication for lattice-based NIST post-quantum cryptography finalists; proceedings of the International conference on post-quantum cryptography, F, 2021 [C]. Springer.

[52] SANAL P, KARAGOZ E, SEO H, et al. Kyber on ARM64: Compact implementations of Kyber on 64-bit ARM Cortex-A processors; proceedings of the International conference on security and privacy in communication systems, F, 2021 [C]. Springer.

[53] BECKER H, HWANG V, KANNWISCHER M J, et al. Neon ntt:

Faster dilithium, kyber, and saber on cortex-a72 and apple m1 [J]. Cryptology ePrint Archive, 2021.

[54] BECKER H, KANNWISCHER M J. Hybrid scalar/vector implementations of Keccak and SPHINCS+ on AArch64; proceedings of the International Conference on Cryptology in India, F, 2022 [C]. Springer.

[55] KIM Y, SONG J, SEO S C. Accelerating falcon on ARMv8 [J]. IEEE Access, 2022, 10: 44446 - 60.

[56] KIM Y, SONG J, YOUN T-Y, et al. Crystals - Dilithium on ARMv8 [J]. Security and Communication Networks, 2022, 2022(1): 5226390.

[57] KIM Y, YOON S, SEO S C. Vectorized implementation of Kyber and Dilithium on 32-bit Cortex-A series [J]. IEEE Access, 2024.

[58] NGUYEN D T, GAJ K. Fast falcon signature generation and verification using armv8 neon instructions; proceedings of the International Conference on Cryptology in Africa, F, 2023 [C]. Springer.

[59] FRITZMANN T, SCHAMBERGER T, FRISCH C, et al. Efficient hardware/software co-design for NTRU; proceedings of the IFIP/IEEE International Conference on Very Large Scale Integration-System on a Chip, F, 2018 [C]. Springer.

[60] BANERJEE U, UKYAB T S, CHANDRAKASAN A P. Sapphire: A

configurable crypto-processor for post-quantum lattice-based protocols [J]. arXiv preprint arXiv:191007557, 2019.

[61] FRITZMANN T, SIGL G, SEPúLVEDA J. Extending the RISC-V instruction set for hardware acceleration of the post-quantum scheme LAC; proceedings of the 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), F, 2020 [C]. IEEE.

[62] ALKIM E, EVKAN H, LAHR N, et al. ISA Extensions for Finite Field Arithmetic Accelerating Kyber and NewHope on RISC-V [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020, 2020(3): 219 – 42.

[63] FRITZMANN T, SIGL G, SEPúLVEDA J. RISQ-V: Tightly coupled RISC-V accelerators for post-quantum cryptography [J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020: 239 – 80.

[64] XIN G, HAN J, YIN T, et al. VPQC: A domain-specific vector processor for post-quantum cryptography based on RISC-V architecture [J]. IEEE transactions on circuits and systems I: regular papers, 2020, 67(8): 2672 – 84.

[65] ZHAO Y, XIE R, XIN G, et al. A high-performance domain-specific processor with matrix extension of RISC-V for module-LWE applications [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2022, 69(7): 2871 – 84.

[66] NANNIPIERI P, DI MATTEO S, ZULBERTI L, et al. A RISC-V post quantum cryptography instruction set extension for number theoretic transform to speed-up CRYSTALS algorithms [J]. IEEE Access, 2021, 9: 150798 – 808.

[67] KARL P, SCHUPP J, FRITZMANN T, et al. Post-quantum signatures on RISC-V with hardware acceleration [J]. ACM Transactions on Embedded Computing Systems, 2024, 23(2): 1 – 23.

[68] MITELOUDI K, BOS J W, BRONCHAIN O, et al. PQ. v. ALU. e: Post-quantum RISC-v custom ALU extensions on dilithium and kyber; proceedings of the International Conference on Smart Card Research and Advanced Applications, F, 2023 [C]. Springer.

[69] LOPEZ-VALDIVIESO J, CUMPLIDO R. Design and implementation of hardware-software architecture based on hashes for SPHINCS+ [J]. ACM Transactions on Reconfigurable Technology and Systems, 2024, 17(4): 1 – 22.

[70] ZHANG D, BAI G. Ultra high-performance ASIC implementation of SM2 with power-analysis resistance; proceedings of the 2015 IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC), F, 2015 [C]. IEEE.

[71] ZEGHID M, AHMED H Y, CHEHRI A, et al. Speed/area-efficient ECC processor implementation over GF (2 m) on FPGA via novel algorithm-architecture co-design [J]. IEEE

Transactions on Very Large Scale Integration (VLSI) Systems, 2023, 31(8): 1192－203.

[72] HARB S, JARRAH M. FPGA implementation of the ECC over GF (2m) for small embedded applications [J]. ACM Transactions on Embedded Computing Systems (TECS), 2019, 18(2): 1－19.

[73] TIAN J, WEI Y, XU D, et al. Fast Scloud+: A Fast Hardware Implementation for the Unstructured LWE-based KEM-Scloud+ [J]. Cryptology ePrint Archive, 2025.

[74] 董海春 左 张. 贯彻全国两会精神丨鄂产车规级芯片获功能安全流程最高认证汽车将装上自主“中国脑” [N]. 2024－03－18-.

[75] 中国联通研究院. 中国联通展示“通密一体”量子通信融合设备 [N]. 2024－07－19-.

[76] S W B W P M. Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms [R]: the National Cybersecurity Center of Excellence（NCCoE）, 2021.

中国联通研究院根植于联通集团（中国联通直属二级机构），作为中国联通科技创新专业子公司，自2022年起，挂牌成立中国网络安全研究院、下一代互联网宽带业务应用国家工程研究中心及首个国家级网络安全产业知识产权运营中心，形成“两院两中心”发展格局，开创了研究院高质量发展的新局面。

中国联通研究院作为服务于国家战略、行业发展、企业生产的战略决策参谋者、技术发展的引领者、产业发展的助推者，坚持以高水平科技自立自强为使命担当，聚焦网络强国、数字中国主责，拓展联网通信、算网数智业务，形成“态度、速度、气度、有情怀、有格局、有担当”的企业文化，以下一代互联网、光网络、5G-A/6G、网络安全、数智网优、低空智能网联和新型智库研究七个领域为主攻方向，坚持“四个聚焦”，开展关键核心技术攻关、科创力量建设、专业技术人才队伍建设、创新成果转化等工作，着力实现价值创造提升、战略科技力量提升、专精特新能力成色提升，争做通信行业科技创新主力军，努力建设成为“国家信赖、行业领先、集团倚重、员工自豪”现代化一流研究院。

战略决策的参谋者
技术发展的引领者
产业发展的助推者

态度、速度、气度

有情怀、有格局、有担当

中国联合网络通信有限公司研究院
地址：北京市亦庄经济技术开发区北环东路1号
电话：010-87926100
邮编：100176