全球抗量子迁移战略白皮书

(2025)

跨越量子鸿沟：以战略引擎驱动全球抗量子迁移

2025 年 12 月

文档历史

版本	日期	描述
1.0.0	2025 年 12 月	2025 年首次发布。
1.0.1	2025 年 12 月	修改了一些措辞。

参与单位

西交利物浦大学后量子迁移交叉实验室（PQC-X）
重庆大学信息物理社会可信服务计算教育部重点实验室（CPS-DSC）
云钞金融服务（北京）有限公司
苏州国芯科技股份有限公司
苏州朗空后量子科技有限公司（朗空量子）
上海巡天千河空间技术有限公司

指导委员会

丁津泰 教授
西交利物浦大学数学物理学院 院长
西交利物浦大学后量子迁移交叉实验室（PQC-X）主任
NIST PQC 标准核心设计者

向宏 教授
重庆大学信息物理社会可信服务计算教育部重点实验室（CPS-DSC） 副主任

郑茳 教授
苏州国芯科技股份有限公司 董事长

编写人员

刘锐
西交利物浦大学后量子迁移交叉实验室（PQC-X）客座教授/副主任
苏州朗空后量子科技有限公司（朗空量子）董事长/CEO

曾能
西交利物浦大学后量子迁移交叉实验室（PQC-X）助理教授

法律声明与免责条款

版权声明

免责声明

1. **信息性质：** 本白皮书所载内容仅供参考，旨在提供抗量子密码（PQC）迁移的战略框架与技术指引，不构成任何形式的法律、金融投资或技术实施的最终建议。

2. **准确性：** 尽管编写团队已尽力确保文中数据（如量子比特需求预测、市场规模预测）的准确性，但鉴于量子技术发展的快速迭代特性，我们不对信息的绝对准确性、完整性或时效性承担法律责任。

3. **风险提示：** 报告中提及的技术方案（如混合模式、加密资产发现）应结合各组织实际情况进行评估。对于因使用本报告信息而产生的任何直接或间接损失，参与单位、指导委员会、编写单位、编写人员不承担责任。

目　录

致决策者：跨越量子鸿沟的战略呼吁

跨越量子鸿沟：将一项生存威胁转化为战略机遇

核心风险：一场已经开始的“数据劫持”

我们数字世界的安全基石——以 RSA 和 ECC 为代表的公钥加密体系——正面临一场根本性的颠覆。能够破解这些体系的量子计算机，其出现并非遥远的理论，而是一个正在加速逼近的技术临界点。

然而，最大的威胁并非未来的某个攻击“事件”，而是一种已经存在且持续发生的当下风险：即“先窃取，后破解”（Harvest Now, Decrypt Later, HNDL）攻击。全球范围内的对手方正在大规模拦截和存储我们今天加密的数据，耐心等待未来量子计算机问世后再行破解。这意味着，对于任何需要长期保密的高价值数据——核心知识产权、长期金融合同、国家机密、个人隐私数据——其安全漏洞实际上已经存在。

推迟行动并非零成本决策，它是在持续积累一笔危险的“量子安全债务”。一旦量子计算机就绪，这笔债务的偿还将是灾难性的，可能导致知识 产权永久性损失、巨额监管罚款和品牌声誉的彻底崩塌。

战略对策：启动“量子安全迁移战略引擎”

面对这一复杂挑战，一次简单的算法替换或一个线性的项目制迁移是远远不够的。本白皮书提出了一个权威且可执行的全新战略框架——量子安全迁移战略引擎。

这是一个动态的、自我增强的生命周期模型，旨在将抗量子密码（PQC）迁移从一个被动的成本中心，转变为构建组织长期韧性的战略能力。其核心原则是“密码敏捷性” (Crypto-Agility)[23]，即构建一个能够灵活适应未来标准演进和未知威胁的弹性技术架构。随着美国（2035 年前禁用第一代公钥密码标准）、欧盟（2030 年前关键基础设施完成迁移）[24] 等全球主要经济体纷纷设定强制性迁移时间表，PQC 迁移已不再是一个选项，而是一项有明确截止日期的紧迫任务。

立即行动：“无悔之举”与您的首要任务

犹豫和观望的窗口期已经关闭。我们强烈建议您立即授权并投入资源，启动被广泛认为是“无悔之举”(No-Regret Moves) [25] 的初始步骤。

这些行动无论量子威胁何时到来，都能极大提升组织当前的安全可见性与管理能力，也是提升整体“密码学成熟度”的契机。您的首要任务是：立即启动一次全面的企业级加密资产盘点和量子风险评估。您无法保护您所不知道的资产。这项工作将为您的迁移引擎提供数据驱动的点火能量，将模糊的风险转化为具体的、可量化的风险规避行动路线图。

从风险到机遇：投资于未来的竞争力

PQC 迁移不仅是一项防御性开销，更是一项对企业未来数字信任和市场竞争力的战略投资。率先完成迁移的企业，能够将其作为一项强大的竞争优势，在赢得高端合同、客户忠诚度和供应链准入方面占得先机。

更具决定性的是，支撑 PQC 主流标准之一的数学基础——格密码，与下一代隐私保护计算的“圣杯”——全同态加密（FHE）——完全一致。这一深刻的数学关联，将一项由合规驱动的防御性成本，彻底转变为一项赋能未来商业创新的主动性战略投资。您今天为 PQC 迁移所做的每一分投入，都是在为部署下一代安全 AI 应用所需的基础设施进行预投资，从而构建起决定性的未来市场竞争力。

战略行动的时刻，就是现在。必须立即启动您组织的迁移引擎，以确保在未来量子时代的生存与竞争力。

摘　要

数字世界的安全基石正面临一场根本性的颠覆。量子计算的崛起并非遥远的理论，而是一个正在加速成为现实的技术临界点，它将使当前保护全球通信、商业和国家安全的加密标准（如 RSA 和 ECC）彻底失效。量子计算对传统公钥密码体系的根本性威胁，正以前所未有的力量，推动密码学市场从“一维”向技术多元化、场景泛化性、生态动态化的“三维”深刻演变。

然而，一个基于线性思维的威胁时间点预测已不再适用。本白皮书旨在阐明，量子威胁不仅是未来的事件，更是一种以“先窃取，后破解”（Harvest Now, Decrypt Later, HNDL）形式存在的当下风险，它要求我们立即采取持续性的应对策略。近期行业报告显示，企业高管层对这一威胁的认知已成主流，例如，凯捷咨询的 2025 年研究表明，65%[1]的组织对 HNDL 攻击的兴起感到担忧。泰雷兹同期报告也印证了这一趋势，指出 58%[2] 的组织将“未来对今日数据的解密”视为主要的量子安全威胁。

面对这一挑战，一次简单的算法替换或一个线性的、基于项目的迁移方法是远远不够的。向后量子密码（Post-Quantum Cryptography, PQC）的过渡，本质上是一次对组织整体信息安全态势的全面升级，其最终目标是达到一种可持续的“密码学成熟度”（Cryptographic Maturity）状态。本白皮书因此提出了一个权威且可执行的全新战略框架——量子安全迁移战略引擎。这是一个自增强的生命周期模型，旨在为组织机构实现并维持长期的量子韧性提供明确的路径。

威胁的本质正在演变。一方面，新兴量子技术（如表面码、猫量子比特（Cat Qubits）[9]）的组合效益正在急剧压缩威胁时间线。另一方面，我们面临着量子与经典风险并存的“双重威胁”：未来量子计算机将破解算法的数学基础，而当下人工智能驱动的密码分析工具正自动化地攻击算法的工程实现。与此同时，量子计算即服务（Quantum Computing as a Service, QaaS）的兴起，正从经济上普及量子攻击的能力，使其不再是少数国家级行为体的专属工具。

量子安全迁移战略引擎框架正是为应对这种动态、持续的威胁而设计。它由五个相互关联、相互促进的阶段构成，其可行性得到了全球领先实践的印证，例如美国国家标准与技术研究院（National Institute of Standards and Technology, NIST）下属的国家网络安全卓越中心（National Cybersecurity Center of Excellence, NCCoE）所组织的迁移项目，其工作模式与本框架高度吻合。

核心原则（引擎底座）： 密码敏捷性[23]设计
初始动力（点火启动）： 战略远见与风险情报
构建动能（动力总成）： 抗量子密码技术堆栈
加速引擎（涡轮增压）： 仿真与验证模块
维持动能（智能调控）： 治理与演进循环

成功的抗量子迁移离不开一个成熟、完整的解决方案生态系统。本白皮书的发布联盟——由西交利物浦大学后量子迁移交叉实验室（PQC-X）、苏州朗空后量子科技有限公司（朗空量子）及其合作伙伴（重庆大学信息物理社会可信服务计算教育部重点实验室（CPS-DSC）、云钞金融服务（北京）有限公司、苏州国芯科技股份有限公司、上海巡天千河空间技术有限公司等）组成——恰恰代表了这样一个能够为引擎的每一个冲程/模块提供动力的、从基础研究到全栈产品和服务的完整生态链。

我们正站在跨越量子鸿沟的边缘。对于全球的决策者、企业领袖和技术专家而言，犹豫和观望的窗口期已经关闭。现在必须启动各自的迁移引擎，以确保组织在未来量子时代的生存与竞争力。战略行动的时刻，就是现在。

第一章

解构数字信任：从恩尼格玛到跨越量子鸿沟

第一章 解构数字信任：从恩尼格玛到跨越量子鸿沟

本部分旨在为后量子（PQC）迁移的紧迫性建立完整的历史与技术背景。报告将论证，“跨越量子鸿沟”并非孤立事件，而是密码学漫长演进与失效历史的必然高潮，这使得我们必须采取合乎逻辑的紧急行动。

1.1 恩尼格玛的先声：密码学失效的永恒教训

要理解当今的量子威胁，我们必须首先回顾历史。第二次世界大战中德军使用的恩尼格玛（Enigma）密码机的故事，不仅是一段引人入胜的战争传奇，更是一部关于密码系统脆弱性的深刻教科书，为今日的后量子密码战略提供了基础案例研究。

1.1.1 对称密码时代的巅峰：机械加密的黄金时代

在现代公钥密码学诞生之前，世界长期处于对称密码的时代。在这种体系中，信息的发送方和接收方必须共享同一个密钥，才能进行加密和解密。从古罗马的凯撒密码到 20 世纪初，这一基本范式始终未变。由德国工程师亚瑟·谢尔比乌斯（Arthur Scherbius）发明的恩尼格玛密码机，正是这一时代机械加密技术的巅峰之作。它通过一系列可配置的转子、插接板和反射板，实现了一种极其复杂的复式字母替换密码。其理论上的密钥空间组合数量高达天文数字，这使得它在当时被普遍认为是无法破解的。

1.1.2 波兰的先驱与布莱切利园的工业化破译：密码学的转折点

然而，恩尼格玛的“不败神话”最早被一群常被历史忽视的英雄所打破——波兰密码局的数学家们。早在 1932 年，由马里安·雷耶夫斯基（Marian Rejewski）领导，并与耶日·鲁日茨基（Jerzy Różycki）和亨里克·佐加尔斯基（Henryk Zygalski）紧密合作的团队，就首次运用严谨的数学群论，成功破解了早期版本的恩尼格玛。他们的成功是数学天赋与法国情报部门从德国间谍汉斯-蒂洛·施密特（Hans-Thilo Schmidt）处获得的关键情报相结合的成果。在 1939 年 7 月，波兰沦陷前夕，他们无私地与英法盟友分享了他们的研究成果、破译方法乃至复制的恩尼格玛样机，这一时刻对整个二战的进程至关重要。

英国布莱切利园（Bletchley Park）的传奇始于波兰人奠定的坚实基础，而艾伦·图灵（Alan Turing）与戈登·韦尔奇曼（Gordon Welchman）则完成了从理论到机械化的关键跨越，设计出了英国版“Bombe”机。然而，若论真正将破译工作推向极致的“工业化生产”与算力巅峰，则不得不提大洋彼岸美国的加入。

在英方设计的启发下，美国投入了强大的工业制造能力（如 NCR 公司），制造出了运行速度更快、稳定性更强、足以应对四转子系统的美国版 Bombe。正是这种“英方设计、美方量产”的跨大西洋合作，将原本的手工与半自动化破译转变为真正的大规模流水线作业，极大地缩短了每日密钥的破译时间，从而最终实现了对德军海量密电的规模化解读。

1.1.3 失败的剖析:密码系统的致命弱点并非源于数学

恩尼格玛的崩溃并非源于其核心加密算法的数学理论被攻破，而是源于一系列设计、操作和认知上的连锁失误。这为我们提供了关于现实世界密码安全最深刻的教训：

设计缺陷：反射板的设计确保了一个字母永远不会被加密成其自身。这个看似微小的特性，却为密码分析员提供了一个宝贵的统计学“后门”，极大地缩小了需要猜测的范围。

操作安全（OPSEC）的灾难：这才是恩尼格玛真正的“阿喀琉斯之踵”。德军操作员在日常使用中的疏忽和为了便捷而形成的固定习惯，制造了大量致命的模式。

重复加密消息密钥：在 1940 年之前，德军规定将三位字母的消息密钥用当日密钥加密两次后发送，以防传输错误。这一“为求保险”的措施反而成了“致命的弱点”，它使得雷耶夫斯基能够通过分析这两段本应相同但加密后不同的密文，分离出转子和插接板的效果，为最初的破译提供了决定性的切入点。

刻板的消息格式：大量电文使用固定的开头和结尾，如“Wetter”（天气预报）、固定的敬语或“无新消息”等。这些可预测的内容为盟军提供了所谓的“Cribs”（明文对照），即已知的明文片段，可以用来与截获的密文进行比对，从而快速验证密钥设置的正确性。

操作员的惰性：一些操作员为了省事，会使用诸如“AAA”或键盘对角线上的字母等懒人密钥。更有甚者，在设置每日新密钥后，直接使用默认的转子位置作为第一封电文的起始位置，而没有随机转动。布莱切利园的密码学家约翰·赫里维尔（John Herivel）敏锐地发现了这一模式，形成了著名的“赫里维尔窍门”（Herivel Tip），极大地减少了寻找转子初始位置的工作量。

组织的傲慢与偏见：尽管有迹象表明密码可能已被破译，但德军最高统帅部始终对恩尼格玛的安全性抱有绝对的信心，将盟军的成功归因于巧合、间谍活动或盟友的背叛，而不是密码系统本身的问题。这种制度性的傲慢，使他们未能及时修复那些致命的操作安全漏洞。

这段历史揭示了一个核心原则：现实世界的安全是一个环环相扣的链条，而最薄弱的环节往往不是深奥的数学理论，而是平庸的工程实现和人为失误。这与本白皮书中描述的“双重威胁”环境形成了惊人的历史呼应：当下的 AI 工具正在自动化地攻击密码

算法的工程实现，而未来的量子计算机则将攻击其数学基础。恩尼格玛的故事，正是这一理念的历史铁证。

此外，德军对恩尼格玛技术牢不可破的信念，直接导致了其在操作安全规程上的松懈，这为今天的组织敲响了警钟。如果一个组织仅仅因为迁移到了 NIST 批准的 PQC 算法就宣告“量子安全”，便可能陷入同样的自满情绪，忽视了持续的经典攻击威胁和 PQC 算法自身未来可能被发现的弱点。安全是一个持续警惕的过程，而非一次性的技术修复。这恰恰印证了白皮书中“战略引擎”模型所强调的持续治理与演进的重要性。

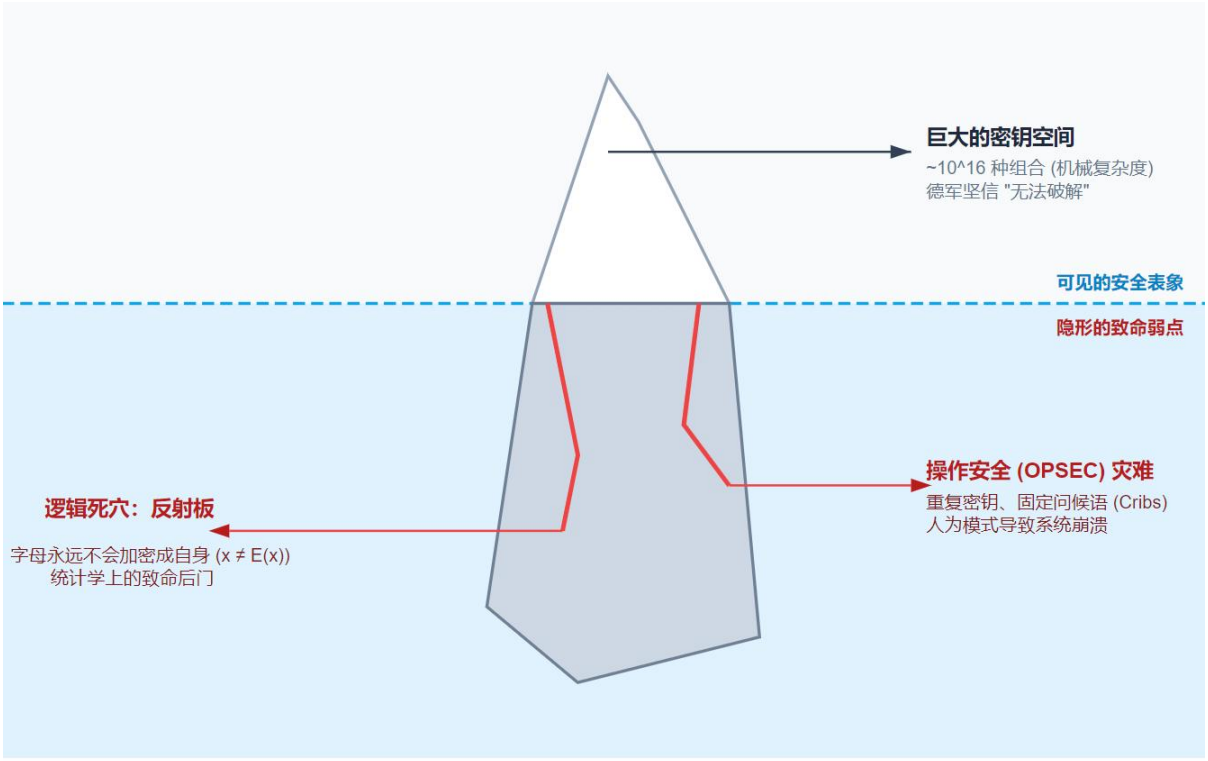
更具战略意义的是，“先窃取，后破解”（Harvest Now, Decrypt Later, HNDL）这一现代网络攻击模型，在恩尼格玛的破译史中早有先例。盟军截获并储存了海量的恩尼格玛密电，即便在暂时无法破译的时期也未曾中断。他们坚信，未来的某个突破——无论是获得新的“Crib”、缴获密码本，还是 Bombe 机的技术升级——终将解锁这些储存的信息。这与今天对手方窃取加密数据，耐心等待量子计算机问世后再行破解的战略逻辑如出一辙。恩尼格玛的故事，让 HNDL 这个抽象的现代威胁变得具体且有史可循。

恩尼格玛的故事并非孤例。一个更近代、甚至更令人不寒而栗的例子，是密码学信任在国家层面被秘密武器化的事件。在 1982 年的马岛战争[3-5]（福克兰战争）中，阿根廷军方依赖从声誉卓著的中立国瑞士公司 Crypto AG 购买的先进加密设备来保护其军事通信。他们相信这些设备是安全的。然而，事实是，这家公司自 1970 年起就已被美国中央情报局（CIA）和西德联邦情报局（BND）秘密收购。这些情报机构在销往全球（包括阿根廷）的加密机中植入了“后门”，使他们能够轻易解密客户的机密通讯。战争期间，美国正是利用这一秘密优势，读取了阿根廷的加密军事电文，并将关键情报分享给了英国，对战局产生了重大影响。更具讽刺意味的是，战后当阿根廷怀疑其密码系统遭破解时，Crypto AG 的代表成功说服他们，其主力设备仍然“牢不可破”，导致阿根廷继续使用这些已被攻破的系统。这个真实案例为我们提供了比恩尼格玛更直接的警示：

如果一个国家或组织掌握了破解主流密码的“万能钥匙”，他们绝对不会公之于众，而是会将其作为最高机密和最强大的战略武器来秘密使用。这使得“跨越量子鸿沟”的威胁变得不再是理论上的推测。一旦某个国家率先建成能够破解当前公钥密码体系的量子计算机，世界不会听到任何新闻发布。相反，全球的政府、企业和个人的加密数据都将可能在不被察觉的情况下被静默地解密。这正是抗量子迁移如此紧迫的根本原因——我们必须在对手的秘密武器形成战斗力之前，完成我们的防御升级。

恩尼格玛时代的漏洞	现代 PQC 的相似挑战	战略性缓解措施（引擎模块）
设计缺陷（无自加密）	PQC 候选算法中潜在的、未被发现的算法弱点	算法多样性（技术堆栈）
操作安全失误（密钥重复、"Cribs"）	不安全的 API 使用、硬编码密钥、实现层漏洞	AI 驱动的代码分析、高保真验证（仿真与验证引擎）
组织自满（坚信技术无懈可击）	“一次性迁移”的错误心态，忽视持续风险	持续的风险情报与治理（战略远见、治理循环）
先截获、后破译	“先窃取，后破解”（HNDL）攻击	基于数据保密寿命进行迁移优先级排序（战略远见）

表 1-1： 恩尼格玛时代的漏洞



历史映射战略： 正如恩尼格玛的崩溃源于“数学之外”的弱点，现代 **PQC 迁移** 也面临同样的 **“双重威胁”**：

- **水上：** 相信 PQC 算法的数学难题（如格密码）无懈可击。
- **水下：** 忽视了 **工程实现漏洞**（如侧信道攻击）和 **管理惯性**，这才是防御体系中最薄弱的环节 。

图 1-1： 复杂性的幻象——恩尼格玛机的系统性崩溃

1.2 公钥革命：建立在数学假定上的现代世界

恩尼格玛的对称加密体系暴露出的根本性缺陷，是“密钥分发难题”。为了安全通信，通信双方必须预先通过一个安全的物理渠道（如信使）交换共享密钥。这在小规模、点对点的军事通信中尚可接受，但对于 20 世纪六七十年代蓬勃发展、连接无数陌生节点的计算机网络而言，这种方式成本高昂、效率低下，完全不具备可扩展性，成为了数字世界发展的巨大障碍。

1.2.1 一场发明的双城记

正是在这一背景下，密码学历史上最伟大的革命——公钥密码学（Public-Key Cryptography, PKC）——应运而生。有趣的是，这场革命几乎同时在两个地方独立上演，一明一暗。

秘密的发明（英国 GCHQ）：在英国政府通信总部（GCHQ），詹姆斯·埃利斯（James Ellis）于 1970 年提出了“非秘密加密”的理论构想。随后，他的同事克利福德·柯克斯（Clifford Cocks）在 1973 年设计出了一种与 RSA 算法极为相似的实现方案，而另一位数学家马尔科姆·威廉姆森（Malcolm J. Williamson）则在 1974 年发明了类似 Diffie-Hellman 的密钥交换方法。然而，由于工作的机密性质，他们的这些开创性成果被深锁在档案柜中，数十年后才为世人所知。

公开的革命（美国斯坦福）：在大洋彼岸的美国，惠特菲尔德·迪菲（Whitfield Diffie）和马丁·赫尔曼（Martin Hellman）在拉尔夫·默克尔（Ralph Merkle）早期思想的启发下，于 1976 年公开发表了题为《密码学的新方向》的里程碑式论文，正式提出了公钥密钥交换的构想。不久之后，麻省理工学院（MIT）的罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）提出了著名的 RSA 算法，它基于大整数分解的数学难题，提供了一个完整、实用的公钥加密和数字签名方案。

1.2.2 非对称的突破

公钥密码学的核心思想是“非对称”。每个用户都拥有一对数学上相关联的密钥：一个是可以任意分发、公之于众的公钥，另一个是必须严格保密的私钥。用公钥加密的信息，只有对应的私钥才能解密。这一设计巧妙地解决了密钥分发难题：人们可以通过任何不安全的渠道（如互联网）交换公钥，而无需事先建立安全连接。密码系统的信任基础从此发生了根本性的转变：不再依赖于密钥传递渠道的物理安全，而是依赖于一个全新的基石——从公钥反向推导出私钥在计算上是不可行的。

1.2.3 社会影响：数字信任的“一维”基石

这场密码学革命的深远影响，塑造了我们今天所知的整个数字世界。

安全通信：PKC（公钥密码）是保障互联网安全通信的核心。我们日常浏览网页时地址栏出现的“锁”形图标，其背后的 SSL/TLS 协议正是利用 PKC 来协商会话密钥，为电子商务、网上银行和即时通讯等应用建立起一条加密信道。

认证与数字签名：PKC 赋予了数字世界“身份”和“信誉”。私钥可以对数据进行“签名”，而任何人都可以用公钥来验证该签名，从而确认信息的来源真实性（认证）和内容未被篡改（完整性）。这一功能至关重要，它被用于确保你的 Windows 软件更新确实来自微软而非黑客，也用于签署具有法律效力的电子合同和保护金融交易。

公钥基础设施（PKI）：为了解决“如何信任一个公钥确实属于它所声称的主体”这一问题，一个庞大的生态系统——公钥基础设施（PKI）应运而生。其中的核心是证书颁发机构（CA），它们如同数字世界的“护照签发机构”，通过颁发数字证书来证明公钥和其所有者之间的绑定关系。

PKC 的巨大成功，也孕育了其自身的脆弱性。过去几十年，传统密码学市场呈现出显著的“一维”特征：技术路径高度集中于 RSA 和 ECC 等少数算法，应用场景也高度集中于金融、通信等少数核心领域。整个数字世界的安全大厦，几乎完全建立在两个核心的数学难题之上：大整数分解（RSA 的基础）和离散对数问题（ECC 等算法的基础）。这种“单点故障”式的依赖，意味着一旦出现能够高效解决这两个问题的计算方法，全球的数字信任体系将瞬间崩塌。它缺乏算法层面的多样性，构成了一种巨大的、系统性的风险。

因此，即将到来的 PQC 迁移，绝非简单的算法替换。它是一次对全球信任基础设施的根本性升级。PKC 的诞生催生了 PKI，而整个 PKI 生态（包括 CA、X.509 证书标准、验证协议等）都是围绕 RSA/ECC 算法的特性（如密钥尺寸较小）来构建的。正如后文将指出的，PQC 算法普遍具有更大的密钥和签名尺寸，这对传统的 PKI 系统构成了巨大的工程挑战。因此，迁移工作需要重新设计我们赖以颁发和验证全球数字身份的核心机制。

密码学时代	核心问题	基础解决方案	信任基础	终极漏洞
对称时代（1970 年代前）	密钥分发	共享密钥（如恩尼格玛）	用于交换密钥的信道物理安全	密钥/密码本被物理缴获；操作失误
公钥时代（1970 年代-2030 年代?）	在开放网络中建立信任	非对称密钥对（RSA/ECC）	数学难题的计算复杂性（分解/离散对数）	能解决该数学问题的新型计算方式

表 1-2 ： 密码学时代对比

1.3 量子风暴：当新物理学湮灭旧数学

如果说当今全球的数字安全体系——公钥密码学（PKC）——是建立在一座名为“数学难题”的坚固堡垒之上，那么量子计算的出现，就如同一场能够直接瓦解堡垒地基的维度打击。这场风暴并非来自传统的计算领域，而是源于物理学的一次范式革命。

1.3.1 理论的黎明：费曼的远见

量子计算机的理论曙光，可以追溯到物理学巨擘理查德·费曼（Richard Feynman）在 1981 年提出的一个深刻洞见。费曼指出，自然界本质上是遵循量子力学规律运行的，用我们基于 0 和 1 逻辑的经典计算机去模拟它，效率极其低下，计算量会呈指数级爆炸式增长，几乎不现实[6]。

他因此提出了一个颠覆性的构想：

“自然界可不是经典物理能解释的，该死！如果你想模拟自然，最好用量子力学来构建。”

这一定义至关重要，它从根本上划清了界限：量子计算机并非一台“跑得更快”的经典计算机，它甚至不是为了解决经典计算机的所有问题而设计的。它是一种遵循量子叠加和纠缠等奇异规则运行的、全新的计算范式，专门用于解决那些经典计算机无法企及的特定难题。

1.3.2 Shor 算法：致命的“杀手级应用”

在费曼提出构想后的十余年里，量子计算很大程度上仍是物理学家和理论家脑中的概念。直到 1994 年，贝尔实验室的数学家彼得·肖尔（Peter Shor[7]）发表了他的量子算法，才将这个物理学概念，正式变成了对整个数字世界具体而致命的威胁。

Shor 算法[7]如同一把精确制导的钥匙，完美打开了公钥密码学堡垒的两把核心门锁。它证明，一台足够强大的量子计算机能够以超乎想象的速度，高效解决两个特定的数学问题：

大整数质因数分解（Integer Factorization）

离散对数问题（Discrete Logarithm Problem）

这并非巧合，而是“精准打击”。这两个问题，恰好是当前应用最广泛的两大公钥密码体系——RSA 和 椭圆曲线密码（ECC）——赖以生存的安全基石。Shor 算法[7] 的出现，意味着支撑全球互联网信任体系的地基开始松动。

1.3.3 从理论到现实：价值 1500 万美元的“3x5”

如果说肖尔（Shor[7]）的论文是向经典密码学发出的“理论宣战”，那么 2001 年的 一次物理实验则真正打响了第一枪，将这种威胁从纸上带入了现实世界。

当时，在 IBM Almaden 研究中心，由麻省理工学院（MIT）的庄以田（Isaac Chuang）领导，并与斯坦福大学及加拿大卡尔加里大学合作的研究团队，成功地在一台拥有 7 个量子比特的核磁共振（NMR）量子计算机上，完整地运行了 Shor 算法[7]。尽管这台原型机据称研发成本高达 1500 万美元，但它成功地完成了看似微不足道的任务：将数字 15 正确地分解为 3 和 5 。

1.3.3.1 这一成就的深远意义

将 15 分解为 3 和 5，对于任何一个小学生或是普通计算器来说都易如反掌，但对于量子计算的发展而言，这却是一个里程碑式的事件，其意义远超计算结果本身：

原理的首次物理验证（Proof of Principle）：这是人类历史上第一次在物理系统中，完整地、可扩展地实现了 Shor 算法[7]。它雄辩地证明了 Shor 算法[7] 不仅仅是数学家的理论推导，更是一个可以在真实物理世界中运行并产生正确结果的程序。它消除了人们对量子算法可行性的根本疑虑。

量子计算可行性的强力证据：这个实验成功地操控了 7 个量子比特，实现了量子叠加、纠缠和干涉等一系列复杂的量子力学现象，并最终得出了确定的经典答案。这为整个量子计算领域注入了强大的信心，表明建造一台有实用价值的量子计算机虽然极端困难，但并非天方夜谭。

对密码学界的实质性警示：尽管分解 15 在密码学上毫无威胁，但它如同一声惊雷，让密码学界和信息安全行业无法再忽视量子计算。它将“量子威胁”从一个遥远的、理论上的可能性，变成了一个清晰可见的、由技术发展路径决定的未来。它促使各国政府、

标准组织和研究机构开始认真投入资源，研发能够抵御量子计算机攻击的后量子密码（PQC）。

因此，庄以田团队的这次实验，虽然成果“简单”，却标志着量子计算从纯理论探索迈向了实验科学的关键一步，是 Shor 算法[7] 从抽象概念走向现实威胁的第一个具体缩影。它所开启的，是一个全新的、量子与经典信息安全体系相互博弈的时代。

1.3.3.2 算法揭秘：不是暴力破解，而是“降维打击”

Shor 算法[7] 的威力并不在于像经典计算机那样更快地尝试每一个可能的钥匙（暴力破解），而在于它利用量子力学原理，直接“看穿”了数学迷宫的整体结构。我们可以通过一个声学比喻来理解这一过程：

量子并行（全知视角）：经典计算机寻找密码就像在黑暗的房间里拿着手电筒逐个照亮角落。而量子计算机利用“叠加态”，仿佛瞬间点亮了整个房间，同时感知到了所有的可能性。

量子干涉（过滤噪音）：这是算法的灵魂。Shor 算法[7] 通过一种名为“量子傅里叶变换”的操作，充当了“降噪耳机”或“透镜”的角色。在这个过程中，所有错误的答案像杂乱的声波一样相互抵消（相消干涉），归于沉寂；而正确的答案（即破解密码所需的“周期”）则像共振一样相互增强（相长干涉），变得清晰可见。

测量（获取结果）：最后，当通过这块“透镜”观测时，正确的密钥就以极高的概率直接显现出来。

结论：这种计算范式上的降维打击，使得一台拥有足够量子比特的计算机，可以在数小时内破解传统超级计算机需要数亿年才能解决的 RSA-2048 难题。

1.3.4 “先窃取，后破解”：已经发生的未来威胁

量子计算机的物理实现仍面临巨大挑战，但这并不意味着我们可以高枕无忧。这一未来的威胁，已经催生了一个迫在眉睫的现实危机——“先窃取，后破解”（Harvest Now, Decrypt Later - HNDL）。全球范围内的对手方，特别是拥有强大资源的国家级行为体，正在积极地拦截和大规模存储当今使用 RSA/ECC 加密的海量数据。他们像松鼠囤积冬粮一样，把这些无法破解的密文数据保存在巨大的服务器集群中，等待未来量子计算机的问世。

他们正在进行一场豪赌，赌注就是未来的量子计算机能够为他们解密这些今天无法打开的信息宝库。这里面可能包含：

国家安全机密

企业核心知识产权

金融交易记录

个人生物基因档案

关键基础设施的控制协议

这一威胁已经从情报界的理论探讨，转变为各国政府和企业的官方关切。包括美国网络安全和基础设施安全局（CISA）和国家安全局（NSA）在内的权威机构，已联合发布公开警告，敦促各组织机构立即开始准备向 PQC 迁移，以应对 HNDL 对国家关键基础设施和敏感信息构成的威胁。

这种威胁的认知已经渗透到企业决策层。一份 2025 年发布的《泰雷兹数据威胁报告》显示，58%[2] 的组织已将“未来对今日数据的解密，包括‘先窃取，后破解’”视为主要的量子计算安全威胁。另一份来自凯捷咨询的同期研究也发现，65%[1] 的组织对 HNDL 攻击的兴起感到担忧。这一系列证据表明，HNDL 已经成功地从一个前瞻性的技术问题，演变为一个主流的、可量化的商业风险，并正在深刻影响企业的战略规划和预算分配。

这意味着，对于任何需要长期保密（例如，超过 5-10 年）的数据而言，其安全漏洞已经存在。

后量子密码（PQC）的迁移，因此不再是一项为保护未来数据而进行的前瞻性投资，而是一项为弥补当前和过去数据泄露风险而必须立即采取的补救措施。这种风险模型从根本上改变了决策者评估风险的时间框架。

传统上，风险评估是基于“此时此地”的威胁。而 HNDL 模型则要求决策者必须进行一场“ 与时间赛跑 ”的计算：

如果 量子计算机的预期出现时间 < 数据的预期保密寿命，那么你的数据就已处于风险之中。

这使得 PQC 迁移，从一个遥远的 IT 技术议题，转变为一项紧迫的、关乎组织长期生存的业务连续性和风险管理要务。

1.4 全球响应：铸造抗量子的未来

面对 Shor 算法[7] 带来的颠覆性威胁，全球学术界、产业界和政府机构并未坐以待毙，而是迅速行动起来，共同开启了一场旨在重塑数字安全未来的协同防御战。

1.4.1 新领域的崛起：抗量子密码学

在 Shor 算法[7] 问世后，一个全新的密码学研究领域——后量子密码学（Post-Quantum Cryptography, PQC，也称为抗量子密码学）应运而生。其核心目标是研发出全新的公钥密码算法，这些算法的安全性基于一些被认为对于经典计算机和量子计算机都同样困难的数学问题，从而能够抵御来自两个维度的攻击。经过多年的探索，研究者们逐渐聚焦于几个主要的候选技术路线，包括：基于格的密码学、多变量密码学、基于哈希的密码学、基于编码的密码学[15] 以及基于同源的密码学。

1.4.2 NIST 标准化：一场开放、协作的全球竞赛

在这场竞赛中，美国国家标准与技术研究院（NIST）发起的 PQC 标准化项目，展现了与恩尼格玛时代敌我分明、暗箱操作截然不同的图景。这种开放、透明和协作的模式并非 PQC 项目的“独创”，而是 NIST 自 DES 征集伊始便开始探索，并在 AES 与 SHA-3 的标准化过程中臻于成熟的“黄金法则”。 PQC 项目正是承袭了这一久经考验的机制，号召全球最顶尖的密码学家在公开的环境下，对候选算法进行长达数年的、最严苛的审查和攻击，从而“在部署前就发现并淘汰弱者”，以最大限度地建立对最终胜出算法的信心。

阶段一：全球征集与初步筛选（2016 - 2017）

2016 年 12 月：发布“英雄帖” NIST 正式发布了 PQC 算法的全球征集公告（Call for Proposals）。公告详细列出了对未来 PQC 标准的期望，包括明确的安全级别要求（对应于破解 AES-128、192、256 的难度）、性能指标（密钥大小、签名大小、计算速度）以及实现的灵活性。这相当于为这场竞赛设定了明确的规则和场地。

2017 年 11 月：海选入围 截止日期前，NIST 收到了来自全球 25 个国家的 82 份提案。这是一个空前的盛况，展现了全球密码学界对这一挑战的高度热情。NIST 对这些提案进行了初步审查，淘汰了那些提交不完整或明显不符合基本要求的方案，最终接纳了 69 个算法作为第一轮的正式候选者。

阶段二：第一轮评审（2018 – 2019）聚焦安全基础

目标：淘汰存在明显安全缺陷的算法。

过程：在接下来的 14 个月里，这 69 个算法的完整设计文档被公之于众。NIST 举办了第一次 PQC 标准化会议，全球的密码学家、黑客和学者都投入到对这些算法的分析中。这期间，大量的学术论文发表，指出了许多算法的理论漏洞、实现缺陷甚至直接的攻击方法。这是一场“找茬”大赛，任何微小的瑕疵都可能致命。

2019 年 1 月：第一轮晋级名单公布 NIST 发布了第一轮的评估报告。基于全球社区的反馈，大量算法被证明是不安全的。NIST 大刀阔斧地将候选名单削减至 26 个。被淘汰的算法大多是因为其所依赖的数学问题被发现存在“捷径”，或者其参数设置不够安全。

阶段三：第二轮评审（2019 – 2020）兼顾性能与实现

目标：在确保安全性的前提下，开始重点评估算法的 性能和实际部署的可行性。

过程：竞争进入白热化阶段。剩下的 26 个算法都是第一轮的“幸存者”，安全性相对更有保障。这一轮的焦点转移到：在真实的硬件（从服务器到小型物联网设备）上，它们的运行效率如何？密钥和签名的大小是否实用？实现代码是否容易出错？全球研究者对这些算法进行了大量的基准测试（Benchmarking）和侧信道攻击分析（Side-channel Analysis），即通过功耗、电磁辐射等物理信息来窃取密钥。

2020 年 7 月：决赛圈诞生 经过又一轮残酷的评估，NIST 公布了第三轮，也就是决赛圈的候选名单。这份名单被分为两组：

7 个决赛入围者（Finalists）： 这些是被认为最成熟、最有希望成为最终标准的算法。其中，基于格的密码学方案因其在安全性和性能上的出色平衡而占据主导地位。

8 个备选方案（Alternate Candidates）：这些算法同样很有潜力，但在某些方面（如成熟度或性能）稍逊一筹。NIST 保留它们作为“B 计划”，以防决赛算法出现意外问题，同时也为了鼓励“算法多样性”。

阶段四：第三轮评审与最终抉择（2020 – 2024）

目标：对决赛选手进行最后的、最深入的审查，并起草标准草案。

过程：这是最后的冲刺。NIST 和全球社区对这 7 个决赛算法进行了最细致的“盘问”。讨论的焦点细化到每一个参数的选择、不同平台上的优化技巧，以及如何编写能够抵抗侧信道攻击的安全代码。与此同时，NIST 开始与这些算法的提交者密切合作，着手编写标准化的技术文档。

2022 年 7 月：宣布首批获胜者 NIST 发布了历史性的公告，宣布了首批将要被标准化的四个算法，结束了人们长期的猜测：

通用加密/密钥封装（KEM）：CRYSTALS-Kyber[12]

通用数字签名：CRYSTALS-Dilithium[13], Falcon

高保障数字签名：SPHINCS+[14]

2023 年 - 2024 年 8 月：标准化与尘埃落定 NIST 发布了基于 Kyber[12] (ML-KEM)、Dilithium[13] (ML-DSA) 和 SPHINCS+[14] (SLH-DSA) 的标准草案 (FIPS 203, 204, 205)，并向公众征求最终反馈。在解决所有技术细节和反馈意见后，2024 年 8 月 13 日，NIST 正式发布了这三份标准的最终版本。这标志着这场历时近八年的全球密码学竞赛，终于取得了里程碑式的成果，为全球的 PQC 迁移提供了坚实的技术基石。

1.4.2.1 首批 PQC 标准：兼顾性能与稳健

最终被 NIST 选定并标准化的首批算法，体现了在性能、效率和安全性之间的审慎权衡：

通用密钥封装机制（KEM）：ML-KEM[12]（基于 CRYSTALS-Kyber 算法）被选中，并被正式确定为 FIPS 203 标准。它基于格密码，在各种平台上都表现出卓越的性能和相对紧凑的尺寸，被认为是通用加密场景（如 TLS 密钥交换）的首选。

通用数字签名：ML-DSA[13]（基于 CRYSTALS-Dilithium 算法）同样基于格密码，因其良好的性能和安全性而被选为通用的数字签名标准，即 FIPS 204。

高保障数字签名：SLH-DSA[14]（基于 SPHINCS+算法）也被标准化为 FIPS 205。它是一种无状态的哈希签名方案。虽然其签名尺寸较大、速度较慢，但其安全性仅依赖

于底层哈希函数（如 SHA-256）的强度。由于哈希函数被认为是抗量子攻击的，这使得 SLH-DSA 成为一种极其保守和可靠的选择，适用于代码签名、根证书签发等对安全性有最高要求的场景。

1.4.2.2 算法多样性：汲取历史教训的战略远见

NIST 的战略远见并不仅限于在 2022 年选出首批标准。他们深刻地认识到，将所有希望寄托于单一类型的数学难题（即格密码）本身就是一种风险。历史已经反复证明，今天看似坚不可摧的数学堡垒，明天可能就会被新的攻击方法所攻破。

为了应对这一挑战，并进一步丰富后量子密码工具箱，NIST 启动了第四轮附加的标准化流程（“On-Ramp”），旨在寻找更多具有潜力的候选算法。这一举措吸引了全球顶尖密码学家的持续参与，其中一个标志性事件，便是辛辛那提大学的丁津泰（Jintai Ding）教授团队提交了新的候选标准。

丁津泰教授的参与具有标志性意义。作为全球 PQC 标准 CRYSTALS-Kyber[12] 的核心缔造者，他持续参与新一轮标准化进程，这深刻反映了业界的战略共识——即在现有格密码体系之外，必须探索异构的数学基础，为未来构建多样化的技术备份。

正是基于这种对“算法多样性”原则的制度化坚持，NIST 在为格密码寻找备份方案。因此，NIST 于 2025 年 3 月 11 日 宣布选择了一种基于完全不同数学难题的算法——基于编码的 HQC[15]——作为另一个 KEM 标准。HQC 基于汉明准循环（Hamming Quasi-Cyclic）码，拥有成熟的数学理论基础。虽然其密文尺寸略大于 ML-KEM，但作为一种不同数学原理的算法，它为抗量子迁移提供了关键的“安全冗余”，用于在格算法可能出现隐患时作为长期稳健的替代方案。

这一系列决策的意义极其深远。它制度化地体现了“算法多样性”原则，即为未来格密码一旦被攻破的“黑天鹅”事件预备了多个 B 计划。这也从根本上向所有正在规划迁移的组织传递了一个明确的信号：未来的安全架构不应是僵化的，而必须是“密码敏捷[23] 的”（Crypto-Agile），即具备在必要时灵活切换到不同密码算法的能力。这正是本白皮书中的“战略引擎”框架的核心底座。

1.4.3 NIST 国家网络安全卓越中心（NCCoE）：从标准到实践的桥梁

仅仅发布技术标准不足以解决复杂的迁移问题。为了将标准转化为可部署的解决方案，NIST 成立了国家网络安全卓越中心（NCCoE），其核心使命是汇集来自工业界、政府和学术界的专家，共同开发能够应对现实世界需求的、实用的、可互操作的网络安全方案。

针对 PQC 迁移这一重大挑战，NCCoE 与 NIST PQC 标准化小组的工作几乎同步展开，早在 2018 年便开始筹备相关工作，并正式启动了“向后量子密码迁移”（Migration to Post-Quantum Cryptography）项目。该项目旨在通过发布白皮书、行

动手册（playbooks）和概念验证（proof-of-concept）实现，为各组织机构的迁移工作提供便利。

该项目的巨大实践价值和行业公信力，体现在其广泛的合作基础上。项目参与者不仅包括 AWS、微软、Cisco、Intel、IBM 等科技巨头和 三星 SDS 等国际企业，还涵盖了汇丰银行（HSBC）、摩根大通（JPMorgan）等金融机构，以及美国国家安全局（NSA）和美国国土安全部网络安全与基础设施安全局（CISA）等政府合作伙伴。

1.4.3.1 战略印证：NCCoE 实践验证“迁移引擎”框架

该项目的组织架构和工作流程，为本白皮书提出的“战略引擎”框架提供了强有力的现实印证。NCCoE 项目主要通过两个核心工作流来推进，其内容与本白皮书的战略模块高度契合：

密码学发现工作流

此工作流专注于利用自动化工具，帮助组织清点其密码学资产，即了解密码学在何处以及如何被用于保护数据和系统。其目标是建立一份详尽的 密码学清单（CBOM），并基于此进行风险管理和迁移优先级排序（例如，应用“莫斯卡定理”[8]）。战略对应：这与本白皮书“战略引擎”的“获得初始动力：战略远见与风险情报”阶段的目标完全一致。

互操作性与性能工作流

此工作流旨在探索和回答一个关键问题：新发布的 NIST PQC 标准算法在现实世界的通信协议（如 TLS、SSH）和硬件安全模块（HSM）中将如何运行。它通过在接近真实的环境中进行测试，验证 PQC 方案的性能影响和系统兼容性。战略对应：这恰恰是本白皮书“引擎”框架中“构建动能：抗量子密码技术堆栈”和“加速引擎：仿真与验证模块”两个阶段的实践体现。

1.4.3.2 融合 NIST CSF 2.0：从技术到管理的闭环

NCCoE 的实践不仅验证了技术路径，更将其深度融入了 NIST 网络安全框架 2.0（CSF 2.0）。NCCoE 将复杂的 PQC 迁移过程，映射到 CSF 2.0 的六大核心功能——治理（Govern）、识别（Identify）、保护（Protect）、检测（Detect）、响应（Respond）和恢复（Recover）——之中。这种映射为企业提供了一套标准化的管理语言，确保 PQC 迁移不仅是技术升级，更是组织整体网络安全治理的一部分。

1.4.3.3 战略方向与合规刚性

NCCoE 确立的这套“技术+管理”框架，实际上是应对全球合规压力的官方蓝图。这与美国联邦政府的顶层战略保持了高度一致：根据 《第 10 号国家安全备忘录[20]》（NSM-10）及相关行政令要求，美国已划定红线，要求国家安全系统（NSS）及关键基础设施在 2035 年前，必须全面完成基于抗量子算法（如 TLS 升级）的产品链替换。

因此，NCCoE 的项目成果不仅证明了“战略引擎”框架的可行性，更向全球产业界揭示了：遵循 CSF 2.0 框架进行有序迁移，是应对 2035 合规大限的唯一正确路径。

1.4.4 IETFRFC9xxx 的发布（2025 年中）

继 NIST 发布底层算法标准后，IETF 正式发布了关于在 TLS 1.3 中支持混合密钥交换（Hybrid Key Exchange）的 RFC 标准文档[16]。这标志着 PQC 不再仅仅是数学层面的算法，而是正式成为了互联网通信协议的核心组件。

该 RFC 的核心价值在于确立了“传统算法 + 后量子算法”的双重保险机制（例如：X25519 + ML-KEM 组合）[16]。这种混合模式具有极高的战略意义：

1. 纵深防御：它同时利用了传统椭圆曲线密码（ECC）成熟的安全性与 PQC 的抗量子特性。即使未来发现 PQC 算法存在理论缺陷，传统的 ECC 依然能守住安全底线，消除了业界对单一新技术路线的顾虑。

2. 对抗“先窃取，后破解”：通过引入 PQC 元素，该协议立即赋予了数据流对抗未来量子计算机解密的能力，解决了长效数据的存储安全问题。

这一互联网通信协议层面的全球通用标准，彻底扫清了云厂商（如 AWS、Azure）和 CDN 服务商（如 Cloudflare、Akamai）在基础设施层面进行大规模切换的最后的协议障碍，使得 PQC 能够从“实验性选项”转变为“默认开启配置”。

1.4.5 全球政策趋同：关闭犹豫的窗口

随着技术基础的奠定和威胁的明确，全球主要经济体纷纷出台政策，将 PQC 迁移从一个选项变为一项强制性任务。这些政策虽然在具体执行机制上有所不同，但在目标和时间表上表现出惊人的一致性，共同构成了一股不可逆转的全球迁移浪潮。

CBOM 的合规红线（2025）：美国网络安全与基础设施安全局（CISA）和欧盟在 2025 年的软件供应链安全指南中，首次明确要求关键基础设施供应商在提交 SBOM（软件物料清单）的同时，必须包含 CBOM（密码物料清单），明确标注所使用的加密算法及其来源。这一举措直接将 PQC 迁移的压力传导至了整个软件供应链的最上游。

1.4.5.1 美国：多层次的强制引擎

美国的 PQC 政策框架是一个复杂而精密的体系，由白宫的战略指令、国会的立法、行政部门的实施指南以及国家安全机构的强制性标准共同构成，层层递进，环环相扣。

战略方向：

白宫《第 10 号国家安全备忘录》（NSM-10[20] ）：2022 年 5 月 4 日，拜登政府发布了《第 10 号国家安全备忘录》（NSM-10）[20]，为美国的 PQC 迁移设定了最高级别的战略方向。该备忘录明确指出，美国的目标是“在 2035 年前，尽可能减轻量子风险”，并指示所有联邦机构启动向 PQC 迁移的多年进程。NSM-10[20] 本身并未设定具体的算法弃用日期，而是作为整个国家行动的“发令枪”，为后续所有具体政策提供了合法性与战略依据。

特朗普政府《关于强化后量子时代国家安全与技术领导力的行政令》（2025 年 6 月）：继 NSM-10[20] 奠定基础后，特朗普总统于 2025 年 6 月 签署了新的行政令，旨在将“战略规划”转化为“雷厉风行的执行”。该命令强调“美国优先”的量子安全供应链，明确引入了“联邦采购熔断机制”——即要求自 2026 财年起，所有联邦政府采购的关键 IT 产品必须具备抗量子能力（或具备明确的升级路径），否则将面临采购禁令。这一举措极大地加速了私营部门（特别是国防承包商和关键基础设施供应商）的合规步伐，迫使其必须在短期内拿出具体的迁移路线图。

立法固化：

为确保政策的连续性，美国国会于 2022 年底通过了《量子计算网络安全准备法案》，并于 2022 年 12 月 21 日 由总统签署成为法律。该法案将 NSM-10[20] 的核心要求以法律形式固定下来，要求行政管理和预算办公室（Office of Management and Budget, OMB）定期向国会报告迁移进展，从而建立了一个确保行政部门执行力和问责制的长效机制。

实施指南：

OMB M-23-02[30] 号备忘录为将 NSM-10[20] 的战略目标转化为具体行动，OMB 于 2022 年 11 月 18 日 发布了 M-23-02 号备忘录。该文件要求所有联邦行政部门（FCEB）机构必须在规定时间内完成对其信息系统中加密系统的盘点，并提交迁移到 PQC 的成本估算。这是 PQC 迁移的第一个具体执行步骤——“摸清家底”。

强制执行引擎：

NSA 的 CNSA 2.0[21] 与 NIST 的弃用时间表 美国政策框架中最具强制力的部分，来自国家安全局（NSA）和 NIST 发布的具体技术标准和时间表。这些文件将高层目标转化为对技术供应商和政府机构具有约束力的硬性要求。

针对国家安全系统（NSS）：2022 年 9 月，NSA 发布了《商业国家安全算法套件 2.0》（CNSA 2.0[21]），为 NSS 及其供应商（包括广大的国防工业基础）设定了极为激进和明确的迁移时间表。例如，它要求：到 2025 年，用于软件和固件签名、Web 浏览器/服务器和云服务的系统，必须支持并优先使用 CNSA 2.0 中指定的 PQC 算法。到 2030 年，传统的网络设备（如 VPN、路由器）以及用于软件/固件签名的系统，必须独占性地使用 PQC 算法，并逐步淘汰不支持 PQC 的设备。

针对联邦系统：2024 年 11 月，NIST 发布了其技术报告草案 IR 8547[22]，为更广泛的联邦系统提供了算法弃用时间表。该报告明确指出，安全性低于 128 位的传统公钥算法（如 RSA-2048）预计将在 2030 年后被“弃用”（deprecated），并在 2035 年后被“禁用”（disallowed）。这与 NSM-10[20] 的 2035 年总目标完全吻合，并提供了具体的技术截止日期。

这一多层级政策体系的精妙之处在于，虽然 CNSA 2.0[21] 的强制性时间表名义上仅适用于国家安全系统，但它实际上起到了为整个美国乃至全球科技市场设定“事实标准”的作用。大型技术供应商，如云计算巨头、操作系统开发商和网络设备制造商，为了能够向美国国防部和情报界等庞大市场销售产品，必须使其商业产品符合 CNSA 2.0 的严格要求。这导致他们会将 CNSA 2.0 的时间表融入其主流产品的研发路线图。其结果是，即便是一个与政府毫无业务往来的普通商业公司，在采购新的软件、硬件和云服务时，也会发现这些产品已经按照 CNSA 2.0 的节奏实现了 PQC 兼容。这种由政府采购驱动的市场涟漪效应，极大地加速了 PQC 在私营部门的普及，其影响范围远远超出了政府指令的直接管辖。

1.4.5.2 欧盟：构建协同的欧洲大陆防线

与美国自上而下的模式不同，欧盟的 PQC 政策演进体现了从成员国各自为政到形成统一战略的协同过程，其最终的执行力将更多地依赖于其强大的监管框架。

先行者：德国与法国

在欧盟层面形成统一政策之前，德国和法国作为技术领头羊，早已开始了前瞻性布局。

德国联邦信息安全办公室（BSI）： 自 2020 年起，BSI 就发布了其 PQC 迁移建议，并持续更新其技术指南（TR-02102-1）。BSI 不仅紧跟 NIST 的步伐，还推荐了如 FrodoKEM 等其认为具有更高安全冗余的算法，并始终强调“密码学敏捷性”（Cryptographic Agility）和混合模式（Hybrid Mode）的重要性。

法国国家网络安全局（ANSSI）：ANSSI 在 2022 年 1 月 发布了其 PQC 迁移立场文件，明确提出分阶段过渡的路线图，并强烈建议采用混合模式，以确保在引入 PQC 时不降低对经典攻击的防御能力。此外，法国还联合德国、荷兰、瑞典等国发布了关于量子密钥分发（QKD）的立场文件，显示了其在早期就寻求跨国协调的意愿。

统一化进程：2024 年委员会建议与 2025 年路线图

欧盟 PQC 政策的转折点出现在 2024 年 4 月 11 日，欧盟委员会发布了一项正式建议，敦促成员国通过网络与信息系统安全合作组（NIS Cooperation Group）制定一个协调一致的 PQC 实施路线图。这一进程在 2025 年 6 月 23 日 达到高潮，欧盟

委员会与成员国共同发布了《PQC 迁移协调实施路线图[24]》。这份文件是欧盟当前最核心的 PQC 政策纲领，设定了明确的里程碑：

到 2026 年底：所有成员国应启动国家级 PQC 迁移战略，并开始采取“第一步”行动，如风险评估和加密资产盘点。

到 2030 年底： 针对高风险用例，特别是关键基础设施[24]（能源、金融、交通、卫生等）的 PQC 迁移必须完成。

到 2035 年底： 对中低风险系统的迁移应尽可能完成。

与美国以联邦采购为主要驱动力不同，欧盟 PQC 路线图的执行力将通过其强大的监管体系来实现。尽管路线图[24] 本身是“建议”，但欧盟的网络安全法规，如《网络与信息系统安全指令第二版》（NIS2）和《网络弹性法案》（CRA），都要求相关实体采取“最先进”（state-of-the-art）的安全措施。随着 PQC 标准最终确定且相关产品商业化，PQC 将被迅速定义为“最先进”的安全实践。届时，欧盟各国的监管机构在执行 NIS2 等法规时，会将未能规划和实施 PQC 迁移视为不合规行为，尤其是在 2030 年大限将至的关键基础设施领域。这种由合规驱动的模式，将通过潜在的巨额罚款和法律责任，强力推动整个欧盟私营部门的 PQC 迁移。

1.4.5.3 英国：务实且结构化的国家路线图

脱欧后的英国，在其国家网络安全中心（NCSC）的领导下，采取了一种既与盟友保持一致又独具特色的务实路径。

2023 年 11 月，NCSC 发布了其 PQC 迁移白皮书，发出了立即开始准备的明确信号。随后，在 2025 年 3 月，NCSC 发布了更为详细的《PQC 迁移时间表》指南[26]，为英国设定了一个清晰的三阶段国家路线图：

第一阶段（到 2028 年）： 组织应完成全面的加密资产发现和评估，定义迁移目标，并制定初步的迁移计划。

第二阶段（到 2031 年）： 完成早期、最高优先级的 PQC 迁移活动，并根据技术和市场的发展完善详细的迁移路线图。

第三阶段（到 2035 年）： 完成所有系统、服务和产品的 PQC 迁移，与美国和欧盟的最终目标保持同步。

NCSC 的指南以其对准备工作的极度重视而著称，特意为发现、评估和规划等前期活动预留了长达 2-3 年的时间，这反映出其对大型组织迁移复杂性的深刻理解和务实态度。

英国的策略可以被看作是连接美国“采购驱动”模式和欧盟“监管驱动”模式的“务实桥梁”。一方面，NCSC 设定了明确的政府时间表[26]，为行业提供了清晰的目标。另一方面，它又非常强调通过市场机制来推动，例如鼓励组织向其供应商发布“迁移意

向声明”，以刺激 PQC 产品和服务的市场供给。此外，NCSC 还计划推出针对 PQC 迁移咨询公司的认证计划，旨在培育一个可信的国内专业服务市场，而非仅仅依赖自上而下的监管。这种混合模式使英国能够在与五眼联盟（尤其是美国）和欧盟保持战略协同的同时，根据本国经济结构灵活地调整实施策略，通过引导市场来达成政策目标。

1.4.5.4 国际标准化组织：全球共识的另一块拼图

除了 NIST 标准外，国际标准化组织（ISO/IEC）也在积极推进 PQC 标准化。ISO/IEC JTC 1/SC 27 已于 2024 年推进相关修正案，将 Kyber 和 Dilithium 等算法纳入 ISO/IEC 18033-2（非对称加密）和 ISO/IEC 14888-3（数字签名）标准体系 [18-19]。对于许多非美国、非欧盟地区的跨国企业而言，ISO 标准往往是采购合规的重要依据，这进一步强化了全球 PQC 标准的覆盖网络。

1.4.5.5 中国的“双轨战略”：密码自主与标准引领

中国的 PQC 战略最显著的特点是其坚定的“自主可控”路线。这一选择的根本驱动力，是源于对外国主导技术中潜在“后门”的深层担忧，以及实现技术自立的国家级宏大战略。这种战略姿态决定了中国不会简单地采纳或跟随美国 NIST 的标准，而是致力于建立一个由中国主导的、独立的密码生态系统。

为实现这一目标，中国通过其官方标准化机构采取了系统性的行动。2025 年 2 月，中国密码行业标准化技术委员会（CSTC）和商用密码标准研究院（ICCS）联合向全球发起了新一代商用密码算法的征集活动[27]。

这一行动迅速取得了实质性进展。2025 年 10 月 9 日，ICCS 正式发布了《关于新一代商用密码候选算法的公告》。这份具有里程碑意义的文件不仅公布了通过初审的算法名单，更明确了中国 PQC 标准化的“时间表”与“路线图”。公告显示，入围算法涵盖了格密码、编码密码及多变量密码等多种技术路线，且明确要求在 2027 年前完成核心标准的草案制定。

这一系列举措体现了一种高度成熟的战略：它既利用全球顶尖的智力资源（如自 2018 年起 CACR 组织的竞赛积累）来提升其国家标准的技术水平，又完全确保了最终成果符合其“自主可控”的核心原则。这实质上是一种“具有中国特色的开放式创新”，旨在打造一个既有全球影响力又由自身牢固掌控的 PQC 标准体系。

与此同时，中国采取了 PQC 与量子密钥分发（QKD）并行的“双轨”战略。中国在基于物理学原理的硬件 QKD 领域投入巨资，构建了全球规模最大的 QKD 骨干网络。

然而，我们必须清醒地认识到 QKD 技术路线的客观局限性。QKD 网络建设成本极为高昂，且严重依赖专用的物理光纤链路，难以在大规模不可信的公共计算机网络（如互联网）中通过软件形式灵活部署。更关键的是，QKD 仅能解决密钥分发问题，无法

提供数字经济中至关重要的“身份认证”功能。 因此，QKD 目前及未来很长一段时间内，主要将被限制在政务、军事及金融骨干网等特定的保密通信专网场景中。

然而需要指出的是，在面向中国商用密码市场、数字经济安全长远发展的角度，中国必将以 PQC 迁移为驱动，培养具有自主知识产权的 PQC 技术链、产业链和应用生态环境。相较于 QKD，PQC 能够以低成本、软件化的方式无缝嵌入现有的 IT 基础设施中，它是唯一能够覆盖从物联网终端到云端数据中心全场景的普适性抗量子解决方案。

1.4.5.6 SM9 的抗量子演进：从标识密码到抗量子标识密码

2025 年，中国国家数据局在推进“全国一体化数据市场”建设中，明确提出在跨区域、跨主体的数据流通（特别是“东数西算”工程）中，开展抗量子加密技术的试点应用。这标志着中国 PQC 的驱动力已从单纯的“安全合规”扩展到了“数据要素资产化”的基础设施建设层面。

要理解中国 PQC 迁移的独特性和复杂性，没有比分析其商用密码（SM）体系中 SM9 算法的后量子演进路径更好的案例了。这一过程不仅是对单一算法的升级，更是对中国整个自主密码战略的一次全面压力测试和能力展示。

SM9 的现状：功能优势与量子脆弱性

SM9 是中国商用密码体系的核心支柱之一，是一种基于标识的密码（Identity-Based Cryptography, IBC）算法。其整个算法家族，包括数字签名、密钥封装和密钥交换协议，不仅在国内广泛应用，也已成功获得 ISO/IEC 国际标准的认可[18-19]，彰显了其技术成熟度和国际影响力。

SM9 的核心创新在于，它允许直接使用用户的唯一身份标识（如电子邮件地址、手机号码或设备 ID）作为其公钥，从而彻底摆脱了传统公钥基础设施（PKI）中复杂的数字证书签发、分发和管理链条。用户的私钥由一个受信任的权威机构——密钥生成中心（Key Generation Center, PKG）——使用系统主密钥生成并安全分发。这种“无证书”模式极大地简化了大规模网络环境下的密钥管理，尤其适用于物联网、工业互联网等拥有海量节点的场景。

然而，SM9 的强大功能建立在一个脆弱的数学基础之上。其安全性依赖于椭圆曲线上的双线性对（Bilinear Pairings）运算。不幸的是，这一数学难题正是彼得·肖尔（Peter Shor[7]）的量子算法能够高效解决的目标之一。这意味着，一旦实用化的量子计算机问世，当前整个 SM9 密码体系的安全性将瞬间瓦解。因此，对 SM9 进行后量子升级，对其生态系统而言并非一个可选项，而是一项关乎生死存亡的必然要求。

SM9 抗量子演进的技术路径展望：基于行业趋势的研判

中国商用密码体系的演进往往遵循严谨的科学逻辑与国家战略需求。虽然具体的官方迁移细则尚在制定中，但结合国家密码战略、公开征求意见稿及学术界共识，我们可以从技术逻辑和产业需求角度，构建一个前瞻性的演进参考框架。

通过主权标准化完成算法内核替换

迁移的核心是对 SM9 的数学引擎进行根本性替换。2025 年由 CSTC/ICCS 发起的全球 PQC 算法征集活动，为 SM9 寻找抗量子“心脏”提供了标准化的选拔平台。 为了完整保留 SM9 作为标识密码的核心优势，简单的采用 NIST 标准化的通用密钥封装机制（如 ML-KEM[12]）是远远不够的。其替代者必须是一种抗量子的标识加密（PQC-IBE）方案[28]。

目前，学术界和工业界公认的最有前景、研究最深入的 PQC-IBE 构建路径是基于格的密码学（Lattice-Based Cryptography）[28]。这与中国的国家战略高度一致。国家密码管理局发布的“十四五”期间密码科技研究指南中，明确将格密码（包括 LWE、SVP 等难题）的安全性分析作为重点支持方向，甚至设定了“刷新相关国际挑战纪录”的考核指标。这表明中国正在集中国家力量，力求在理论和实践上完全掌握构建下一代 PQC-IBE 所需的核心数学工具，为 SM9 的升级奠定坚实的理论基础[28]。

以混合实现模式构建务实的过渡桥梁

对于一个已深度融入各类应用的大规模密码体系，激进的“一刀切”式替换是不可行的。全球密码学界的共识，包括 IETF 的草案和 NIST、NCSC 等机构的指南，都指向了混合实现模式（Hybrid Mode）[17]作为最平稳、风险最低的过渡策略。混合模式将一个成熟的传统算法（如现有的 SM9）与一个新的 PQC 算法（如未来的 PQC-SM9）相结合，只要两者中至少有一个是安全的，整体的安全性就能得到保障。

中国的迁移规划明确支持这一路径。前述的国家科研指南中，明确设立了“现役密码协议与抗量子公钥密码算法的融合方法研究”这一课题。这为 SM9 采用混合模式提供了官方的政策和资金支持。在实践中，一个混合的 SM9-PQC 方案，其密钥封装过程可能会同时执行一次经典的基于配对的运算和一次全新的基于格的运算，并将两个结果组合起来生成最终的会话密钥。这种设计可以同时实现两个关键目标：

后向兼容性：尚未升级的系统可以忽略 PQC 部分，继续使用经典部分进行通信，确保业务不中断。

前向安全性：PQC 部分的存在可以有效抵御“先窃取，后破解”（HNDL）攻击，因为即使对手未来拥有量子计算机，也无法破解被 PQC 保护的那部分密钥。

进行系统性的基础设施与生态重构：信任锚点的代际更迭

SM9 的迁移面临着比传统 PKI 更严峻的挑战——信任锚点的重置。在 SM9 体系中，用户的私钥由密钥生成中心（PKG）利用主密钥派生。

信任源重建：迁移到抗量子算法（如格密码 PQC-IBE）意味着 PKG 必须更换其数学“心脏”（主密钥）。这不仅仅是软件升级，而是要求所有用户必须重新向新的 PKG 注册并获取新的私钥。

历史数据包袱：旧的 PKG 不能立即下线，否则无法解密历史数据；新的 PKG 必须并行上线。这种“双信任源”的长期共存和最终切换，是 SM9 迁移中最大的工程风险点。

这一现实决定了 SM9 的迁移不能是渐进式的修补，而必须是一次精心策划的“整体及格”。

所以，SM9 的迁移绝非简单的算法更替，而是要求对现有的标识密码生态进行一次彻底的、系统性的重构。 中国的规划者对此有清醒的认识。国家科研指南中要求承接单位研制“密码基础设施、密码设备抗量子迁移的总体技术架构”，并包含对“底层抗量子密码算法、数字证书的适配指标要求”。

这清晰地表明，迁移计划是一项全栈工程，其范围覆盖：

核心基础设施：对密钥生成中心（PKG）进行软硬件升级，使其能够管理和分发基于格的 PQC-IBE 私钥。

应用开发： 为应用开发者提供全新的、支持混合模式和纯 PQC 模式的软件开发工具包（SDK）。

密码硬件：研发并部署支持新型 PQC-IBE 算法的硬件安全模块（HSM）、加密卡和安全芯片，如中国电子信息产业集团（CEC）已发布的“量铠”系列产品，为高性能场景提供硬件加速。

协议与标准：定义新的协议流程和数据格式，以适应 PQC-IBE 算法带来的更大公私钥尺寸和签名体积。

成功迁移 SM9，将是中国能够独立自主地完成一次复杂的下一代密码体系代际更迭的最终证明，它将成为中国“自主可控”PQC 战略的旗舰项目和最佳范例。同时，这一决策也揭示了其战略优先级：为了保留标识密码在密钥管理上的巨大便利性，中国愿意承担相应的迁移复杂度，这是一种着眼于长期运营效率而非短期迁移便利的战略远见。

下表总结了 SM9 从当前状态到未来抗量子状态的演进框架。

特性	当前的 SM9（基于 GM/T 0044 等标准）	未来的抗量子 SM9（推演）

密码学基础	基于椭圆曲线的双线性对（Pairing-Based）	基于格的密码学（Lattice-Based），如 LWE/Ring-LWE 问题
安全态势	可抵御经典计算机攻击；对 Shor 量子算法脆弱	可抵御已知的所有经典和量子攻击
密钥管理模型	标识密码（无 PKI 证书），依赖中心化的密钥生成中心（PKG）	保持标识密码模型，依赖经过 PQC 升级的 PKG
标准化载体	GM/T 0044-2016, ISO/IEC 11770-3 等	通过 2025 年 CSTC/ICCS 后量子密码算法征集产生的新国家标准[27]
过渡策略	不适用	混合模式：并行运行经典 SM9 与新型 PQC-IBE，确保后向兼容与前向安全
生态系统组件	基于双线性对的 PKG、SDK、硬件和应用	升级后的 PKG、全新的 PQC-IBE SDK、新型硬件密码模块及适配应用
信任锚点迁移难度	N/A (体系已建立)	极高（需重建根密钥，所有用户需重新获取私钥，面临“双根并存”的复杂运维）

表 1-3 ： SM9 迁移框架：从当前状态到后量子未来

战略影响与展望：商密全面焕新重塑产业格局

中国围绕商用密码的 PQC 迁移战略，不仅是一次防御性的安全升级，更是一次旨在重塑全球密码学格局、争夺未来技术标准主导权的战略进攻。这一进程将引发整个网络空间安全产业的大变局，并产生深远的战略影响。

首先，商用密码体系的全面代际更替，将催生庞大的产业重构机遇。这不仅仅是单一算法的替换，而是从底层的密码芯片、操作系统，到上层的应用软件、网关设备的一次全栈式更新。随着中国建立起一套独立自主的 PQC 标准体系（涵盖 PQC-SM2/3/4/9 等全系列），所有在中国运营的跨国企业将面临显著的“合规摩擦”（Compliance Friction）。企业必须开发和维护具备高度“密码敏捷性”的系统，使其能够根据地理

位置和监管要求，在基于 NIST 的标准和中国的商密标准之间灵活切换。这将倒逼网络安全产业从单纯的“合规销售”转向提供“双栈兼容”的高技术含量解决方案，从而极大地增加了研发、测试和供应链管理的复杂性与价值门槛。

其次，从更宏观的层面看，这可能加速全球数字基础设施走向“技术两极化”或“密码学分岔”的趋势。未来可能出现两个并行的、互不兼容的密码生态系统：一个以美国/NIST 标准为核心，另一个以中国/CSTC 标准为核心。这一局面将对全球互联网的互操作性、国际数据流动的通畅性以及全球科技供应链的完整性构成长期而深刻的挑战。

1.4.5.7 日本：积极研发与战略协同

日本的 PQC 工作由国家信息与通信技术研究所（NICT）和密码研究与评估委员会（CRYPTREC）主导。日本的策略是“两条腿走路”：一方面，积极投入自主研发和安全评估，甚至向 NIST 提交了自己的候选算法，旨在建立国内的专业知识体系，而非被动接受外部标准。另一方面，其公开发布的指南和行业实践又显示出与 NIST 进程的高度一致性，以确保与西方伙伴的互操作性。日本同样在 QKD 领域有重要研究，但其整体战略显得更加融入西方技术生态。

1.4.5.8 韩国：全面的国家总体规划

韩国政府展现了极强的顶层设计能力，发布了结构清晰的《后量子密码转换总体规划》，目标直指 2035 年完成全国性迁移。这一规划得到了国家级战略科技发展计划的强力支持，承诺投入数万亿韩元（数十亿美元）用于开发包括千比特级量子计算机在内的核心技术，并培养庞大的量子技术人才队伍。该规划被细分为技术获取、法规修订、产业基础建设等六大方向，展示了一个高度组织化、旨在全面打造“量子经济”的宏伟蓝图。

但韩国标准的国际影响力较小。主要原因在于它的国际 PQC 标准征集活动规定：所有方案的牵头者必须是韩国人。 这一排他性条款在一定程度上限制了全球顶尖学者的参与深度，使其标准更倾向于国内专用而非国际通用。

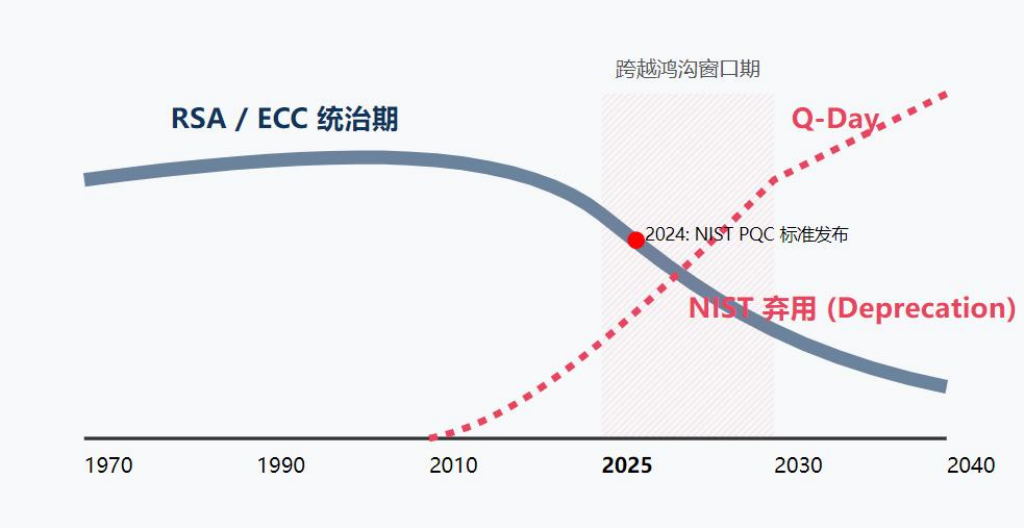


图 1-2： 数字信任范式的代际更替时间轴（1970-2040）

第二章

加速的威胁态势：驱动引擎的外部压力

第二章 加速的威胁态势：驱动引擎的外部压力

本部分旨在阐明“为何行动”——那些不容忽视的、强大的外部压力，正迫使全球组织机构开始启动强劲的迁移引擎。

2.1 缩短的时间线：为何量子威胁迫在眉睫

随着量子计算技术的不断发展，其对现有加密算法（如 RSA 和 ECC）的潜在威胁已引起广泛关注。Shor 算法[7]的提出，从理论上展示了量子计算机破解这些经典加密算法的能力。为了将这种加速的趋势具体化，我们可以采用一种基于研究成果的量化分析模型，评估破解不同加密算法所需的量子资源和预期时间。

HNDL 攻击彻底改变了网络安全防御的时间逻辑，引入了极度危险的“非对称紧迫性”。防御方必须在数据失去保密价值之前完成密码迁移，而攻击方则拥有相对充裕的等待时间。加拿大滑铁卢大学的米歇尔·莫斯卡（Michele Mosca）教授提出的莫斯卡定理（Mosca's Theorem）[8]精辟地量化了这一危机，为我们提供了一个清晰的决策模型：

$$X+Y > Z$$

其中：

X 代表数据需要保持机密的年限（例如，房贷合同可能为 30 年，国家机密可能为 50 年）。

Y 代表整个金融系统迁移至抗量子密码所需的时间（包括标准制定、软硬件升级、互操作性测试等）。

Z 代表实用化量子计算机（CRQC）问世并具备破解能力的时间。

定理指出，如果 $X + Y > Z$，则系统已处于实质性的不安全状态，因为在迁移完成之前，量子计算机就已经能够解密那些尚处于保密期内的数据。

对于任何依赖长期敏感数据的行业而言，这个不等式都极其令人担忧。大量的核心高价值数据（如商业机密、知识产权、个人隐私档案、医疗记录或关键基础设施蓝图）的保密期往往长达 20 至 50 年。

而考虑到现代信息系统的庞大体量、遗留架构的复杂性以及供应链的深度依赖，实现全系统的安全迁移保守估计需要 5 至 10 年，甚至更久。鉴于业界专家普遍预测

CRQC 可能在未来 10 至 15 年内（即 $\mathbf{Z}$ 值）出现，不等式 $\mathbf{X+Y>Z}$ 在当前大概率已经成立。

这意味着，对于那些具有长期价值的数据而言，安全的“最后期限”实际上已经过去，我们正处于与时间赛跑的“加时赛”阶段。这种紧迫性迫使各行各业必须在量子计算机尚未完全成熟的今天，就立即启动大规模的抗量子迁移准备，任何等待都等同于将未来的信息资产拱手让予对手。

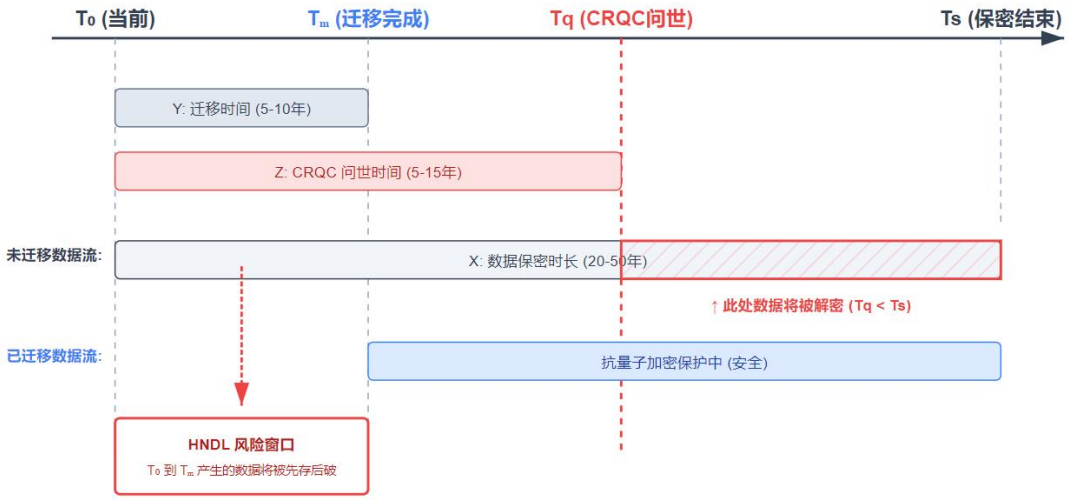


图 2-1： 莫斯卡定理与 HNDL 威胁的时间轴演进

该图展示了在“先窃取，后破解”威胁下，数据安全的时间窗口。由于数据保密期（$\mathbf{X}$, 20-50 年）往往远长于量子计算机问世时间（$\mathbf{Z}$, 5-15 年），即 $\mathbf{T_q < T_s}$，导致当前时刻（$\mathbf{T_0}$）产生的传统加密数据面临确定性的未来解密风险。注意: Tm 和 Tq 哪个先发生目前是未知的，只有 $\mathbf{T_q > T_s}$，$\mathbf{T_0}$时刻产生的数据才是安全的。

以及，该图直观地展示了“安全赤字”是如何形成的。请看以下典型场景：

现实案例（2025 年）： 某银行今日签署了一份 30 年期 的住房抵押贷款合同或存储了一份 50 年保密期 的国家基础设施蓝图（$X = 30 \sim 50$）。

量子节点（2035 年）： 业界预测具备破解能力的量子计算机将在 10 年后 出现（$Z = 10$）。

结论： 即使我们忽略迁移所需的时间（Y），不等式 $X > Z$ 已经成立。这意味着，这份今日生成的数据，在未来的 20-40 年保密期内将处于“裸奔”状态。 对于长期资产而言，风险窗口不是在未来打开，而是现在已经敞开。

2.1.1 量化分析：破解 RSA 和 ECC 的量子比特需求与时间线

根据 Shor 算法[7]以及 ETSI/QSC 2024（新加坡）年会报告 披露的最新数据，破解 RSA 和 ECC 加密算法所需的逻辑量子比特数在不同密钥长度下有所不同。以下表格基于上述前沿会议的研判，展示了具体的资源需求和基于当前发展趋势的时间预测。

加密算法	密钥长度	破解所需逻辑量子比特数	破解所需物理量子比特数（预估）	预期达成时间(考虑容错)
RSA	1024 位	2000-2500	~200 万	2030 年
RSA	2048 位	4000-5000	~400 万	2040 年
ECC	160 位	1500	~150 万	2028 年
ECC	256 位	4000	~400 万	2035 年

表 2-1 ： 破解 RSA/ECC 所需逻辑量子比特数

逻辑量子比特 vs. 物理量子比特： 表中的“逻辑量子比特”是执行算法所需的、理想化的、无错误的计算单元。然而，现实世界的量子比特（“物理量子比特”）极易受到环境噪声的干扰而出错。为了构建一个可靠的逻辑量子比特，需要使用大量的物理量子比特组成纠错码进行保护。

值得警惕的是，这一转换比率（开销）正在经历颠覆性的突破。 传统观点认为该比率高达 1000:1 甚至更高，但根据 2024 年国际公开文献及 ETSI/QSC 2024 新加坡年会报告 指出，得益于量子纠错编码技术的飞跃，物理-逻辑量子比特的转换比率已大幅优化至约 7.8:1。这一关键数据的更新意味着，建造一台具有实用破译能力的量子计算机，其工程难度和所需硬件规模比预想中下降了两个数量级，威胁迫近的速度远超预期。

2.1.2 战略启示：RSA 和 ECC 的未来

RSA 加密算法：破解 1024 位 RSA 密钥大约需要 2000 到 2500 个逻辑量子比特，预计将在 2030 年 被实现。而当前广泛使用的 2048 位 RSA 密钥则需要 4000 到 5000 个

逻辑量子比特，预计将在 2040 年 被破解。近期研究进一步细化了这些估计，例如，有研究表明，使用约 372 个物理量子比特和数千的电路深度即可挑战 RSA-2048。

ECC 加密算法：破解 160 位 ECC 密钥（相当于 1024 位 RSA）大约需要 1500 个逻辑量子比特，预计将在 2028 年 被实现。破解 256 位 ECC 密钥（相当于 2048 位 RSA）则需要大约 4000 个逻辑量子比特，预计将在 2035 年 被实现。一项对二进制椭圆曲线的详细资源估算表明，破解 n=233 的 ECC（接近 256 位安全级别）需要约 3035 个逻辑量子比特，在 1μs 码周期的超导量子计算机上运行时间约为 7.9 分钟。

2.1.3 技术协同效应：进一步压缩时间线的催化剂

根据 ATIS（电信行业解决方案联盟）2025 年发布的最新战略报告[11]，以及 Gouzien (2023) 和 Gidney (2025) 的突破性研究，破解主流公钥密码体系所需的资源门槛正在被大幅拉低。以下表格展示了基于这些最新硬件架构创新的资源需求和时间预测。

加密算法	密钥长度	传统预估物理量子比特数	最新架构下的物理量子比特数（基于猫量子比特[9]）	预期达成时间（激进/混合攻击）
RSA	2048 位	~2000 万	< 100 万（基于表面码优化）	2030 年代初
ECC	256 位	~1000 万 - 3000 万	~12.6 万（基于猫量子比特[9]）	2020 年代末（混合攻击）

表 2-2 ： 技术突破下的威胁加速（猫量子比特）

传统的估算通常认为需要数百万甚至上千万个物理量子比特才能构建出一台具有破解能力的容错量子计算机（CRQC）。然而，ATIS 报告指出[11]，通过引入“猫量子比特”和先进的“表面码（Surface Codes）”技术，这一壁垒正在崩塌。

ECC 的极速破解： 根据 Elie Gouzien 等人的最新分析，一种基于猫量子比特的容错架构，仅需约 126,000 个物理量子比特，即可在 9 小时内 破解 256 位 ECC 加密。这与传统架构所需的数百万个量子比特相比，实现了数量级的缩减。

RSA 的门槛降低： C. Gidney (2025) 的研究表明，通过优化表面码[10]，破解 2048 位 RSA 整数所需的资源可能降至 100 万个噪声物理量子比特以下。

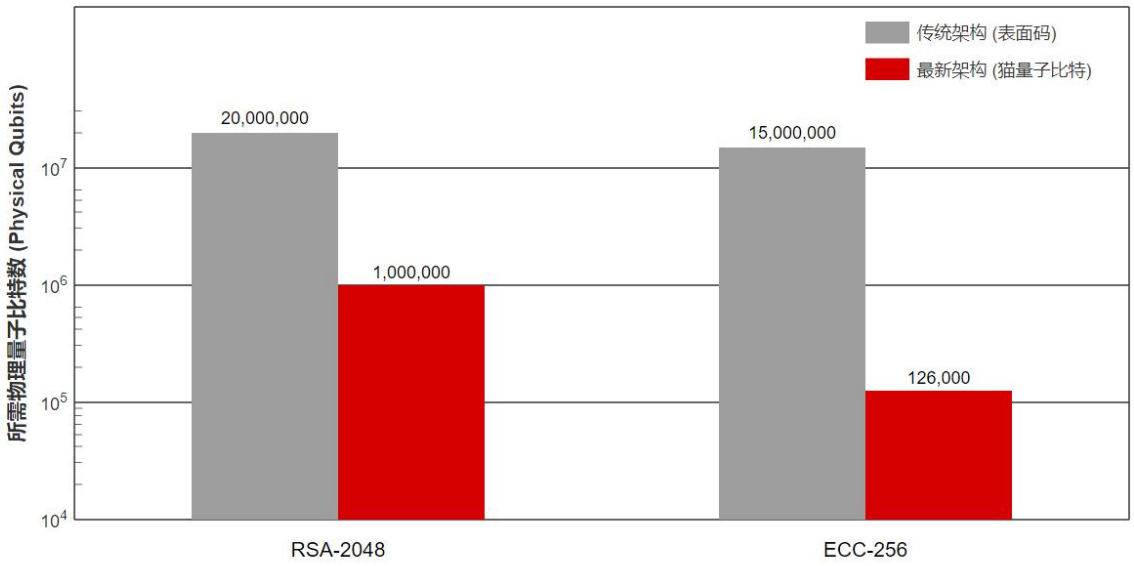


图 2-2： 技术突破下的威胁加速——破解所需资源对比

这意味着，随着硬件保真度的提升和这些新型纠错架构的结合，量子威胁的时间线可能被压缩 5-10 年。虽然保守估计仍指向 2035 年，但一个激进且合理的预测是：针对部分加密系统的混合攻击或将在 2020 年代末出现，而全面的破解能力可能在 2030 年代初就已具备。

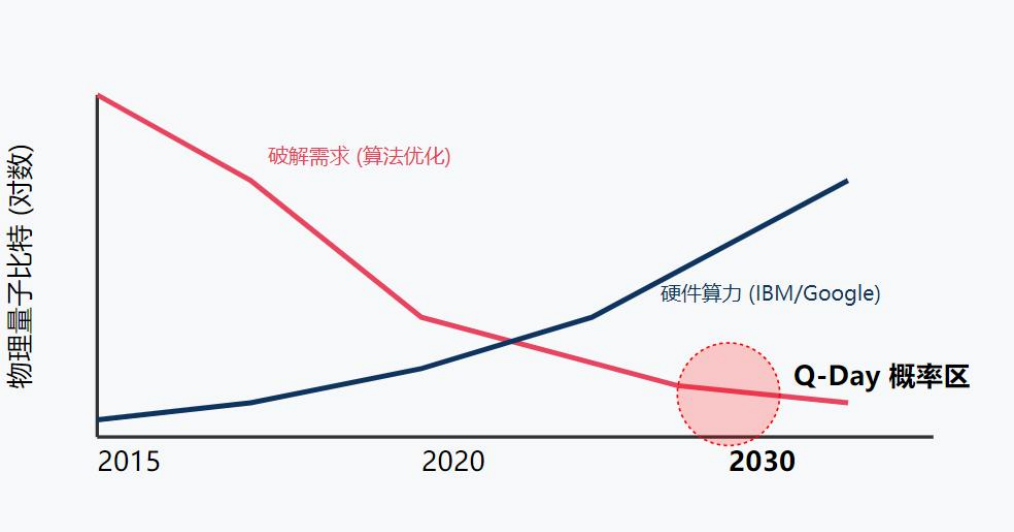


图 2-3： 破解门槛的崩塌——量子算力需求演进趋势

2.2 演进中的威胁图景：超越 Shor 算法

在应对抗量子迁移的挑战时，组织机构正面临一场“双线作战”。我们面对的并非单一威胁，而是一个由未来量子风险和当前经典风险构成的双重威胁环境。

广为人知的“量子威胁”，即 Shor 算法[7]对现有公钥密码体系（RSA/ECC）的颠覆，是一项长期的、战略性的风险。然而，一个同样强大且更为直接的“经典威胁”正持续演进，它利用现代计算技术，特别是人工智能驱动的分析工具，将攻击目标从算法的数学基础转向了密码学的具体工程实现。以 CodeQL 等为代表的符号 AI 工具和以 CryptoGuard 等为代表的机器学习工具，能够自动化、规模化地发现密码学实现过程中的细微缺陷，例如硬编码的密钥或不安全的 API 误用，这些缺陷足以完全绕过算法在数学层面提供的所有安全保障。

“先窃取，后破解”（Harvest Now, Decrypt Later, HNDL）攻击模型正是连接这两种威胁的桥梁。攻击者现在就可以利用现有技术大规模拦截并存储加密数据，等待未来量子计算机问世后进行破解。这种模式从根本上改变了迁移的性质。对于任何需要长期保密的数据——如需要保存数十年的房贷合同、企业核心知识产权或个人健康档案——其安全漏洞实际上已经存在。PQC 迁移因此不再是一项保护未来数据的前瞻性投资，而是一项补救过去和现在数据泄露风险的即时性措施。

近期西浦 PQC-X 实验室团队成功攻破 200 维达姆施塔特（Darmstadt）SVP 挑战[35]和成功破解了 Bochum Challenges 中的 Kyber-208 实例，这是经典威胁不断升级的一个鲜明实例。此项成就由本联盟核心成员西交利物浦大学 PQC-X 实验室的丁津泰教授领导。最有前景的 PQC 算法家族——格密码学——其安全性正是建立在解决高维 SVP（最短向量问题）等问题的假定难度之上。这一成就不仅为 PQC 系统的安全性提供了至关重要的现实世界基准，更是 PQC 威胁“迭代性”的有力证明。它与该团队揭示 NIST 部分候选方案（如 GeMSS、LUOV）存在弱点的研究一起，共同警告我们，必须警惕 PQC 迁移可以“一劳永逸”的观念。即便是作为防御核心的 PQC 算法本身，也正成为不断演进的经典攻击方法的目标。这种迭代性的威胁，决定了我们的防御体系不能是一次性的替换，而必须是一个能够持续学习、适应和演进的动态过程——这正是迁移引擎的核心理念。

2.3 全球响应：政策与标准的趋同

抗量子迁移并非由单一技术驱动，而是在全球范围内由政府政策、国际标准和行业共识共同推动的一场协同变革。这种全球性的趋同为 PQC 迁移设定了明确的方向和不容忽视的时间表，使其从一个技术议题上升为一项全球性的战略任务，为运转中的引擎提供了强大的外部推力。

美国国家标准与技术研究院（NIST）自 2016 年发起的 PQC 标准化项目，已成为全球 PQC 技术发展的“北极星”。2024 年 8 月，NIST 正式发布了首批 PQC 标准，包括作为通用密钥封装机制的 ML-KEM[12] (Kyber)和作为通用数字签名标准的 ML-DSA[13] (Dilithium)与 SLH-DSA[14] (SPHINCS+)。更具战略意义的是，NIST 选择了基于编码的

HQC 作为 ML-KEM 的备份标准，其目的正是为了提供“算法多样性”[15]，以应对未来基于格的数学难题被攻破的潜在风险。这一举措深刻体现了对密码安全深思熟虑的战略，并从根本上要求企业在架构设计中必须具备密码敏捷性[23]。

紧随 NIST 的步伐，全球主要经济体的政府迅速将 PQC 迁移提升至国家战略和政策指令的高度。

美国： 白宫发布的《第 10 号国家安全备忘录[20]》（NSM-10）和相关行政命令，为联邦政府设定了明确的时间表：到 2030 年，RSA-2048 等传统公钥算法将被“弃用”；到 2035 年，将被完全“禁用”。

欧盟： 发布的《关于向后量子密码过渡的协调实施路线图[24]》要求，到 2030 年底，关键基础设施必须完成向 PQC 的迁移。

中国： 国家密码行业标准化技术委员会（CSTC）和商用密码标准研究院（ICCS）已发起全球 PQC 算法征集活动，旨在加速推进并构建独立自主的 PQC 标准体系。

这些由政策驱动的确定性，正在深刻地影响着全球企业的技术战略和投资决策。与此同时，后量子密码联盟（PQCA）等行业组织和 Open Quantum Safe (OQS)等开源项目正在积极构建支撑迁移的生态系统，共同降低实施门槛[36]。全球政策的趋同、政府指令的明确以及行业生态的协同，共同构成了一股强大的力量，推动着 PQC 迁移的浪潮。这不再是一个是否需要迁移的问题，而是如何在既定的时间框架内，以最具战略性和成本效益的方式完成迁移的问题。

区域/机构	关键文件/事件	日期	关键里程碑/要求	对全球组织的意义
美国（NIST）	首批 PQC 标准发布（FIPS 203, 204, 205）	2024 年 8 月	正式确定 ML-KEM, ML-DSA, SLH-DSA	为产品开发提供了稳定、经过审查的算法。
美国（NIST）	HQC 被选为 KEM 备份	2025 年 3 月	提供了算法多样性[15]，以应对潜在的格密码破解风险。	强化了对密码敏捷性的需求。
美国（政府）	NIST IR 8547 / 行政命令修订[22]	2024 年 11 月 / 2025 年 6 月	设定了 2030 年弃用和 2035 年禁用 RSA/ECC 的期限。	确立了不可协商的迁移硬性时间表。

欧盟	协调实施路线图	2025 年 6 月	成员国在 2026 年前启动迁移；关键基础设施在 2030 年前完成[24]。	创造了统一的欧洲市场需求和合规环境。
中国 (ICCS/CSTC)	全球 PQC 算法征集	2025 年 2 月	启动独立的国家标准化进程。[27]	提供不同于西方的、具备自主知识产权的另一种安全选择，贡献全球数字安全治理的“中国智慧”。

表 2-3 ： 全球 PQC 政策与标准化里程碑

第三章

量子安全迁移战略引擎：一个战略性框架

第三章 量子安全迁移战略引擎：一个战略性框架

本部分将详细阐述“量子安全迁移战略引擎”。这不是一个静态的流程图，而是一个动态的、循环加速的动能系统。想象一个精密的涡轮引擎：“密码敏捷性”是其坚固的底座，承载一切运转；“战略远见”是点火装置，启动第一波能量；“技术堆栈”是动力总成，确保持续输出；“仿真验证”是涡轮增压，成倍提升效率；而“治理演进”则是 ECU（控制单元），确保引擎在双重威胁的复杂路况下始终平稳运行。

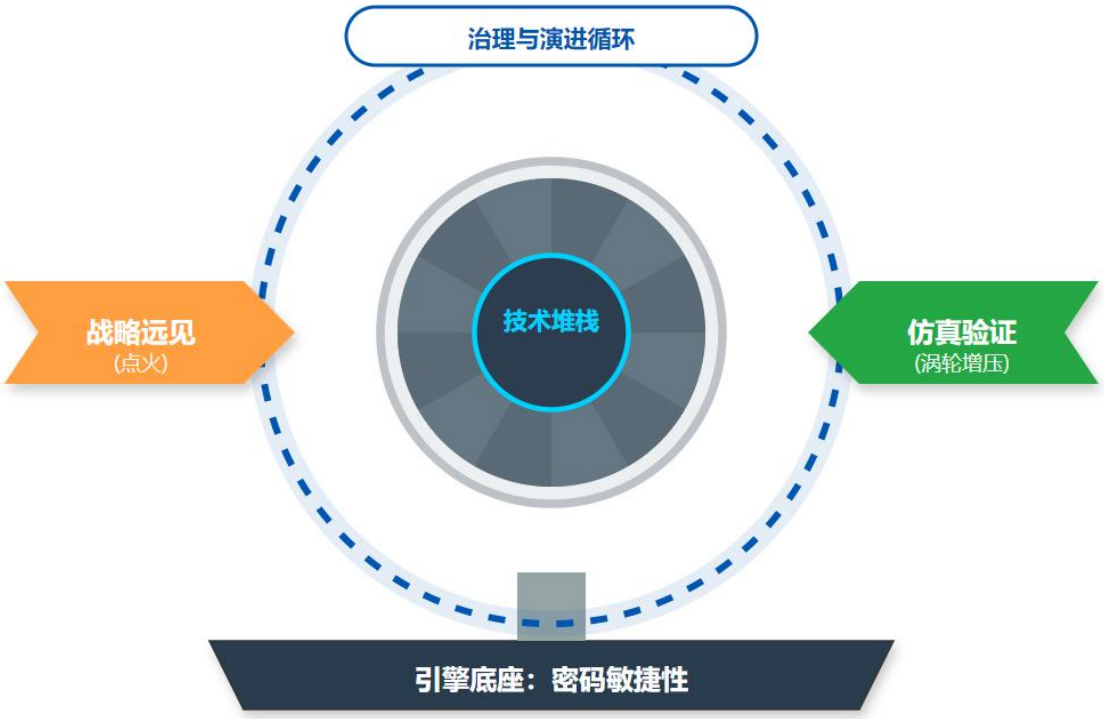


图 3-1： 量子安全迁移战略引擎框架

图 3-1 展示了量子安全迁移战略引擎（Quantum-Safe Migration Strategic Engine），这是一个以密码敏捷性为坚实底座 ，通过战略远见实现初始点火，以抗量子密码技术栈作为核心动力输出，并利用仿真验证进行效率增压，最终在治理与演进循环的持续调控下，将组织从传统加密体系平稳、动态地推进至具备长期量子韧性的新一代信任架构。

3.1 引擎底座：密码敏捷性（异构融合与动态重构）的核心原则

如果说迁移引擎需要持续运转，那么密码敏捷性[23]（Crypto-Agility）就是支撑其运转的、不可动摇的底座。它并非一个简单的技术特性，而是应对未来不确定性的战略性架构保障。这一原则的战略重要性，得到了美国国家标准与技术研究院（NIST）的权

威认可[23]。在其发布的开创性白皮书 NIST CSWP 39, 《实现密码敏捷性的考量：战略与实践》(Considerations for Achieving Cryptographic Agility: Strategies and Practices) 中，由 Lily Chen、Dustin Moody 等专家组成的团队，为这一概念奠定了官方基础。

根据 NIST 的正式定义，“密码敏捷性[23]是指在不中断运行系统流程的情况下，为实现韧性而替换和调整协议、应用、软件、硬件及基础设施中的密码算法所需的能力”。这意味着信息系统必须能够在不进行重大重新设计或中断服务的前提下，灵活、高效地切换或更新其所使用的密码算法、协议及相关参数。

然而，实现密码敏捷性[23]并非易事。NIST 在其白皮书中明确指出了多项严峻挑战，例如：PQC 算法普遍更大的密钥和签名尺寸对性能造成的开销、在算法协商过程中可能遭受的降级攻击、难以更新的遗留系统和长生命周期设备中硬编码的算法，以及在维护互操作性的同时淘汰老旧算法的困难。

成功的迁移必须在工程层面将密码敏捷性[23]根植于系统的协议构造与架构设计之中，而本白皮书提出的技术方案，正是对 NIST 所识别挑战的直接回应。

NIST CSWP 39 识别的关键密码敏捷性挑战	引擎框架中的应对策略	具体技术实现
算法协商过程中的降级攻击	核心原则：密码敏捷性设计	采用受强完整性保护的算法协商协议，防止攻击者强制系统使用弱算法。
PQC 的性能开销（大密钥/签名）	技术堆栈：软硬件协同设计	部署 PQC 硬件加速卡以处理高吞吐量场景；为资源受限设备提供轻量化软件库。
异构环境中的互操作性	核心原则：密码敏捷性设计	设计并部署异构认证密钥交换（AKE）协议，允许不同密码能力的系统安全通信。
遗留系统中的硬编码算法	执行引擎：灰度演进；核心原则：密码敏捷性设计	对于无法改造的系统，通过支持 PQC 的安全网关进行“封装”保护；使用加密 API 而非

		直接实现。
PKI 迁移的复杂性	核心原则：密码敏捷性设计	采用混合 X.509 证书，使单一证书能同时被新旧系统验证，实现平滑过渡。

表 3-1 ： 实现密码敏捷性：NIST 挑战与应对

成功的迁移必须在工程层面将密码敏捷性[23]根植于系统的协议构造与架构设计之中。这需要一系列先进的技术实现作为支撑，将抽象的敏捷性原则转化为具体、可操作的工程实践：

3.1.1 异构环境下的协议互操作性工程

在企业庞大而复杂的生态系统中，不同机构、不同系统的 PQC 迁移进度必然存在差异，这将导致一个长期的、密码基础设施不一致的“异构环境”。为解决这一关键痛点，必须设计并部署 异构认证密钥交换（Heterogeneous Authenticated Key Exchange, AKE）协议。该协议的核心目标是，允许持有不同类型长期密钥（例如，一方已迁移至基于密钥封装机制 KEM 的 Kyber[12]，而交易对手方仍在使用基于数字签名的 Dilithium[13]）的实体完成安全的身份认证和密钥协商。这使得组织可以在不强制要求所有交易对手同步升级的情况下，分阶段、分批次地进行迁移，是实现密码敏捷性[23]的关键协议层创新。

3.1.2 混合实现模式作为过渡桥梁

在完全过渡到纯 PQC 环境之前， 混合加密模式是一种被广泛推荐的务实策略。它将一个经过充分验证的传统算法（如 ECC）与一个新的 PQC 算法（如 Kyber[12]）结合使用，其安全性的基础在于，只要两个算法中至少有一个是安全的，整个连接就是安全的。这包括两种主要的技术路径：

可分离混合模式 (Separable Hybrid Mode): 经典密码计算与 PQC 计算独立并行进行，例如，在 TLS 握手时同时执行一次 ECDHE 和一次 ML-KEM[12]密钥交换。这种模式实现相对简单，允许根据策略灵活启用 PQC 部分。

不可分离混合模式（Inseparable Hybrid Mode）：将经典密码与 PQC 深度融合，例如，通过嵌套加密机制，客户端先用经典算法加密，再用 PQC 算法对中间密文进行二次加密。这种模式虽然实现更复杂，但可以有效减少通信开销。

为了支撑这些复杂的混合模式，协议本身也需要进行深度优化。例如，可以设计一种优化的 TLS 握手流程，让服务器先行发送其 PQC 公钥，从而减少一次往返交互，显著提升协议效率。朗空量子团队研发的“朗空量子护盾”便是一个支持混合数字签名、密钥封装和密钥交换的后量子敏捷框架，是实现混合模式平稳过渡的典型实践。

图 3-2： 混合协议栈架构 —— “双重保险箱”设计

3.1.3 敏捷的公钥基础设施（PKI）管理

PQC 对现有的公钥基础设施（PKI）带来了巨大挑战，其中最突出的是 PQC 公钥和签名尺寸远大于传统算法，导致数字证书体积显著增加。为了平滑过渡，一种有效的技术方案是设计 混合 X.509 证书。该方案将 PQC 公钥和对应的签名值存储在证书的扩展域中。这样，升级后的系统可以从扩展域中提取信息进行 PQC 验证，而传统系统则可以忽略扩展域，继续使用经典算法进行验证。这种设计使得一套证书体系能够同时满足新旧系统的验签需求，是实现 PKI 敏捷迁移的关键技术。

密码敏捷性[23]是整个引擎平稳点火的基础。一个敏捷的架构确保了后续的技术选型、部署验证和长期治理都具备灵活性，从而减少了未来因标准或威胁变化而产生的摩擦和成本。

3.2 获得初始动力：战略远见与风险情报

为组织的‘量子安全迁移战略引擎’完成点火启动。这股力量来自于基于情报的战略远见和对风险态势的精准把握。值得强调的是，这一阶段的许多核心活动，都可以被

视为“无悔之举”。这一战略概念源自 TNO 等机构发布的 PQC 迁移手册[25]，指的是那些无论量子威胁何时到来、甚至是否到来，都能为组织带来显著安全价值的行动。

将 PQC 迁移视为一次提升组织整体“密码学成熟度”（Cryptographic Maturity）的契机，而非一次简单的技术升级，是至关重要的战略视角。密码学成熟度意味着组织对自身的密码学使用有全面的了解，有能力评估相关风险，并制定了与法规和业务目标相符的策略。从这个角度看，启动迁移的初始步骤，本身就是一次对安全治理的全面升级。

在此战略框架下，我国国家重点研发计划“抗量子迁移体系架构顶层设计”（课题编号：2023YFC3305501，即“055 项目”）提出了专门针对银行业等关键信息基础设施的迁移参考架构。该架构深刻洞察到金融行业对高可信、高稳定性和互操作性的严苛要求 ，不仅在顶层设计上与美国 NIST 最新发布的“网络安全框架 2.0”（CSF 2.0）保持战略一致 ，更创新性地引入了“密码敏捷性科学”。项目团队明确提出，银行业的迁移不应止步于算法替换，而必须构建一套包含“实施敏捷性、合规敏捷性及平台敏捷性”的综合治理体系。通过建立精准的密码资产清单、制定分阶段的迁移规划以及实施严格的互操作性测试 ，055 项目旨在为复杂的金融遗留系统提供一条风险可控的演进路径，确保在应对未来量子威胁的同时，不破坏现有金融业务的连续性与稳定性。这正是将“战略远见”转化为“工程实践”的最佳范例。

3.2.1 从清单到情报：数据驱动的加密资产发现

在行动之前，必须首先全面了解组织当前的加密状况。这正是 PQC 迁移中最核心的“无悔之举”——加密资产管理（Cryptographic Asset Management）。建立一份全面的加密资产清单，不仅是 PQC 迁移的先决条件，更是现代网络风险管理的基础。它能帮助组织在面临任何密码学漏洞（无论是否与量子相关）时，都能快速响应，从而提升整体安全韧性。

一个数据驱动的敏捷迁移框架为此提供了核心指导，它超越了简单的资产盘点，强调以“数据”为核心进行全方位分析：

以数据流向为主线：追踪敏感数据在系统中的完整生命周期，绘制出与业务紧密关联的动态加密地图。

以数据类型为准则：根据数据的 保密寿命 对其进行分类。需要保存数十年的长期合同，与仅需短期保密的会话数据，其面临的“先窃取，后破解”（HNDL）风险等级截然不同。这种分类方法能够直接为迁移工作的优先级排序提供决策依据。

以数据兼容度为标尺：评估新的 PQC 解决方案与现有数据处理路径的兼容性，度量不同迁移方案的“敏捷度”。

通过这一数据驱动的方法，组织能够构建一份远比静态清单更深刻、更具洞察力的加密资产视图，为后续的风险评估和战略规划奠定坚实的情报基础。这一过程也催生了专业的咨询、风险评估、密码资产清单管理等服务市场，市场研究机构普遍预测市场将经历爆炸性增长，预计到 2034 年的复合年均增长率（CAGR）将处于 37%至 47% 的高位区间。

3.2.2 全面的风险评估：可视化系统性风险

在掌握了内部加密资产状况后，必须结合对外部威胁的全面分析，构建完整的风险图景。这需要一个覆盖“风险识别-评估预警-迁移监管”全链条的理论框架。

首先，在风险识别层面，系统性地梳理信息系统在算法、协议和业务层面临的量子脆弱性，绘制一份详尽的风险点清单（Risk Point Inventory）。

其次，在风险评估层面，通过构建风险矩阵（Risk Matrix），结合风险发生的概率和造成的影响两个维度，对不同风险进行评级。

更为关键的是，必须对风险的传导机制进行建模。量子攻击的影响并非孤立的，它可能通过系统间的内在联系引发连锁故障。通过绘制风险传染图谱（Risk Contagion Map），可以直观地展示风险的传导路径。例如，一个针对外部网站的攻击，不仅可能导致该系统的数据泄露，还可能因为数据交互而将风险扩散至整个企业生态。这张图谱是转化和理解 HNDL 威胁的关键工具，它将潜在的、延迟的威胁，转化为当前可见的、可分析的系统性风险，从而极大地提升了决策者对迁移紧迫性的认知。这也意味着，系统的迁移优先级不仅取决于其承载数据的保密寿命，更取决于其在风险传染图谱中的“连接度”。

这项初步评估为引擎提供了点火能量，并将随着引擎的运转/加速，通过后续“执行与验证”阶段收集到的真实世界数据不断进行优化。

3.3 构建动能：抗量子密码技术堆栈

核心要点：

一个组织机构需要的是一个多样化的 PQC 工具组合，而非单一解决方案。本章解释了投资于正确的软硬件组合将如何确保组织机构的业务在保持安全的同时，也能维持卓越的性能。

为使引擎输出持续强劲的动力，必须构建一个坚实、高效且全面的技术堆栈。这个技术堆栈赋予引擎以“核心动力总成”，确保迁移过程既安全可靠，又能在核心业务的严苛性能要求下平稳运行。这正是市场三维重构中“技术多样性裂变”维度的体现。

3.3.1 算法组合：为通用场景定制的密码工具箱

不存在一种“万能”的 PQC 算法，最佳选择总是取决于具体的应用环境和安全需求。组织需要的是一个经过精心筛选和优化的算法组合（Algorithm Portfolio），以应对其多样化的业务场景。PQC 的发展已呈现出基于格、编码、哈希、多变量、同源等多种数学难题构建的算法并存发展的“百花齐放”局面。

基于格的密码（Lattice-Based Cryptography）：以 NIST 标准化的 ML-KEM[12] (Kyber) 和 ML-DSA[13] (Dilithium) 为代表，是当前发展最成熟、性能最均衡的技术路线，在 NIST 首批标准中占据主导地位，适用于构建安全通信信道等通用核心场景。

基于哈希的签名（Hash-Based Signatures）：以 NIST 标准化的 SLH-DSA[14] (SPHINCS+) 为代表，其安全性仅依赖于底层哈希函数的强度，是一种极为保守和可靠的选择。它适用于对安全性有最高要求、可以容忍性能开销的场景，如为根证书颁发机构（Root CA）签发证书、签署固件更新等。

基于多变量的密码（Multivariate Cryptography）：以 UOV 等为代表，其突出优势在于极快的签名和验证速度，特别适合需要处理海量签名验证的场景，如大规模物联网设备认证或高频业务系统。

基于编码的密码（Code-Based Cryptography）：以 HQC 为代表，作为格密码的备用方案，提供算法多样性，适用于加密速度至关重要的场景。

算法家族	标准化范例	相对密钥/签名尺寸	相对性能	安全性基础	主要应用场景
格密码	ML-KEM (Kyber), ML-DSA (Dilithium)	中等	良好/优秀	在高维格中求解最短向量问题 (SVP) 等难题的困难性。	通用核心场景：TLS/IPsec 安全通道建立、业务数据加密与签名、云服务数据保护。
基于哈希的签名	SLH-DSA (SPHINCS+)	极大（签名）	慢（签名）	底层加密哈希函数（如 SHA-256）的安全性。	高保障、长周期场景：根 CA 证书签发、系统固件/软件更新签名、长期合同与法律文书的归档签名。
多变	UOV	公钥大，	验证速	求解多元二	高频验证场景：大规模设备

量密码		签名小/中	度极快	次多项式方程组的困难性。	（如 POS 机）身份认证、高频业务系统的签名验证、内部风控系统。
基于编码的密码	HQC	大（公钥）	快（加密）	一般线性码的解码难题。	KEM 备份与算法多样性：作为格密码的备用方案，适用于加密速度至关重要的场景。

表 3-2 ： 面向企业场景的 PQC 算法组合策略

3.3.2 实现引擎：软硬件协同设计

鉴于 PQC 算法普遍存在的性能开销（更大的计算量、密钥和签名尺寸），仅有算法理论是远远不够的。必须通过软硬件协同设计，构建一个强大的实现引擎，确保 PQC 能够在系统的高负载下高效运行。这种实现策略必须是差异化的。

硬件加速层：对于后台核心业务系统等需要处理海量并发请求的场景，硬件加速是必由之路。这催生了对抗量子芯片、协处理器及 ASIC/FPGA 上的优化实现等针对性硬件创新。这包括为数据中心量身打造的抗量子服务器密码机。

优化软件层：对于服务器端的通用计算环境和客户端的资源受限环境，必须提供高度优化的软件实现。

CPU 平台软件模块：针对主流 X86 服务器平台，通过缓存优化、自动向量化（SIMD 指令集利用）等技术，在纯软件层面实现卓越性能。

移动端 SDK：针对计算和内存资源有限的移动设备，必须开发专用的轻量化 SDK。通过采用 NEON 汇编指令对核心计算模块进行深度优化，可成功研制适用于 Android 和 iOS 平台的 PQC SDK，为移动应用的安全迁移提供了关键技术支撑。

一个坚实的技术堆栈构成了战略引擎的核心‘动力总成’，确保了动力的持续输出与系统的稳定运行。这些技术选择将在‘执行与验证’阶段得到检验，其性能数据又将反馈回来，为未来的引擎性能调优提供依据。

3.4 加速引擎：仿真与验证模块

核心要点：

任何战略规划都必须在现实世界中得到检验。本章描述的验证平台和工具集，是确保 PQC 迁移计划平稳落地、避免业务中断并控制实施风险的关键。

拥有了战略远见和坚实的技术堆栈之后，下一步便是将迁移引擎付诸实践，在真实的业务环境中构建和加速其动能。这一阶段的核心是“仿真与验证”，它通过一个高保真的验证环境和一套完备的工具集，将理论规划转化为可度量、可控制、可迭代的部署行动，并直接应对迁移过程中最严峻的现实挑战。

3.4.1 量子就绪的工具集

为了高效、安全地执行迁移，需要研发一套完整的“量子就绪工具集”，为组织提供了从算法库、协议库到评估软件的全方位支持。这个工具集是执行阶段的“兵器库”，确保迁移的每一个环节都有精准的工具可用，包括经过充分验证和性能优化的抗量子密码适配算法库和协议库、能够签发混合 X.509 证书的证书管理工具，以及用于合规性与安全性检查的评估软件。

3.4.2 高保真验证环境：迁移试验平台

理论和实验室测试远不足以应对业务的复杂性。PQC 方案在投入生产前，必须在尽可能接近真实环境的条件下进行严苛的验证。为此，需要构建一个核心的验证设施——抗量子密码迁移试验平台。这个平台不仅是一个测试场，更是演练和优化迁移策略、积累实践经验的“高保真模拟器”。

该平台的核心能力体现在两个方面：

工程化验证（Engineering Validation）：平台能够模拟行业典型业务场景（如移动应用、Web 平台），注入真实的业务报文，完成端到端全链路测试。通过这种方式，可以精准、量化地评估 PQC 方案对业务性能（如延迟、吞吐量）的实际影响，识别潜在的性能瓶颈和兼容性问题。

灰度演进（Gray-Scale Evolution）：平台内置了强大的策略编排和版本治理引擎。通过策略调度，平台可以灵活地组合传统密码与 PQC 算法，实现双轨并行运行，并按需将不同比例的流量引导至新方案。版本治理机制则支持对算法、协议等进行分阶段的 A/B 测试、金丝雀发布，并具备在出现异常时自动触发的风险回退能力。这使得迁移过程从高风险的“一刀切”切换，转变为一个风险可控、过程可观测、结果可度量的动态演进闭环。

关键迁移挑战	挑战描述	引擎框架中的应对组件/策略	具体技术示例

性能开销与资源限制	PQC 算法的计算复杂度和更大的密钥/签名尺寸，对系统性能和资源受限设备构成压力。	技术堆栈：实现引擎	硬件加速： 部署抗量子服务器密码机，实现 21 万次/秒的加密性能。 软件优化： 为移动应用提供基于 NEON 汇编优化的轻量级 SDK。
供应链复杂性与依赖风险	企业的 IT 系统由大量第三方软硬件构成，任何一个组件不支持 PQC 都可能成为迁移的瓶颈。	核心原则：密码敏捷性设计	协议层敏捷： 采用异构认证密钥交换协议，允许与尚未升级的第三方系统进行安全通信。 架构层敏捷： 插件化的算法集成框架，支持快速替换加密库。
遗留系统集成	大量“影子密码”深藏于无法直接升级的遗留系统中，发现和改造极为困难。	执行引擎：灰度演进 核心原则：密码敏捷性设计	风险隔离： 对于无法改造的系统，通过支持 PQC 的安全网关进行“封装”保护。 兼容性设计： 使用混合 X.509 证书，确保新系统签发的证书仍能被遗留系统验证。
实施风险与迁移失败	不当的 PQC 实施可能引入新的安全漏洞，导致安全性不升反降。	执行引擎：高保真验证	全链路测试： 在迁移试验平台上注入真实业务报文，进行端到端的功能、性能和安全验证。自动化回退： 利用平台的灰度演进能力，在监测到异常时自动回滚至稳定的传统密码方案。

表 3-3 ： 迁移挑战与引擎框架的应对策略矩阵

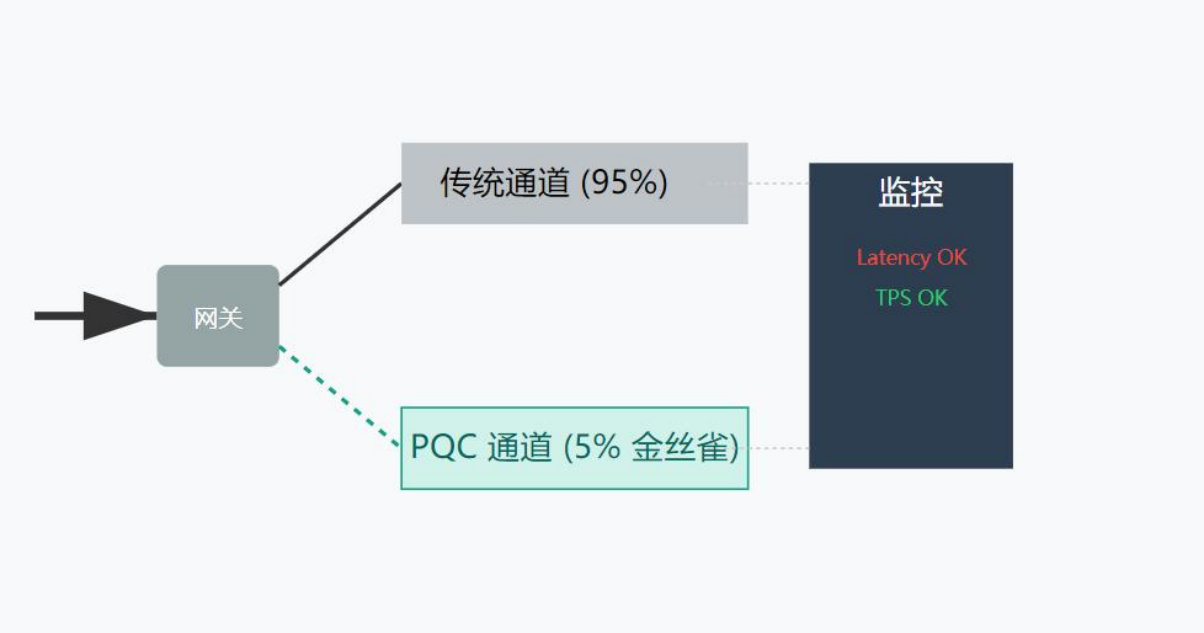


图 3-3： 风险可控的灰度迁移机制

至关重要的是，迁移试验平台不仅是执行和验证的终点，它更是引擎实现‘智能增压’的关键。在验证过程中产生的所有数据——性能指标、兼容性报告、故障日志——都是极其宝贵的新情报。这些情报会实时反馈回引擎的“战略远见”阶段，用于动态修正风险评估、调整迁移优先级和优化技术方案。正是这个由“执行-验证-反馈”构成的闭环，将一个线性的迁移过程，转变为一个持续学习、持续优化的螺旋式上升循环。引擎每完成一个循环，都会积累更多的经验和数据，使得后续的动力输出更加高效。

3.5 维持动能：治理与动态演进

量子安全迁移战略引擎一旦启动，其目标并非是达到某个静止的“完成”状态，而是进入一个持续运转、不断适应和演进的良性循环。为了维持引擎的动力并确保其长期有效，必须建立一个强大的治理框架。这个治理循环是引擎的 ECU（电子控制单元），它确保引擎的运转始终与组织战略、外部环境和新兴威胁保持同步。

3.5.1 建立常态化的治理结构

PQC 迁移的长期性要求将其从一个临时性项目，转变为企业风险管理和技术治理的常态化组成部分。这需要建立一个明确的、多层次的治理结构，以确保持续的监督、决策和资源投入。一个可供借鉴的模型包括：由高级管理层组成的 领导小组 、由内外部专家组成的 专家委员会，以及负责日常执行的 项目工作组。重要的是，该治理模型被设计为能够与企业现有的风险管理（ERM）框架（如 ISO 31000 或 COSO）无缝对接

和整合，将 PQC 风险纳入企业整体的风险管理视图中，从而使用高层领导已经理解和信任的语言和结构进行沟通。

3.5.2 打造持续的情报与反馈闭环

治理循环的核心是建立一个正式的、持续的情报反馈机制，确保引擎能够根据最新的内外部信息进行动态调整。

内部反馈：必须将从迁移试验平台和生产环境中收集到的监控数据制度化地反馈给“战略远见”团队。这些一手数据是修正风险模型、优化技术方案的最宝贵输入。

外部情报：必须指定专门的团队或角色，建立量子威胁情报与监测网络，负责持续追踪全球 PQC 的发展动态，包括 NIST、IETF、中国 CSTC 等国际标准组织的最新进展，以及新的密码分析成果。由于 NIST 标准与中国国密 PQC 标准并存可能导致技术路线分化，这种持续的情报对管理互操作性风险至关重要。

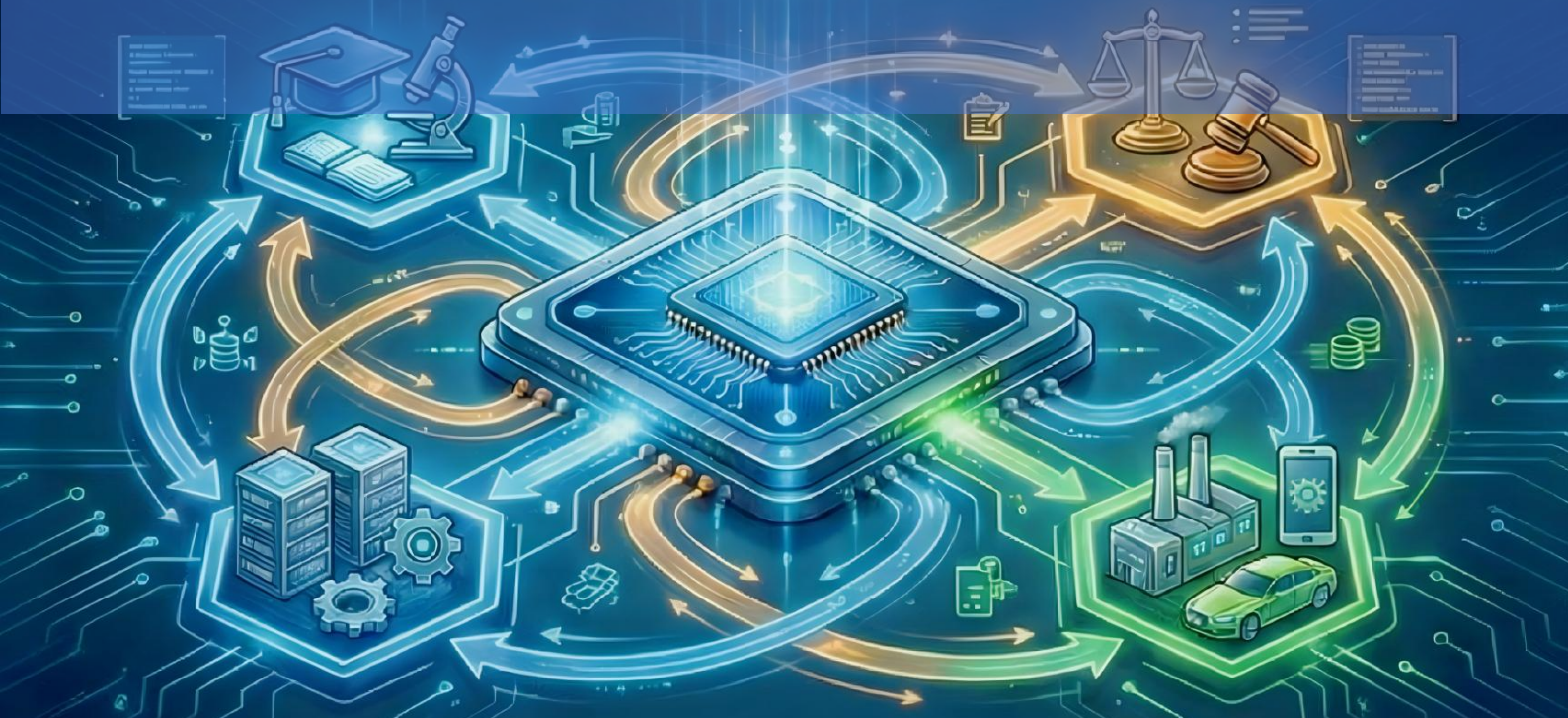
3.5.3 投资于“人类防火墙”

技术和流程最终需要由人来执行。先进的算法和平台如果缺乏具备相应知识和技能的专业人才来规划、实施和维护，PQC 迁移同样会失败。当前，掌握 PQC 算法、实施迁移、进行安全评估的专业人才相对稀缺，构成了人力资源瓶颈。因此，对人才的投资是维持引擎动力的最根本保障。成功的 PQC 专家需要具备跨学科的复合能力，包括深厚的密码学理论、卓越的软件工程能力、系统架构与硬件知识，以及风险管理与战略规划能力。组织应建立内部培训计划，并通过与高校和研究机构建立联合实验室等方式，系统性地构建人才梯队，弥合人才鸿沟。

一个强大的治理循环，通过为引擎的长期运转提供稳定的能量和正确的方向，确保引擎不会因项目结束而熄火，而是作为一个动态的生命体，持续从“执行与验证”阶段汲取养分，为新一轮的“战略远见”提供更精准的输入。

第四章

量子安全的经济学、生态系统与未来



第四章 量子安全的经济学、生态系统与未来

本部分将探讨成功实施迁移引擎的更广泛背景和深远影响，分析其经济合理性，展示驱动引擎的强大生态系统，并展望其在下一代技术浪潮中的应用前景。

4.1 跨越量子鸿沟的经济学：投资、风险与机遇

将 PQC 迁移从技术议题提升至战略决策层面，需要清晰地理解其经济学原理。投资于 PQC 不仅是避险，更是投资于数字经济的“盾”；相比于量子计算硬件这支高风险的“矛”，PQC 提供了由全球合规驱动的、确定性的市场增长逻辑。这不仅是一笔安全开销，更是一项对企业未来韧性和市场竞争力的战略投资。

4.1.1 不作为的代价：量化“量子安全债务”

推迟 PQC 迁移并非零成本决策，它实际上是在积累一种“量子安全债务”。这种债务的核心由“先窃取，后破解”（HNDL）攻击的风险构成，其潜在的财务影响是巨大的，包括知识产权的永久性损失、巨额的监管罚款以及品牌声誉的崩塌。

4.1.2 迁移的投资回报（ROI）：投资于数字信任

PQC 迁移的总拥有成本（TCO）是巨大的。虽然美国联邦政府基于早期规划给出的预算预估约为 71 亿美元，但这被业界普遍视为一个极为保守的下限（Conservative Floor）。考虑到庞大的遗留系统发现成本、复杂的供应链依赖以及长周期的“双轨”运行需求，实际的行业迁移总开销预计将数倍于此，甚至达到数百亿美元的量级。

然而，这笔投资的回报是多维度的。最直接的回报是清偿了“量子安全债务”，避免了灾难性的财务损失。更重要的是，在一个日益关注数据安全的市场中，率先完成 PQC 迁移的企业可以将其作为一项强大的竞争优势。能够向客户和合作伙伴证明其数据具备长期安全性，将成为赢得高端合同和客户忠诚度的关键。随着大型企业和政府机构将 PQC 合规性作为其供应商选择的硬性标准，早期完成迁移的企业将在供应链中获得优先准入和更强的议价能力。

4.1.3 市场机遇：PQC 驱动的指数级跃迁

全球 PQC 市场正在经历爆炸性增长。基于对存量市场替代和新兴市场增量的双重驱动，PQC 市场规模有望实现指数级增长。我们可以用一个简化的三层渗透模型来理解其潜力：

$$V_{PQC} = (S_{legacy} \times \alpha) + (S_{emerging} \times \beta) + V_{services}$$

其中：

V_{PQC} 是 PQC 市场的总规模。

S_{legacy} 代表需要进行 PQC 升级的传统密码学应用市场存量规模。

α 是 PQC 在存量市场的替代率。

$S_{emerging}$ 代表由数字化转型催生的、直接采用 PQC 的新兴应用市场规模。

β 是 PQC 在新兴市场的渗透率。

$V_{services}$ 代表伴随 PQC 部署而产生的咨询、集成、运维、监测等服务市场规模。

据多家市场研究机构预测，全球 PQC 市场规模预计将从 2025 年的约 4 亿至 16 亿美元，以高达 37%以上的年复合增长率，在 2034 年增长至近 70 亿至 100 亿美元。资本市场正逐渐将“密码敏捷性平台”视为核心数字基础设施资产，其价值在于为企业提供了长期的合规护城河，是实现长期社会价值与经济回报统一的关键抓手。

4.2 量子就绪联盟与实践先驱

抗量子迁移已不再是理论探讨，全球技术领导者已经开始在数亿用户规模的实际产品中部署 PQC，为整个行业树立了标杆，证明了大规模 PQC 部署的可行性。

谷歌： 在其 Chrome[32]浏览器中试验并部署了基于 ML-KEM[12]的混合密钥交换机制，保护 TLS 连接，并在其云密钥管理服务中增加了对 PQC 数字签名的支持。

苹果： 为其 iMessage[31]发布了名为 PQ3 的突破性后量子加密协议，其最显著的创新在于实现了后量子密钥的持续更新（rekeying），为端到端加密通信树立了新的安全典范。PQ3 的推出将从 iOS 17.4、macOS 14.4 等版本开始。

微软： 致力于将 PQC 能力深度集成到其 Windows 和 Linux 操作系统中，通过在 Windows Insiders 版本中向 Cryptography API: Next Generation (CNG) 添加对 ML-KEM[12]和 ML-DSA[13]的支持，极大地降低了企业在其现有 IT 环境中采用 PQC 的门槛。

Meta: 已在其内部 TLS 流量中采用基于 Kyber[12]的混合密钥交换机制，作为过渡时期的纵深防御策略。

Signal： 作为安全通信领域的“黄金标准”，Signal 于 2023 年 9 月推出了 PQXDH（Post-Quantum Extended Diffie-Hellman）协议[30]。这是全球首个在大规模消费者应用中落地的 PQC 混合密钥协商协议，证明了 PQC 可以在不牺牲通话延迟等用户体验的情况下进行部署，并直接带动了 WhatsApp 等后续应用的跟进。

Zoom： 2024 年 5 月，Zoom 宣布在其 Zoom Workplace 等产品中支持端到端加密（E2EE）的后量子升级，成为首个大规模部署 PQC 的企业级视频会议平台。这一举措填补了企业协作工具迁移的空白，验证了 PQC 在实时音视频流等高带宽、低延迟场景下的可行性[33]。

Linux 基金会 (PQCA)：开源生态的基石此外，必须特别关注的是 2024 年 2 月由 Linux 基金会牵头成立的 PQC 联盟（PQCA）。该联盟联合了 AWS、IBM、Google、NVIDIA 等科技巨头及滑铁卢大学等顶尖科研机构 ，旨在为全球提供生产就绪（Production-ready）的开源 PQC 软件实现。通过整合知名的 Open Quantum Safe 项目和新推出的 PQ Code Package ，PQCA 致力于构建符合 NSA CSNA 2.0 标准的高安全性开源算法库。这意味着 PQC 的能力将被标准化地注入到开源生态的底层代码中，极大降低了全球开发者获取 PQC 能力的门槛，并确保了整个软件供应链在未来面对量子威胁时的密码敏捷性。

4.2.1 联盟即引擎整体：从寡头垄断到多元共生

PQC 市场的兴起打破了传统密码市场由少数寡头垄断的稳定结构，催生了一个更加复杂、动态和多层级的“多元共生”生态系统。一个强大的生态系统是成功实施迁移引擎的关键。本白皮书的发布联盟，其组织架构本身就是战略引擎框架的物理体现，旨在为客户提供一个“开箱即用”的、能够驱动引擎所有阶段的集成化能力。

4.2.2 战略远见与算法引擎

西交利物浦大学 PQC-X 实验室：由 NIST 标准 ML-KEM[12]的核心设计者之一丁津泰教授领衔，其兼具“矛”（密码分析）与“盾”（算法设计）的双重能力，为引擎的“战略远见”阶段提供最权威的风险评估和算法选型指导。该实验室致力于抗量子迁移通用关键技术的研发和技术转移，旨在构建一个开放式的国际化研发与技术转移中心。

重庆大学信息物理社会可信服务计算教育部重点实验室：依托指导委员会专家向宏教授在国际标准组织（如 ETSI）的深厚影响力，该实验室专注于信息物理社会系统（CPSS）的安全治理与国际标准协调。作为联盟的“战略雷达”，它负责追踪全球 PQC 标准演进（特别是 NIST 与 ETSI 动态），为联盟提供跨越技术与社会治理维度的宏观战略情报，确保迁移方案具备国际互操作性与合规性。

技术堆栈引擎（硬件基石与软件框架）：联盟实现了“软硬协同”的闭环能力。在硬件层面，以国芯科技研制的自主可控 PQC 芯片（如 AHC001）为代表，确立了算力底座；在软件层面，朗空量子等成员构建了完整的敏捷框架与 SDK。两者通过深度协同设计，共同构成了驱动引擎运转的强劲“技术堆栈”。

云钞金融服务（北京）有限公司（云钞金服）： 作为聚焦于金融量子安全科技前沿的国家级高新技术企业，云钞金服由国家金融安全及系统装备工程技术研究中心与中国人民银行所属全资企业联合创立。公司确立了“数字工程、融合工程、创新工程”三大战略核心，致力于构建自主可控的金融安全屏障。在联盟中，云钞金服发挥其作为科技部国家重点研发计划“银行业及其关键基础设施信息系统 PQC 迁移技术研究”项目核心参与单位的技术优势，重点推动 PQC 技术在金融基础设施的深度应用。其关键贡

献包括：构建数字货币安全系统，为发行、流通全流程提供抗量子加密；实施金融基础设施升级，将 PQC 技术融入区域现金处理中心、数字化智能金库及无人银行系统；以及提供量子安全的征信与数据服务，保障敏感金融信息的传输安全。云钞金服正致力于成为量子时代领先的金融数字安全服务商与产业创新引领者。

这种优势并非简单的学术联系，而是一种能够深刻洞察全球两大 PQC 标准体系演进的战略情报能力。白皮书已明确指出，“全球标准分歧与合规摩擦”是 PQC 迁移面临的重大政策挑战之一。通过向宏教授在国际标准组织（如担任 2017 年 ETSI QCS 年会 PQC 分组主席、成功争取 ETSI 及 PQCrypto 等顶级国际会议首次在华举办）和国内标准制定的深度参与，联盟获得了直面这一挑战的核心能力。对于业务遍布全球的客户而言，这意味着联盟不仅能提供技术层面的迁移方案，更能就如何应对 NIST 标准与中国国密标准并存的复杂局面提供战略咨询，帮助其设计具备高度密码敏捷性[23]的架构，从而在管理供应链风险、确保未来互操作性方面获得决定性优势。这实质上将联盟的角色从技术实施方，提升到了 PQC 领域的地缘技术风险战略顾问。

4.2.3 仿真与验证引擎

朗空量子 提供了迁移框架和工具集，而上海巡天千河 （航天）以及金融与能源领域的专业联合实验室则提供了最真实的行业试验场，共同构成了引擎的“仿真与验证生态”。

4.2.4 治理与人才培养

PQC-X 实验室计划在三年内培养 20-50 名 PQC 专家，直接为“治理循环”中的“人类防火墙”提供燃料，确保持续的动能。

重庆大学信息物理社会可信服务计算教育部重点实验室的加入，则弥补了技术与社会信任之间的鸿沟。该实验室将致力于建立 PQC 迁移的社会信任模型与治理框架，研究如何在复杂的信息物理系统（CPS）中建立可验证的信任链。同时，依托其教育部重点实验室的平台优势，重点培养具备全球视野的标准化专家与安全治理人才，为维持引擎动力提供高端智力支持。

这种设计并非巧合，而是一个为系统性解决 PQC 迁移挑战而精心构建的战略共同体。联盟不是一个松散的伙伴关系，而是一个活的、呼吸的、随时可以部署的迁移引擎。

4.2.5 资本与市场引擎

资本与市场引擎（产业孵化与资源配置）： 为了跨越科研成果转化的“死亡谷”，联盟引入了专业的产业资本力量。战略投资合作伙伴专注于解决“矛与盾”的产业融合命题，作为联盟的战略投资与产业孵化引擎，通过“耐心资本”支持 PQC 敏捷性平台

等基础设施的建设，打通技术与资本的循环，加速 PQC 技术的商业化落地与并购整合，为生态系统提供持续的资金血液与战略导航。

伙伴机构	核心专长	联盟角色	关键贡献与技术	代表性经验/产品
西交利物浦大学 PQC-X 实验室	PQC 算法设计与密码分析	算法引擎	自主 PQC 算法研发；NIST 标准（ML-KEM）核心设计；高级密码分析（攻破 GeMSS, LUOV）；SVP 挑战赛世界纪录	丁氏密钥交换；Rainbow, UOV, TUOV 签名算法设计
重庆大学信息物理社会可信服务计算教育部重点实验室	信息物理社会系统(CPSS)安全；国际标准治理	治理与战略引擎	国际标准协调；社会信任模型构建；高端人才培养	深度参与 ETSI 等国际标准制定；拥有复杂系统可信计算理论成果
苏州朗空后量子科技有限公司（朗空量子）	全栈 PQC 工程化与产品化	商业化引擎	PQC 敏捷框架；SDK；云 SaaS 平台；AI 辅助迁移模型	“朗空量子护盾”框架；已成功应用于 AI 大模型（DeepSeek）安全与 Hyperledger Fabric 的抗量子迁移
苏州国芯科技股	自主 CPU 核；安	硬件基石	研制高性能、自	AHC001 抗量子

份有限公司	全芯片设计与量产		主可控的 PQC 芯片与密码卡；抗侧信道攻击（SCA）设计	密码芯片（28nm 工艺，自主 CPU 核）；CCUPHPQ01 抗量子密码卡
云钞金融服务（北京）有限公司（云钞金服）	金融基础设施抗量子升级；数字货币安全；国家重点研发计划核心参研	金融基础设施与数字货币安全引擎	研发抵御量子攻击的新一代金融安全基础设施；构建数字货币发行、流通、存储全流程安全加密体系；金融征信数据抗量子传输保护	国家重点研发计划核心单位；数字货币安全系统；区域现金处理中心
上海巡天千河空间技术有限公司	商业卫星研制与在轨验证	行业试验场（航天）	提供卫星通信场景适配与在轨/高仿真环境测试	领先的商业卫星 ODM 制造商；拥有低成本新技术在轨验证平台

表 4-1 ： 量子就绪联盟伙伴与能力矩阵

第五章

特定行业的战场：根据行业现实调整迁移策略

第五章 特定行业的战场：根据行业现实调整迁移策略

抗量子迁移并非“一刀切”的过程。不同行业的业务特性、监管环境、数据敏感度和设备生命周期差异巨大，因此必须量身定制迁移策略，为各自的“迁移引擎”进行精确“调校”。迁移策略的紧迫性和优先级，在很大程度上取决于该行业典型的“数据寿命”（数据需要保持机密的时间）和“设备寿命”（设备在现场的服役年限及其可升级性）这两个核心因素。本章将展示如何将抽象的“迁移引擎”框架具体应用于不同关键领域的独特运营现实，从理论走向实践，提供量身定制的行动手册。

图 5-1： 战略分诊——迁移优先级决策矩阵

5.1 行业特定行动手册：引擎适配

5.1.1 关键基础设施（金融+能源+电网）

5.1.1.1 金融服务

独特挑战：金融服务业面临双重极端挑战：一方面，核心交易系统要求极低的延迟和极高的吞吐量；另一方面，大量金融数据（如抵押贷款合同、保险单）的保密寿命长

达数十年，使其成为“先窃取，后破解”（HNDL）攻击的最高价值目标。作为国家金融体系的“压舱石”，金融银行业的 PQC 迁移对于防范和化解重大经济金融风险至关重要。

引擎调校：

技术堆栈：在技术选型上，必须优先部署高性能的 PQC 硬件安全模块（HSM）和专用密码卡（如联盟成员国芯科技研制的 CCUPHPQ01 密码卡），以加速核心交易处理，满足签名速率不低于每秒 4000 次、验签速率不低于每秒 8000 次等严苛的性能指标。

执行与验证引擎：必须利用专业的验证平台。例如，联合行业头部金融机构，共同利用行业领先的金融安全创新平台，在覆盖手机银行、网上银行和跨行交易三大核心业务场景的高仿真环境中，对 PQC 方案进行全面的功能、性能和安全验证，确保客户终端的平滑过渡。

5.1.1.2 能源与公用事业（电网）

独特挑战：能源与电网领域最大的挑战在于保护其工业控制系统（ICS）和运营技术（OT）。这些系统的生命周期极长（通常超过 20 年），且通常被设计为“安装后即固定”，难以甚至无法进行直接的软件或固件更新。同时，电力系统对高可靠性和实时性的要求不容任何妥协。

引擎调校：

技术堆栈：技术选择必须倾向于轻量级、低功耗且具备高可靠性的 PQC 芯片和密码模块。这需要与具备国家电网核心芯片研发能力的专业伙伴紧密合作，确保方案满足工业级标准。

执行与验证引擎：由于无法直接改造遗留系统，核心策略是采用“封装”保护。通过部署支持 PQC 的安全接入网关（由在能源领域有深厚部署经验的专业设备厂商开发），在不触动现有 OT 系统的情况下，为其外部通信提供 PQC 安全保障。所有方案必须在模拟电网运行的专业实验室环境中，进行全面的仿真验证和安全攻击测试。

5.1.2 长周期设备（工业物联网+车联网+卫星）

5.1.2.1 工业互联网与物联网（IIoT/IoT）

电信行业的全球共识（2025）：3GPP 在其 Release 19 标准冻结及 Release 20 的预研中，正式接纳了针对 5G 核心网（5G Core）和用户身份模块（SIM/eSIM）的后量子迁移技术规范。GSMA（全球移动通信系统协会）随之发布了《电信行业后量子迁移白皮书 2.0》，警告全球运营商必须在 6G 商用前完成基础设施的 PQC 升级[29]。

独特挑战：工业物联网面临着海量（数以亿计）的资源受限设备，这些设备的计算能力、内存和功耗都极为有限。同时，这些设备通常部署在难以物理接触的环境中，大

规模的固件空中下载（OTA）更新极具挑战性。其长生命周期使其成为 HNDL 攻击的理想目标。

引擎调校：技术堆栈的选择必须优先考虑为资源占用而优化的轻量级 PQC 算法（如 Falcon 和 Kyber[12]），并采用专为物联网网关设计的紧凑型硬件（如 Mini-PCIe 抗量子密码卡）。至关重要的是，必须使用 PQC 数字签名来保护 OTA 更新过程本身的安全，防止恶意固件被分发。

5.1.2.2 智能网联汽车（ICV）

独特挑战：V2X（车对万物）通信的安全性直接关系到驾乘人员的生命安全和道路交通的公共安全。一辆汽车的生命周期通常超过 15 年，这意味着今天出厂的汽车，其安全系统必须能够抵御 2040 年及以后的网络威胁。因此，PQC 能力必须在整车电子电气架构（EEA）的初始设计阶段就进行深度集成。

引擎调校：迁移重点是将 PQC 改造作为整车 EEA 安全投入的核心组成部分，在车载单元（OBU）和路边单元（RSU）中部署适用于车载环境的紧凑型 PQC 密码卡，以保护长生命周期车辆的通信安全和身份认证。

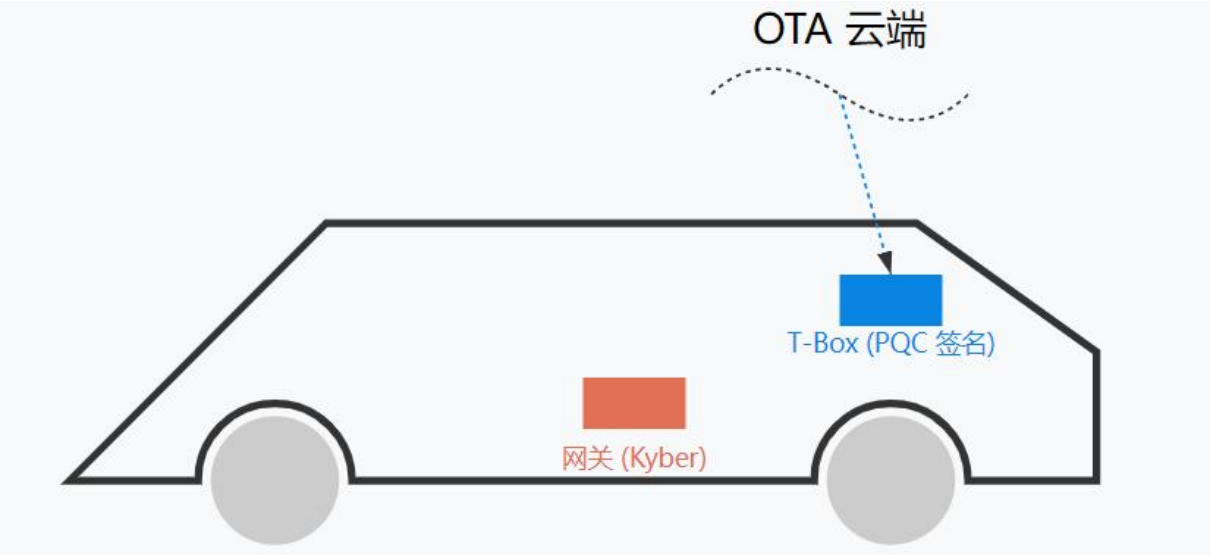


图 5-2： 软件定义汽车的量子免疫系统（ICV EEA）

5.1.2.3 卫星通信

独特挑战：空间环境极为严苛，卫星上的资源（计算能力、功耗、存储）高度受限，通信链路具有高延迟和有限带宽的特点。一旦发射入轨，硬件升级几乎不可能。此外，还需考虑抗空间辐射的设计。

引擎调校：必须与国内领先的商业卫星 ODM 制造商上海巡天千河等专业伙伴合作，研究 PQC 算法的轻量化实现，并开发抗辐射的 ARM 加密模块。在执行验证阶段，利用

其在轨验证平台或高仿真空间环境实验室，对“星地协同分层加密”等创新方案进行全面测试与评估，确保在严苛条件下星地码速率大于 1kbps 且误码率低于10^{-4}。

5.1.3 新型数字生态（AI+区块链+Web）

5.1.3.1 人工智能与先进机器人系统

PQC 对于保护大规模 AI 模型、训练数据以及用户交互隐私至关重要。联盟成员朗空量子的技术框架已成功应用于保护 Qwen、DeepSeek 等 AI 大模型的通信与数据库安全。对于具有长服役周期的具身智能机器人，PQC 是确保其控制指令和数据流安全，防止物理安全风险的关键防御策略。

5.1.3.2 Web3.0 与区块链

DApps、数字身份、DAO 治理等新兴范式的安全性深度依赖底层密码学的健壮性。项目负责人丁津泰教授拥有“抗量子区块链”相关专利，联盟成员朗空量子的“朗空量子护盾”框架也已成功用于 Hyperledger Fabric 分布式操作系统的抗量子迁移。在 DAO 等社区中，规划和部署抗量子攻击的防护措施已成为发展趋势。

5.1.3.3 生命科学与医疗健康

基因组数据、电子病历（PHI）等是需要长期保存的高度敏感信息，其全生命周期的安全防护变得空前重要。该领域是 PQC 解决方案的主要需求方之一。引擎调校重点是采用能够抵御未来量子攻击的强加密手段，利用 PQC 数据封存与销毁系统对医疗记录进行长期安全存储和合规销毁，催生量子安全数据存储与处理的细分市场。

这些行业特定的行动手册揭示了一个核心原则：PQC 迁移策略的紧迫性和优先级，在很大程度上取决于该行业典型的“数据寿命”和“设备寿命”。引擎框架的灵活性使其能够针对这些不同需求进行有效调校。

5.2 新的疆域：抗量子密码在人工智能与物理安全中的应用

一个成功运转的迁移引擎所构建的，不仅仅是防御能力，更是一种可以应用于下一代安全挑战的创新能力。PQC 的应用正迅速超越传统的通信加密范畴，进入人工智能安全和物理资产认证等新领域。

5.2.1 保障自主未来：抗量子密码赋能人工智能安全

人工智能系统，特别是自主智能体（AI Agent），其核心功能就是处理和创造具有长期保密价值的高价值数据（如企业的战略规划、研发成果），这使其成为 HNDL 攻击

的天然目标。一个新兴的多层次纵深防御架构，正通过结合 PQC 与隐私保护计算（PPC）技术，为 AI 系统提供端到端的、经得起未来考验的保护。

通信安全（传输中数据）：通过在 TLS 等协议中集成 PQC 算法（如 ML-KEM[12]），确保 AI 智能体的所有外部通信都能抵御量子解密攻击。

情报完整性（静态数据与代码）：利用 PQC 数字签名技术（如 ML-DSA[13]），对 AI 模型、训练数据集和软件更新包进行加密签名，以验证其来源和完整性，从而抵御数据投毒和模型篡改攻击。

认知保护（使用中数据）：引入全同态加密（FHE）等先进的隐私保护计算技术，保护 AI 在进行推理和决策过程中数据的机密性。

这其中蕴含着一个深刻的战略契机。许多最先进的全同态加密（FHE）方案，其数学基础恰恰与 NIST PQC 标准（如 Kyber[12]和 Dilithium[13]）的核心——基于格的密码学——完全一致。这意味着，组织机构在为应对未来量子威胁而被迫进行的 PQC 迁移投资，实际上并非纯粹的防御性成本。这些为 PQC 迁移而建立的技术能力，包括对格密码的深刻理解、专门的硬件加速能力（如加速格运算的协处理器）以及优化的软件库，都可以被直接复用于部署下一代的隐私保护 AI 应用。因此，PQC 迁移从一个被动的、由合规驱动的成本中心，转变为一项主动的、为企业在未来 AI 竞赛中获得竞争优势的战略性赋能投资。这为加速 PQC 迁移提供了强有力的商业理由。

下表总结了 AI 智能体面临的主要威胁及相应的密码学缓解措施。

威胁向量	威胁描述	主要密码学缓解技术	技术工作原理
通信窃听（HNDL）	攻击者拦截智能体的加密通信，等待未来用量子计算机解密。	PQC 增强的 TLS 1.3（使用 ML-KEM 等）	使用抗量子攻击的算法协商会话密钥，使截获的密文在未来也无法被破解。
模型/软件篡改	攻击者在分发过程中篡改智能体的软件或模型更新包。	PQC 数字签名（使用 ML-DSA 等）	所有更新包都附有开发者的 PQC 签名，智能体在安装前验证签名以确保其真实性和完整性。

数据/模型投毒	攻击者通过污染训练数据或学习反馈来破坏智能体的长期决策能力。	PQC 数字签名 + TEE	对可信数据源进行 PQC 签名；在可信执行环境（TEE）内进行模型训练/微调，确保训练过程的完整性不被外部干扰。
用户数据隐私泄露（使用中）	服务提供商或攻击者在智能体处理用户查询时，获取用户的敏感输入数据。	全同态加密（FHE）	用户提交加密查询，智能体在加密数据上直接计算并返回加密结果，全程无需解密，实现零知识处理。

表 5-1 ： AI 智能体威胁与 PQC/PPC 缓解矩阵

5.2.2 量子抵抗认证的兴起：抗量子防伪产业

PQC 正从一项纯粹的防御性技术，演变为催生新商业模式的赋能技术。通过将 PQC 数字签名技术应用于实体商品，可以创造出一种能够抵抗未来任何已知计算攻击的、永久性的真伪证明。朗空量子在高价值收藏品、艺术品和快速消费品等领域的早期市场验证案例，清晰地揭示了这一新兴产业的轮廓。其核心价值在于，一个 PQC 签名所提供的认证，其安全性根植于数学难题，为物理商品和数字资产的“身份”创造了一个全新的、永恒的信任标准。这标志着 PQC 已开始从风险缓解工具，转变为价值创造和市场开拓的引擎。

行业领域	主要挑战（数据 vs. 设备寿命）	关键迁移策略	相关联盟伙伴专长
金融服务	数据寿命极长（数十年），交易系统对性能要求极高	硬件加速（HSM/密码卡）；在高仿真环境中进行全业务验证	苏州国芯（硬件）
能源/电网	设备寿命极长（>20 年），运营技术（OT）系统难以升级	“封装”保护（PQC 安全网关）；工业级芯片与模块；专业实验室仿真	工业级芯片合作伙伴（试验场）、专业系统集成商（系统集成）

工业物联网	海量资源受限设备，固件更新（OTA）困难	轻量级算法与硬件；以 PQC 签名保护 OTA 更新过程	苏州国芯（芯片）、朗空量子（软件框架）
智能网联汽车	车辆生命周期长（>15 年），安全直接关乎生命	在整车电子电气架构（EEA）初始设计阶段深度集成 PQC	苏州国芯（车规级芯片/密码卡）
卫星通信	空间环境严苛，资源高度受限，发射后无法升级硬件	轻量化、抗辐射实现；在轨/高仿真环境验证	上海巡天千河（试验场/ODM）
人工智能	AI 模型与训练数据价值高，是 HNDL 攻击的天然目标	PQC 与 FHE 协同部署，保护通信、数据与计算全过程	朗空量子（AI 大模型安全应用）

*理由：该矩阵将第五章的详细论述提炼为一目了然的速查表，便于读者快速比较不同行业的战略要点，并直观了解联盟成员如何匹配这些需求。

表 5-2 ： 关键行业 PQC 迁移驱动因素与策略矩阵

第六章

全球抗量子密码迁移挑战综合概述

第六章 全球抗量子密码迁移挑战综合概述

全球向抗量子密码（PQC）的迁移是一项前所未有的系统性工程，其挑战横跨技术、政策、经济和组织等多个维度。以下是对这些核心挑战的综合概述。

6.1 技术层面挑战：穿越工程与性能的雷区

性能开销与算法选择：NIST 标准化的 PQC 算法（如 ML-KEM[12], ML-DSA[13]）在带来量子安全性的同时，也引入了显著的性能开销，主要体现在远大于传统算法的密钥和签名尺寸，以及更高的计算复杂度。这给带宽和存储受限的环境（如物联网）以及高吞吐量系统（如金融交易）带来了巨大压力，往往需要专门的硬件加速来弥补性能损失。

密码敏捷性的实现难度：在未来威胁不确定的情况下，系统必须具备灵活切换加密算法的“密码敏捷性”。然而，改造现有硬编码了算法的庞大应用群、在协议层设计防降级攻击的协商机制，以及管理多样化的算法（如 NIST 为格密码选择的基于编码的备份方案 HQC）在工程上都极为困难。

遗留系统与公钥基础设施（PKI）改造：迁移的最大技术障碍之一是处理深植于企业运营中的遗留系统和“影子密码”。对于这些无法直接改造的系统，只能通过部署 PQC 安全网关进行“封装”保护。同时，PQC 巨大的密钥尺寸要求对全球 PKI 的核心——X.509 证书标准进行根本性改造，推广如“混合 X.509 证书”等方案，但这需要对证书颁发、验证的全链条进行升级，工程浩大。

演进中的“双重威胁”：组织不仅要防御未来 Shor 算法[7]对数学基础的攻击，还必须应对当前利用 AI 工具攻击 PQC 工程实现的“经典威胁”。这一挑战的严峻性，被近期由本联盟核心成员西交利物浦大学 PQC-X 实验室的丁津泰教授团队成功破解 200 维 SVP[35]挑战的事件所凸显。该事件有力地证明，即便我们迁移到了被认为是“抗量子”的下一代密码，针对其数学基础的经典攻击能力仍在不断进化。这与对 NIST 部分候选方案弱点的揭示一起，共同警示我们，PQC 迁移绝非“一劳永逸”，而是一个需要持续警惕和迭代的动态过程。除了数学基础的挑战，针对工程实现的攻击也已成为现实威胁。例如，2023 年底披露的“KyberSlash”侧信道漏洞，利用了 Kyber（即 ML-KEM 标准）实现过程中除法运算的时序差异，允许攻击者恢复私钥[34]。这一案例有力地警示我们，算法理论的安全并不等同于工程实现的安全，高保真的验证环境和抗侧信道设计在迁移中至关重要。

6.2 政策与治理层面挑战：驾驭分歧与内部惯性

全球标准差异与双重合规的高标准要求：全球 PQC 政策正呈现“大分流”态势。以美国为首的 NIST 标准阵营和中国追求技术主权的独立标准路线并存。这种差异对跨国企业提出了更高等级的安全保障要求，可能迫使其为不同市场维护不兼容的产品线，增加了研发成本和供应链复杂性，甚至有造成全球互联网技术基础碎片化的风险。

冲突的全球时间表：美国、欧盟、英国等主要经济体虽大方向一致，但在迁移里程碑（如 2030 年、2035 年）和强制性要求上存在差异。这迫使全球企业必须以“最严苛要求”为准来规划，进行复杂的全球风险评估和资源优先级排序，以应对最紧迫的合规压力。

内部治理的艰巨性：在组织内部，PQC 迁移面临两大治理难题。首先是进行全面的“加密资产发现”，这项工作因“影子密码”遍布、系统异构和缺乏自动化工具而极其困难。其次是建立常态化的治理结构，将 PQC 迁移从一次性项目转变为永久性的风险管理职能，这需要克服高层重视度衰减、跨部门协作困难和组织惯性等管理挑战。

6.3 生态与经济层面挑战：弥合成本与人才的鸿沟

高昂的成本与“量子安全债务”：PQC 迁移的总拥有成本（TCO）极其高昂，美国联邦政府的预估就超过 70 亿美元。然而，不行动的代价是积累一笔由“先窃取，后破解”（HNDL）攻击风险构成的“量子安全债务”，其潜在损失可能远超迁移成本。如何向决策层清晰论证这笔战略投资的必要性，是一大挑战。

关键的人才瓶颈：全球 PQC 迁移面临的最根本制约是人才的极度稀缺。合格的 PQC 专家需要具备密码学理论、软件工程、系统架构和风险管理等罕见的复合能力。人才短缺不仅推高了项目成本，更可能导致迁移的实际步伐落后于政策时间表，甚至催生为了合规而进行的、有缺陷的仓促实施，反而引入新风险。

发展中的生态系统：支撑大规模迁移的 PQC 生态系统在多方面仍显不成熟。市场上缺乏成熟的自动化发现和改造工具，解决方案呈现碎片化，具备深厚迁移经验的专业服务商仍然是少数。这需要像本白皮书发布联盟那样的战略共同体，整合产学研用能力，提供集成化解决方案。

6.4 特定行业层面挑战：因地制宜的战场

PQC 迁移策略必须根据不同行业的现实进行“调校”，每个行业都面临其独特的挑战组合：

金融服务：面临数据需长期保密与交易系统需极低延迟、高吞吐量的双重压力。

能源与关键基础设施：最大难题是保护生命周期长达数十年且无法直接更新的工业控制（OT）系统。

物联网（IoT）：面临设备资源（计算、内存、功耗）极端受限和大规模固件更新困难的挑战。

智能网联汽车：安全直接关系生命，且车辆生命周期长，要求将 PQC 深度集成到整车电子电气架构的初始设计中。

第七章

战略结论：构建有韧性的迁移引擎

第七章 战略结论：构建有韧性的迁移引擎

7.1 对企业领袖（CISO,CIO,CEO）的建议

7.1.1 承认紧迫性，提升战略定位：将风险转化为机遇

作为企业领袖，必须将 PQC 迁移视为一项关乎企业生存和竞争力的当前战略风险，而不是一个可以推迟的遥远 IT 升级项目。这一风险的紧迫性源于“先窃取，后破解”（Harvest Now, Decrypt Later, HNDL）攻击模型，即对手方正在大规模拦截和存储当今加密的数据，等待未来量子计算机问世后再行破解。这意味着，对于任何需要长期保密的数据——例如企业核心知识产权、长期金融合同、个人健康档案——其安全漏洞实际上已经存在。

因此，推迟 PQC 迁移并非零成本决策，它实际上是在不断积累一种无形的、但极其危险的“量子安全债务”。这笔债务的潜在“偿还”成本可能是灾难性的，包括知识产权的永久性损失、因违反《网络与信息系统安全指令第二版》（NIS2）等法规而导致的巨额罚款，以及对品牌声誉和客户信任的毁灭性打击。历史的教训（如 Crypto AG[3–5]事件）告诉我们，一旦对手掌握了破解主流密码的“万能钥匙”，他们绝不会公之于众，而是会将其作为最高机密武器秘密使用。必须在对手的秘密武器形成战斗力之前，完成防御升级。

首要职责，为组织的‘量子安全迁移战略引擎’完成点火启动。率先完成迁移的企业，能够将其作为一项强大的竞争优势，在赢得高端合同和客户忠诚度方面占得先机，并在日益严格的供应链准入中获得优先权。

7.1.2 立即启动“无悔之举”：以情报驱动决策

任何成功的迁移都始于清晰的认知。因此，应立即授权并投入资源，启动一次全面的企业级加密资产盘点和量子风险评估。这项工作被广泛认为是“无悔之举”（No-Regret Move），因为它无论量子威胁何时到来，都能极大提升组织的安全可见性和管理能力，是提升整体“密码学成熟度”的契机。

这项工作的目标远不止是制作一份静态的资产清单，而是要构建一个动态的、数据驱动的加密情报视图：

绘制加密地图：以数据流向为主线，追踪敏感数据在系统中的完整生命周期，了解加密在何处、如何以及为何被使用。

评估风险敞口：根据数据的保密寿命对其进行分类。需要保存数十年的长期合同，与仅需短期保密的会话数据，其面临的 HNDL 风险等级截然不同。这种分类方法能够直接为迁移工作的优先级排序提供决策依据。

可视化系统性风险：通过绘制风险传染图谱，理解单个系统的漏洞可能如何通过数据交互扩散至整个企业生态，从而识别出那些处于风险传导路径关键节点上的系统。

这项任务之所以艰巨，是因为“影子密码”无处不在，系统高度复杂异构，且企业普遍缺乏自动化的盘点工具和标准化的流程。然而，这项工作为启动迁移引擎、获得初始点火能量提供了先决条件，并将抽象风险转化为具体、可量化的行动。更重要的是，它为获取高层支持提供了强有力的依据。欧盟发布的 PQC 迁移路线图[24]已明确指出，像加密资产管理这样的“无悔之举”，是遵守 NIS2 等法规的组成部分，而相关实体的管理层可能因未能采取“最先进”的安全措施而被追究责任[5]。这使得启动 PQC 迁移的初始步骤，从一个应对未来威胁的前瞻性项目，转变为一项满足当前法律合规要求的必要行动，为 CISO 和 CIO 向董事会申请资源提供了坚实的法律基础。

7.1.3 投资于敏捷性，而非特定算法：构建面向未来的架构

将密码敏捷性[23]确立为所有新技术架构和采购决策的核心原则。根据 NIST 的权威定义，密码敏捷性是指“在不中断运行系统流程的情况下，为实现韧性而替换和调整……密码算法所需的能力”。未来的密码学标准和威胁环境仍有变数，只有能够灵活切换加密算法的架构，才能在未来保持韧性。投资于敏捷性至关重要，原因如下：

应对标准演进：NIST 的标准化进程远未结束。其启动第四轮附加流程，以及选择基于编码的 HQC 作为格密码的备份方案，都表明了对“算法多样性[15]”的制度化坚持。架构必须能够适应未来可能出现的新标准，而非被锁定在单一技术路线上。

抵御迭代性威胁：我们面临的是一个“双重威胁”环境。即便是作为未来防御核心的 PQC 算法本身，也正成为不断演进的经典攻击方法的目标，近期对 200 维 SVP[35]挑战的成功破解便是明证。一个敏捷的架构使您能够在发现新漏洞时快速响应，通过切换算法来修复安全防线，而不是进行伤筋动骨的系统重构。

驾驭全球分歧：随着中国等国家建立独立的 PQC 标准体系，全球标准正呈现“大分流”态势。对于跨国企业而言，一个能够支持并灵活协商不同密码套件的敏捷架构，是在不同监管环境中保持合规和互操作性的唯一现实途径。

密码敏捷性[23]是整个迁移引擎的“底座”，它确保了引擎能够平稳、持续地运转，以适应任何外部环境的变化。在实践中，这意味着推动技术团队采用抽象的加密 API、支持混合 X.509 证书的 PKI，以及能够在协议层安全协商算法的现代通信协议。

7.2 对政策制定者与监管机构的建议

抗量子迁移是一项关乎国家安全、经济稳定和技术主权的系统性工程。政策制定者与监管机构的角色，是为所有组织的“迁移引擎”扫清障碍，并提供强大的外部“顺风”，确保国家整体能够平稳、安全地度过此次密码学代际更迭。为此，我们提出以下四点核心建议：

7.2.1 细化实施路径，强化战略执行力

鉴于我国已明确了抗量子密码的战略方向与标准制定路线图，当前的重心应从“战略规划”转向“战术执行”。PQC 迁移面临的最大挑战之一是组织内部的惯性，因此，政策制定的重点应在于将顶层设计转化为具体的落地抓手，确保国家战略能够穿透至各行业。

发布分行业的实施细则与强制时间表： 在国家既定战略框架下，应进一步为金融、能源、交通等关键基础设施领域设定不容协商的硬性迁移期限（例如，在 2030 年前完成高风险系统迁移）。通过将宏观目标分解为可考核的阶段性任务，为整个社会提供一个可预期的、稳定的政策执行环境。

利用政府与国企采购作为市场杠杆： 借鉴美国国家安全局（NSA）CNSA 2.0 策略的成功经验，将符合 PQC 标准作为政府和关键行业采购的强制性要求。这将产生强大的市场涟漪效应，激励技术供应商在其商

业产品中优先集成 PQC 能力，从而极大加速 PQC 技术在私营部门的普及和应用。

提供财政激励，培育数字经济新增长点： 应将 PQC 迁移视为数字经济基础设施升级的关键一环。建议设立专项基金或税收优惠政策，不仅为了降低中小企业的合规成本，更旨在通过迁移需求拉动高端密码产业、网络安全服务业的发展，将其打造为数据要素流通的安全底座，从而不仅解决安全问题，更创造经济增量。

7.2.2 推动标准协调，减少全球合规摩擦

在全球化的数字经济中，标准的碎片化将带来巨大的经济成本和安全风险。政策制定者的关键职责是充当桥梁，最大限度地减少技术壁垒。

积极参与并促进国际标准对话：面对以美国 NIST 为代表的标准体系与中国追求独立自主标准体系并存的“大分流”趋势，应通过外交和技术交流渠道，积极推动 NIST、欧盟网络与信息安全局（ENISA）、中国密码行业标准化技术委员会（CSTC）等主要标准制定组织之间的沟通。探索建立标准互认或跨标准互操作性测试框架，以降低跨国企业的合规成本和供应链复杂性。

鼓励并投资于“密码敏捷性”架构：鉴于未来标准和威胁环境的不确定性，应将“密码敏捷性”确立为国家网络安全架构的核心原则。资助能够支持异构密码环境的技术研发，例如能够同时处理不同国家 PQC 标准的安全网关和协议，确保在标准分歧的背景下，本国系统依然能够保持广泛的互操作性。

7.2.3 持续资助研发生态，弥合技术与人才鸿沟

PQC 迁移是一场长期的技术演进，需要持续的创新和知识储备来维持“迁移引擎”的动力。

精准资助下一代基础研究：资金支持不应止步于当前已标准化的算法。应持续投入，支持对现有 PQC 标准（特别是作为主流的格密码）的持续安全分析，以应对如 SVP 挑战被破解等不断演进的“经典威胁”。同时，应重点资助具备不同数学基础的备份算法（如基于编码、同源的密码），确保“算法多样性”，为未来可能出现的“黑天鹅”事件做好储备。

大力支持迁移工具与平台开发：PQC 迁移的复杂性急需成熟的工具来简化。应设立专项资金，鼓励学术界和产业界合作开发能够自动化进行“加密资产发现”、提供“高保真验证”和实现“灰度演进” 的开源及商业化工具集，降低整个社会的迁移成本和实施风险。

大力支持 PQC 迁移验证体系建设： 建立健全的 PQC 迁移验证与评估机制是确保迁移安全性的关键。应授权并支持第三方检测机构和行业实验室，依据国家标准制定科学的迁移验证规范。重点针对 PQC 产品的合规性、迁移方案的有效性以及系统的兼容性开展权威评测，为各行业的迁移工作提供可信的质量认证与风险兜底。

建立国家级人才培养体系：认识到 PQC 专业人才的极度稀缺是迁移最根本的制约因素，应将人才培养提升至战略高度。通过支持高校设立专门课程、建立如 PQC-X 实验室产学研联合培养基地，并为参与 PQC 培训的企业和个人提供补贴，系统性地构建能够满足未来十年需求的跨学科人才梯队。

7.2.4 支持公私合作伙伴关系（PPP），加速实践落地

PQC 迁移的规模和复杂性远超任何单一实体所能应对，需要构建一个紧密的国家级合作网络。

推广国家网络安全卓越中心（NCCoE）模式：NIST 的 NCCoE 项目是公私合作的典范，它成功地联合了技术巨头、关键行业用户和政府机构，共同开发了具体、可操作的迁移指南和实践方案。应在本国复制并推广这一模式，针对金融、能源、医疗等关键行业建立专门的 PQC 迁移创新中心，将标准转化为符合行业需求的解决方案。

资助行业性试点项目与验证平台：政府应带头投资，联合行业龙头企业，共同构建行业级的“迁移试验平台”。通过在真实或高仿真环境中验证 PQC 方案的性能和业务兼容性（如江苏银行在金融场景的实践），积累宝贵的实践数据，形成行业最佳实践，并向全行业分享，从而加速整个行业的迁移进程。

7.3 对技术社区的建议

技术社区是实现全球抗量子密码（PQC）迁移的最终执行者，是为整个“迁移引擎”打造和维护高效、可靠组件的核心力量。面对这场深

刻的技术变革，技术社区的行动将直接决定迁移的成败、速度与安全水平。为此，我们提出以下三点核心建议：

7.3.1 协作与贡献：共建开放、稳健的 PQC 生态系统

PQC 迁移的复杂性远非任何单一组织所能应对，一个开放、协作、经过实战检验的生态系统是成功的基石。

深度参与标准化进程：积极参与 NIST、IETF、中国 CSTC 等国际和国家标准组织的工作。这不仅指提交新的算法方案，更意味着投入到对候选算法严苛、公开的密码分析中，成为“在部署前发现弱者”的关键力量。同时，为 TLS、IPsec、X.509 等关键协议的 PQC 适配贡献力量，解决 PQC 算法带来的密钥/签名尺寸增大、需要支持混合模式等实际工程问题。

强化开源社区贡献：积极参与由 Linux 基金会于 2024 年 2 月成立的后量子密码联盟（PQCA）。PQCA 整合了包括 AWS、Google、IBM 等科技巨头资源，并正式接管了 Open Quantum Safe (OQS) 等核心开源项目的治理。这标志着 PQC 开源生态已从松散的社区驱动转变为工业级联合治理。建议重点关注 OQS 项目，为其贡献代码、安全审查和最佳实践。

高性能实现：开发并优化针对不同平台（如 x86、ARM）和指令集（如 AVX2、NEON）的算法实现，特别关注抵抗侧信道攻击的能力。

语言与框架集成：创建流行编程语言（如 Go, Rust, Python, Java）的 PQC 库封装，并将其集成到主流的加密框架（如 OpenSSL）和应用中，降低开发者的使用门槛。

建立密码分析文化：持续对已标准化的 PQC 算法进行公开的学术攻击和安全审计，建立负责任的漏洞披露机制，推动算法的持续改进和安全演进。近期对 200 维 SVP[35]挑战的成功破解即是社区贡献价值的明证。

7.3.2 负责任地创新：简化安全，抵御“双重威胁”

技术社区的核心职责是让安全地使用 PQC 变得简单，让“默认安全”成为新常态，以应对“双重威胁”的挑战。

构建“防误用”的 API 与库：鉴于 PQC 迁移中最普遍的风险源于不安全的工程实现（如硬编码密钥、不安全的 API 使用），技术社区应致

力于开发高层级的、对开发者友好的加密库。这些库应封装复杂的底层操作，提供简洁、安全的 API，让开发者难以犯错。

开发自动化的安全工具：为应对 AI 驱动的密码分析工具对工程实现的自动化攻击，社区应开发相应的开源防御工具。这包括：

加密资产发现工具：开发能够自动化扫描代码库、二进制文件和网络流量的工具，帮助组织建立其“加密物料清单”（CBOM），发现“影子密码”。

实现层漏洞扫描器：构建能够静态或动态分析代码的工具，专门用于查找 PQC 实现中的常见漏洞。

打造模块化的迁移与验证框架：创建开源的迁移验证平台和工具集，支持 A/B 测试、金丝雀发布和风险回退等“灰度演进”策略，帮助组织在将 PQC 投入生产前，进行高保真的功能、性能和安全验证。

7.4 聚焦前瞻性应用：拓展 PQC 的价值新疆域

PQC 不仅是防御性技术，更是赋能下一代技术创新的引擎。技术社区应超越传统加密场景，探索 PQC 的增值应用。

赋能人工智能与自主系统安全：人工智能系统是“先窃取，后破解”攻击的天然目标。技术社区应开发专用框架，将 PQC 深度集成到 AI 的各个层面，包括：

使用 PQC 保护 AI 智能体之间、及其与用户间的通信安全。

使用 PQC 数字签名保护 AI 模型、训练数据和软件更新的完整性，抵御数据投毒和模型篡改。

探索格密码在 PQC 和全同态加密（FHE）之间的深刻数学协同性，为构建下一代隐私保护 AI 奠定基础。

催生新的商业模式与产业：将 PQC 技术应用于解决物理世界的信任问题。例如，利用 PQC 数字签名的长期安全性，为高价值商品、艺术品、法律文件等提供可抵抗未来任何计算攻击的防伪认证，催生“抗量子防伪”这一新兴产业。

为新兴数字生态提供安全基石：为 Web3.0、区块链、工业互联网（IIoT）和智能网联汽车（ICV）等新兴领域提供深度定制的 PQC 解决方案。例如，为资源受限的物联网设备开发轻量级 PQC 固件更新机制，或为区块链设计抗量子的数字签名方案。

7.5 您的最初 90 天：PQC 迁移快速入门指南

对于已被本白皮书说服、希望立即采取行动的领导者而言，最直接的问题是：“我下周一该做什么？” 本指南将“战略远见与风险情报”一章的核心思想，提炼为一个目标明确、分阶段的即时行动清单。这 90 天的核心目标，是为组织的“迁移引擎”施加一股强大而精准的点火能量。

第一阶段第 1-30 天—建立领导核心、统一战略认知

此阶段的目标是奠定组织基础，将 PQC 迁移从一个技术问题提升为一项全员共识的战略要务。

第 1 周：组建跨职能 PQC 专项小组

指定负责人：任命一位高级管理人员（如 CISO、CIO 或 CTO）作为项目发起人，赋予其决策权和资源调动能力。

建立核心团队：团队成员必须跨越部门墙，包括来自信息技术、网络安全、应用开发、法律、合规、风险管理和关键业务部门的代表。这确保了迁移决策能从一开始就兼顾技术可行性、合规要求和业务影响。

第 2-4 周：举行战略启动会议，形成高层共识

阐明紧迫性：向专项小组及企业核心决策层（包括 CEO、CFO）清晰传达量子威胁的性质。重点讲解“先窃取，后破解”（HNDL）攻击模型，强调对于需要长期保密的数据，安全风险已经存在，推迟行动是在积累“量子安全债务”。

确立战略视角：将 PQC 迁移定位为一次提升组织整体“密码学成熟度”（Cryptographic Maturity）的战略契机，而非一次简单的技术升级。强调这是一项关乎企业未来生存和竞争力的业务连续性要务，是必须立即采取的“无悔之举”（No-Regret Moves）。

第二阶段第 31-60 天—启动资产发现、完成初步评估

此阶段的目标是“摸清家底”，从模糊的风险感知转向数据驱动的、可量化的风险认知。

第 5-7 周：启动加密资产发现

执行扫描：利用自动化工具或聘请专业服务机构，对网络、应用程序、数据库和代码库进行全面扫描。目标是建立一份初步的“加密物料

清单”（Cryptography Bill of Materials, CBOM），了解组织内加密算法、协议、密钥和证书的使用情况。

识别“影子密码”：特别关注那些深植于遗留系统或由第三方组件引入的、未被文档记录的加密实现。

第 8-9 周：识别高价值数据资产并进行分类

绘制数据地图：与业务部门合作，以数据流向为主线，识别并列出具有最长保密寿命和最高业务价值的数据资产。这包括核心知识产权、长期客户合同、个人生物基因档案、金融交易记录等。

按寿命排序：根据数据的预期保密寿命对其进行分类。这是后续风险排序和确定 HNDL 威胁优先级的关键依据。

第三阶段第 61-90 天—量化核心风险、确定试点并规划路线图

此阶段的目标是将宏观风险转化为具体的行动计划，为启动引擎的下一阶段做好准备。

第 10-11 周：举办风险评估与可视化研讨会

量化风险：结合加密资产清单和高价值数据清单，基于公式“风险 = 数据保密寿命 > 量子威胁出现时间”对不同系统进行风险排序。

构建风险矩阵：通过构建风险矩阵（Risk Matrix），结合风险发生的概率和造成的影响两个维度，对不同风险进行评级。

绘制风险传染图谱：分析风险的传导机制，绘制“风险传染图谱”（Risk Contagion Map），识别那些处于关键节点、一旦被攻破可能引发连锁反应的系统。

第 12-13 周：确定试点项目并制定初步路线图

选择试点：基于风险评估结果，确定 3-5 个最关键的系统作为第一批迁移试点。理想的试点项目应具备：风险最高、数据保密寿命最长、同时技术上相对可行（例如，非高度耦合的遗留系统）、且成功后能产生显著示范效应的特点。

制定路线图：为试点项目制定一份高阶迁移路线图。内容应包括：

明确的目标和范围。

初步的时间表和关键里程碑。

对所需资源（人力、预算、外部专家）的初步估算。

向 PQC 专项小组和决策层汇报，以获得正式批准和预算支持，为引擎的下一阶段“构建动能：抗量子密码技术堆栈”做好准备。

核心术语表

英文缩写	英文全称	中文全称	解释/白皮书语境
AKE	Authenticated Key Exchange	认证密钥交换	允许通信双方验证身份并协商密钥的协议。文中强调需部署“异构 AKE”以解决 PQC 迁移期的兼容性问题。
ANSSI	National Cybersecurity Agency of France	法国国家网络安全局	法国网络安全主管部门，发布了 PQC 迁移立场文件，建议采用混合模式过渡。
BSI	Federal Office for Information Security (Germany)	德国联邦信息安全办公室	德国信息安全主管机构，发布了 TR-02102-1 指南，推荐 FrodoKEM 等算法作为冗余备份。
CA	Certificate Authority	证书颁发机构	负责签发数字证书的权威机构。PQC 迁移要求 CA 升级以支持混合 X.509 证书。
CAGR	Compound Annual Growth Rate	复合年均增长率	用于描述 PQC 市场规模的增长速度。文中预测到 2034 年 PQC 市场 CAGR 将达

			37%-47%。
CBOM	Cryptography Bill of Materials	密码物料清单	记录系统中所有加密资产（算法、密钥、库）的清单。美国和欧盟已将其列为供应链合规的红线要求。
CDN	Content Delivery Network	内容分发网络	如 Cloudflare 等服务商。IETF 的新标准扫清了 CDN 进行大规模 PQC 切换的协议障碍。
CISA	Cybersecurity and Infrastructure Security Agency	美国网络安全与基础设施安全局	美国负责关键基础设施安全的机构，与 NSA 联合发布警告并推动 CBOM 合规。
CISO	Chief Information Security Officer	首席信息安全官	企业安全负责人。文中建议 CISO 应牵头组建 PQC 专项小组并向董事会汇报风险。
CNSA	Commercial National Security Algorithm Suite	商业国家安全算法套件	NSA 发布的算法套件（2.0 版），强制要求国家安全系统在 2030-2035 年间完成 PQC 迁移。
CRA	Cyber Resilience Act	《网络弹性法	欧盟法规。要求相关实体采

		案》	取“最先进”安全措施，未能实施 PQC 迁移可能被视为违规。
CRQC	Cryptographically Relevant Quantum Computer	密码学相关量子计算机	指具备足够规模和纠错能力，能运行 Shor 算法破解 RSA/ECC 的实用化量子计算机。
CSF	Cybersecurity Framework	网络安全框架	NIST 发布的框架（CSF 2.0）。NCCoE 将 PQC 迁移映射到该框架的治理、识别、保护等核心功能中。
CSTC	Cryptography Standardization Technical Committee	密码行业标准化技术委员会	中国密码标准制定机构，联合 ICCS 发起了全球 PQC 算法征集，推动中国自主 PQC 标准体系建设。
Crypto-Agility	Cryptographic Agility	密码敏捷性	核心战略原则。指系统在不中断业务的情况下，灵活切换密码算法的能力，是应对未来不确定性的底座。
DAO	Decentralized Autonomous	去中心化自治组	Web3.0 中的组织形式。文中

	Organization	织	提到 DAO 社区正规划部署抗量子防护措施。
ECC	Elliptic Curve Cryptography	椭圆曲线密码	当前广泛使用的公钥密码体系。因依赖离散对数问题，面临 Shor 算法的直接破解威胁。
EEA	Electronic Electrical Architecture	电子电气架构	汽车的电子系统架构。因车辆寿命长，需在 EEA 设计阶段深度集成 PQC 能力。
ETSI	European Telecommunications Standards Institute	欧洲电信标准化协会	国际标准组织。文中引用了其 2024 年新加坡年会关于量子比特需求的研判数据。
FHE	Fully Homomorphic Encryption	全同态加密	允许对密文进行计算的技术。其数学基础（格密码）与 NIST PQC 标准一致，具有战略协同效应。
HNDL	Harvest Now, Decrypt Later	“先窃取，后破解”	核心威胁模型。指攻击者现在窃取加密数据，等待未来量子计算机解密。这使得长期数据的风险已成现实。

HQC	Hamming Quasi-Cyclic	汉明准循环	一种基于编码理论的 KEM 算法。被 NIST 选为格密码的备份标准，以提供算法多样性[15]。
HSM	Hardware Security Module	硬件安全模块	用于密钥管理和加密运算的物理设备。金融等高性能场景需部署抗量子 HSM。
IBC	Identity-Based Cryptography	基于标识的密码	使用身份（如邮箱）作为公钥的密码体系（如 SM9）。文中探讨了其向 PQC-IBE 演进的路径。
ICCS	Institute of Commercial Cryptography Standardization	商用密码标准研究院	中国机构，发布了关于新一代商用密码（PQC）候选算法的公告和路线图。
ICS	Industrial Control Systems	工业控制系统	能源电网等领域的核心系统。因生命周期长且难以升级，是 PQC 迁移的难点。
ICV	Intelligent Connected Vehicles	智能网联汽车	需在 V2X 通信中集成 PQC 以保障长期安全的汽车系统。
IETF	Internet Engineering Task	互联网工程任务	负责互联网标准的组织。发

	Force	组	布了在 TLS 1.3 中支持混合密钥交换的 RFC 标准。
ISO/IEC	International Organization for Standardization	国际标准化组织	已推进修正案，将 Kyber 和 Dilithium 纳入 ISO/IEC 18033-2 等国际标准体系。
KEM	Key Encapsulation Mechanism	密钥封装机制	用于协商共享密钥的机制。ML-KEM（Kyber）是 NIST 选定的通用 KEM 标准[12]。
LWE	Learning With Errors	容错学习问题	格密码学的核心数学难题，是中国构建下一代抗量子标识密码的重要研究方向。
ML-DSA	Module-Lattice-Based Digital Signature Standard	基于模格的数字签名标准	NIST 发布的通用 PQC 数字签名标准（FIPS 204），即 Dilithium。
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism	基于模格的密钥封装机制	NIST 发布的通用 PQC 加密标准（FIPS 203），即 Kyber。[12]
NCCoE	National Cybersecurity Center of Excellence	国家网络安全卓越中心	NIST 下属机构，通过与产业界合作（如迁移项目），将 PQC 标准转化为实践指南。

NCSC	National Cyber Security Centre	英国国家网络安全中心	英国安全机构，发布了详细的 PQC 迁移三阶段路线图（2028-2035）。
NIS2	Network and Information Security Directive (2)	《网络与信息系统安全指令第二版》	欧盟指令。强制关键基础设施采取高水平安全措施，驱动 PQC 合规需求。
NIST	National Institute of Standards and Technology	美国国家标准与技术研究院	全球 PQC 标准化的领跑者，通过多轮竞赛选定了首批 PQC 算法标准。
NSA	National Security Agency	美国国家安全局	发布 CNSA 2.0 算法套件，为国家安全系统设定了强制性的 PQC 迁移时间表。
OQS	Open Quantum Safe	开放量子安全项目	一个开源项目，提供 PQC 库（liboqs）。现已并入 Linux 基金会的 PQCA 联盟。
OTA	Over-The-Air	空中下载技术	远程固件更新技术。必须使用 PQC 签名保护 OTA 过程，防止恶意固件注入。
OT	Operational Technology	运营技术	用于监控和控制物理设备的硬件/软件（如电网控制）。

			通常难以更新，需“封装”保护。
PKC	Public-Key Cryptography	公钥密码学	现代数字信任的基石。因 Shor 算法的出现，传统的 PKC 体系正面临重构。
PKG	Key Generation Center	密钥生成中心	标识密码体系（SM9）中的核心组件，负责生成私钥，需进行抗量子升级。
PKI	Public Key Infrastructure	公钥基础设施	基于数字证书的信任体系。PQC 迁移要求 PKI 支持更大的密钥尺寸和混合证书。
PPC	Privacy-Preserving Computation	隐私保护计算	包括多方计算、同源加密等技术。文中提到 PQC 与 PPC 结合可保障 AI 全生命周期安全。
PQC	Post-Quantum Cryptography	后量子密码（国内官方文件及标准中常称为“抗量子密码”）	指能够运行在现有经典计算机上，利用数学难题构建的，足以抵御未来大规模量子计算机攻击的新一代公钥密码算法体系。它是本白皮书探

			讨的核心技术路径。
PQCA	Post-Quantum Cryptography Alliance	后量子密码联盟	由 Linux 基金会牵头，AWS、IBM 等参与的联盟，致力于提供生产就绪的开源 PQC 软件。
QaaS	Quantum Computing as a Service	量子计算即服务	通过云平台提供量子算力。这使得攻击者更易获取量子能力，增加了安全威胁。
QFT	Quantum Fourier Transform	量子傅里叶变换	Shor 算法的核心步骤，能高效寻找函数周期，从而破解 RSA 等数学难题。
QKD	Quantum Key Distribution	量子密钥分发	基于物理原理的密钥分发技术。文中指出其难以解决认证问题，需与 PQC 互补。
RFC	Request for Comments	请求意见稿	IETF 发布的互联网标准文档。RFC 9xxx 确立了 TLS 1.3 中的混合密钥交换标准。
ROI	Return on Investment	投资回报率	投资收益比。文中强调 PQC 迁移是清偿“量子安全债务”并获得竞争优势的高 ROI 投

			资。
RSA	Rivest-Shamir-Adleman	RSA 加密算法	最主流的公钥加密算法之一。因基于大整数分解难题，将被量子计算机破解。
SBOM	Software Bill of Materials	软件物料清单	软件供应链清单。PQC 合规要求在 SBOM 基础上补充密码信息。
SDK	Software Development Kit	软件开发工具包	文中提到需开发针对移动端优化的轻量级 PQC SDK。
SLH-DSA	Stateless Hash-Based Digital Signature Standard	无状态基于哈希的数字签名标准	NIST 标准（SPHINCS+）。安全性极高但性能较低，适用于代码签名等场景。
SVP	Shortest Vector Problem	最短向量问题	格密码的安全基石。西浦 PQC-X 实验室成功挑战了高维 SVP，提示了持续的经典威胁。
TCO	Total Cost of Ownership	总拥有成本	PQC 迁移的全部成本。文中指出其实际成本可能高达数百亿美元。
TEE	Trusted Execution	可信执行环境	硬件隔离的安全区域。用于

	Environment		保护 AI 模型训练过程免受投毒攻击。
TLS	Transport Layer Security	传输层安全协议	保护 Web 流量的协议。PQC 迁移的核心场景之一是升级 TLS 握手以支持抗量子算法。
UOV	Unbalanced Oil and Vinegar	非平衡油醋算法	一种多变量数字签名方案。特点是验证极快，适合物联网等低算力终端。
V2X	Vehicle-to-Everything	车用无线通信技术	车辆与外界的交互技术。需在设计阶段植入 PQC 以抵御未来威胁。
Web3.0	Web 3.0	第三代互联网	基于区块链的去中心化网络。其数字身份和资产安全深度依赖 PQC 的升级。

参考文献

[1]Capgemini Research Institute, "Future Encrypted: Why Post-Quantum Cryptography Tops the New Cybersecurity Agenda," Capgemini, 2025. [Online]. Available: https://www.capgemini.com/insights/research-library/post-quantum-crypto/

[2] Thales Group, "2025 ThalesData Threat Report: AI, Quantum and the Evolving Data Threatscape," Thales CPL Research, 2025. [Online]. Available:https://cpl.thalesgroup.com/ppc/data-threat-report?utm_source=google&utm_medium=cpc&utm_source=google&utm_medium=cpc

[3] G. Miller, "The Intelligence Coup of the Century," The Washington Post, 2020. [Online]. Available: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

[4]P. Oltermann, "CIA controlled global encryption company for decades, says report," The Guardian, 2020.[Online].Available: https://www.theguardian.com/us-news/2020/feb/11/crypto-ag-cia-bnd-germany-intelligence-report

[5]National Security Archive, "The CIA's 'Minerva' Secret," The George Washington University, 2020. [Online]. Available: https://nsarchive.gwu.edu/briefing-book/chile-cyber-vault-intelligence-southern-cone/2020-02-11/cias-minerva-secret

[6]R. P. Feynman, "Simulating Physics with Computers," International Journal of Theoretical Physics, vol. 21, 1982. [Online]. Available: https://link.springer.com/article/10.1007/BF02650179

[7]P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proc. 35th Annu. Symp. Found. Comput. Sci., 1994. [Online]. Available: https://ieeexplore.ieee.org/document/365700

[8]M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" IEEE Security & Privacy, vol. 16, no. 5, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8490169

[9]E. Gouzien et al., "Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126,133 Cat Qubits," Physical Review Letters, vol. 131, 2023. [Online]. Available: https://arxiv.org/abs/2302.06639

[10]C. Gidney, "How to factor 2048 bit RSA integers with less than a million noisy qubits," arXiv preprint arXiv:2505.15917, 2025. [Online]. Available: https://arxiv.org/abs/2505.15917

[11]Alliance for Telecommunications Industry Solutions (ATIS), "Quantum Technologies and the Cryptographic Threat Timeline: A Strategic Overview," 2025. [Online]. Available: https://atis.org/resources/quantum-technologies-and-the-cryptographic-threat-timeline-a-strategic-overview/

[12]NIST, "Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203)," 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/203/final

[13]NIST, "Module-Lattice-Based Digital Signature Standard (FIPS 204)," 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/204/final

[14]NIST, "Stateless Hash-Based Digital Signature Standard (FIPS 205)," 2024. [Online]. Available: https://csrc.nist.gov/pubs/fips/205/final

[15]NIST, "NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption," NIST News Release, 2025. [Online]. Available: https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption

[16]F. Driscoll et al., "Terminology for Post-Quantum Traditional Hybrid Schemes (RFC 9794)," IETF, 2025. [Online]. Available: https://www.rfc-editor.org/info/rfc9794

[17]D. Stebila et al., "Hybrid key exchange in TLS 1.3 (draft-ietf-tls-hybrid-design)," IETF Internet-Draft, 2025. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/

[18]ISO/IEC, "ISO/IEC 11770-3:2021 Information security — Key management — Part 3: Mechanisms using asymmetric techniques," 2021. [Online].
Available: https://www.iso.org/standard/82709.html

[19]ISO/IEC, "ISO/IEC 14888-3:2018 Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms," 2018. [Online].
Available: https://www.iso.org/standard/76382.html

[20]The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10)," 2022. [Online].
Available: https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[21]National Security Agency (NSA), "Announcing the Commercial National Security Algorithm Suite 2.0," 2022. [Online].
Available: https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

[22]NIST, "Transition to Post-Quantum Cryptography Standards (NIST IR 8547 Draft)," 2024. [Online]. Available: https://csrc.nist.gov/pubs/ir/8547/ipd

[23]NIST, "Considerations for Achieving Crypto Agility: Strategies and Practices (CSWP 39)," 2025. [Online].
Available: https://www.nist.gov/news-events/news/2025/12/nist-publishes-cswp-39-considerations-achieving-crypto-agility

[24]European Commission, "A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography," 2025. [Online].
Available: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

[25]TNO, AIVD, & CWI, "The PQC Migration Handbook, Version 2," 2023. [Online].

Available: https://publications.tno.nl/publication/34641918/oicFLj/attema-2023-pqc.pdf

[26]National Cyber Security Centre (NCSC), "Timelines for migration to post-quantum cryptography," 2025. [Online].
Available: https://www.ncsc.gov.uk/guidance/pqc-migration-timelines

[27]Institute of Commercial Cryptography Standards (ICCS), "Announcement on Launching the Next-generation Commercial Cryptographic Algorithms Program (NGCC)," 2025. [Online].
Available: https://www.niccs.org.cn/en/

[28]State Cryptography Administration of China, "GM/T 0044-2016: SM9 Identity-based Cryptographic Algorithms," 2016. [Online]. Available: http://www.gmbz.org.cn/main/bzlb.html

[29]GSMA, "Post Quantum Cryptography Guidelines for Telecom Use Cases V2.0" 2024. [Online].
Available: https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/post-quantum-cryptography-guidelines-for-telecom-use-cases-pq-03-2/

[30] Signal Foundation, "PQXDH: The New Post-Quantum Agreement Protocol for Signal," 2023. [Online]. Available: https://signal.org/blog/pqxdh/

[31]Apple Security Engineering and Architecture, "iMessage with PQ3: The new state of the art in quantum-secure messaging," 2024. [Online].
Available: https://security.apple.com/blog/imessage-pq3/

[32] Google Chrome Team, "Advancing Our Amazing Bet on Asymmetric Cryptography," Chromium Blog, 2024. [Online].
Available: https://blog.chromium.org/2024/05/advancing-our-amazing-bet-on-asymmetric.html

[33]Zoom Video Communications, "Zoom bolsters security offering with the inclusion of post-quantum end-to-end encryption in Zoom Workplace," 2024. [Online].
Available: https://news.zoom.com/post-quantum-e2ee/

[34]D. J. Bernstein et al., "KyberSlash: Exploiting secret-dependent division timings in Kyber implementations," IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025. [Online]. Available: https://kyberslash.cr.yp.to/

[35] XJTLU PQC-X Lab, "XJTLU team sets code-breaking record for testing post-quantum online security," 2025. [Online]. Available: https://www.xjtlu.edu.cn/en/news/2025/03/xjtlu-team-sets-code-breaking-record-for-testing-post-quantum-online-security

[36]Linux Foundation, "Announcing the Post-Quantum Cryptography Alliance (PQCA)," 2024. [Online]. Available: https://pqca.org/