安全牛
AQNIU.NET

抗量子安全应用迁移与落地实践研究（2026版）

迁移窗口紧 标准与多元落地并行

版权声明

本报告为北京谷安天下科技有限公司（以下简称“本公司”）旗下媒体平台安全牛研究撰写，报告中所有文字、图片、表格均受有关商标和著作权的法律保护，部分文字和数据采集于公开信息，所有权为原著者所有。未经本公司书面许可，任何组织和个人不得将本报告内容作为诉讼、仲裁、传媒所引用之证明或依据，不得用于营利或用于未经允许的其他用途。任何未经授权的商业性使用本报告的行为均违反《中华人民共和国著作权法》及其他相关法律法规、国际条约。未经授权或违法使用者需自行承担由此引发的一切法律后果及相关责任，本公司将依法予以追究。

免责声明

本报告仅供本公司的客户或公司许可的特定用户使用。本公司不会因接收人收到本报告而视其为本公司的当然客户。任何非本公司发布的有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以本公司发布的本报告完整版本为准。

本报告中的行业数据主要为分析师市场调研、行业访谈及其他研究方法估算得来，仅供参考。因调研方法及样本、调查资料收集范围等的限制，本报告中的数据仅服务于当前报告。本公司以勤勉的态度、专业的研究方法，使用合法合规的信息，独立、客观地出具本报告，但不保证数据的准确性和完整性，本公司不对本报告的数据和观点承担任何法律责任。同时，本公司不保证本报告中的观点或陈述不会发生任何变更。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。

本报告所包含的信息及观点不构成任何形式的投资建议或其他行为指引，亦未考虑特定用户的个性化需求或投资目标。用户应结合自身实际情况独立判断报告内容的适用性，必要时应寻求专业顾问意见。报告中涉及的评论、预测、图表、指标、理论等内容仅供市场参与者及用户参考，用户需对其自主决策行为负责。本公司不对因使用本报告全部或部分内容所产生的任何直接、间接、特殊及后果性损失承担任何责任，亦不对因资料不完整、不准确或存在任何重大遗漏所导致的任何损失负责。

引 言

随着量子计算技术的强劲创新发展，作为其工程化落地的现实版量子计算机终会问世，或者说传统密码体系是否升级迁移并不能阻挡量子计算能力的发展和量子计算机的问世。因此，传统公钥密码体系必须面对日益现实的颠覆性威胁，而关键信息基础设施领域的重要数据也必须面对“先存储、后解密（HNDL）”的威胁挑战。

根据 NIST 首批 PQC FIPS 标准发布、NIST IR 8547 迁移时间线、NSA/CNSA 2.0 等规划以及关键信息基础设施密码迁移周期判断，2026-2035 年可视为全球密码系统向抗量子安全体系迁移的关键十年，也是最后有效解除风险的行动窗口。与此同时，这场密码体系的重构，并非简单的算法替换，而是涉及协议栈、证书体系、硬件兼容、密钥治理、业务连续性及供应链协同的系统性工程。因此，面向真实场景、聚焦落地过程、跟踪实践成效，开展抗量子安全应用迁移与落地实践研究，已成为当前重点行业必须提前规划、分阶段实施的重要课题。

当前，全球抗量子安全建设已进入标准落地、协议适配、产品验证与过渡期混合部署并行的关键阶段。国际上，NIST 已发布 FIPS 203、FIPS 204、FIPS 205，分别对应 ML-KEM、ML-DSA、SLH-DSA，产业界正围绕 TLS、IPSec、PKI、代码签名、设备身份等场景开展集成验证与分阶段试点；国内，国密后量子密码算法标准化稳步推进，政策导向明确，具有中国特色的“国密合规底座+PQC 规模化替换+QKD 高安全链路+QRNG 熵源增强”多元混合落地架构日渐清晰。在各行业中，金融领域试点最早、实践最深、案例最丰富；运营商、能源、政务等重点行业也陆续进入规划、验证和分级迁移阶段，成为抗量子安全迁移的重点领域。

2025 年，安全牛在业内首个抗量子安全主题研究报告——《后量子密码安全能力构建技术指南（2025 版）》中，率先指出重视量子计算威胁的必要性和紧迫性，并系统梳理出量子计算的演进发展给传统密码体系（尤其是非对称密码）带来的具体影响和重构挑战；2026 年，安全牛又在密码安全产业年度研究报告——《密码安全产业发展关键动因与竞争格局演变（2026 版）》中，从技术对抗维度重点阐述了量子计算发展与量子计算威胁分别为催生出量子安全和后量子密码安全的多元化抗量子安全领域技术路线和发展路径。为统一产业认知、厘清技术边界，该报告海以“抗量子安全”为整体框架，将量子安全与后量子密码安全纳入其中并给出明确定义，清晰界定了 QKD、PQC、QRNG 的技术定位、适用场景与互补关系，为产业提供了统一、清晰、可落地的概念基准。而本次报告则将以应用迁移与落地实践为核心视角，遵循“风险演进—技术锤炼—行业推行”的主线，系统呈现抗量子安全从算法到标准、从产品到各行业落地应用的现实迁移及规模化部署的推进过程，客观反映各行业在抗量子安全实践过程中的探索、突破与经验沉淀。

本报告将围绕抗量子安全工程化落地的核心问题展开深度梳理，重点覆盖密码资产盘点、量子脆弱性评估、混合架构部署、性能优化、多源密钥统一管理、阶梯式迁移、业务连续性保障以及密码敏捷性构建等关键环节。同时结合厂商技术能力、产品成熟度与典型方案，全景呈现产业发展现状，以此识别当前成果与未来能力建设方向。

在此基础上，报告还将以金融行业为核心标杆，提炼可复用的迁移范式，并由此延伸至运营商、能源、政

务等高优先级领域，分别明确行业现状、迁移路径及中长期建设目标，最终为全行业呈现场景化选型规则、分阶段实施步骤、标准化解决方案与成效判定指标。

本报告既是对 2025 年后量子密码产业化进程的延续，也是对 2026 抗量子安全重塑阶段实践成果的系统总结，力求以务实、客观、可落地的研究内容，为行业用户、技术厂商及标准推进方提供参考，共同推动我国抗量子安全体系平稳、有序、高质量落地。

关键发现

1. **安全牛将 2026 年定义为“抗量子安全重塑元年”**，旨在强调抗量子安全行动窗口愈加紧迫，标志着国内抗量子安全建设正在从技术研究、单点试点阶段，进入标准跟踪、资产盘点、试点验证、规模化规划和产业生态重塑并行推进的新阶段，但不同地区、行业和系统的迁移成熟度差异明显。

2. **全球后量子密码正式进入标准化落地周期**，NIST 已发布 ML-KEM、ML-DSA、SLH-DSA 三项首批 PQC 标准，国际生态正围绕标准算法、混合部署、协议适配和密码发现工具进行工程化验证；我国则需在坚持商用密码合规和自主可靠底线的基础上，兼顾国际互联场景对 NIST 标准的适配需求和国内关键信息基础设施对国密体系、本土算法和密评合规的要求，形成“国际互通+本土合规”的兼容式发展道路。

3. **抗量子安全建设是覆盖全业务体系、全密码生命周期和全信任链条的系统性升级工程：**并非单一密码算法替换。整体建设需以密码资产盘点、CBOM 和量子脆弱性评估为迁移起点，同步推进 PQC 算法工程化落地、QKD 高安全链路适配、QRNG 熵源增强、统一密钥与证书生命周期管理、签名类资产迁移、灰度上线和回退策略，依照业务风险和数据长期价值分阶段、分领域稳步推进。

4. **提出“抗量子就绪度（PQR）指标体系”：**通过多维度加权评分划定成熟等级，搭配阶梯式成熟度模型，引入指标证据、数据来源、最低门槛和否决项机制，将抗量子迁移概念性评分工具升级为可用于迁移规划、阶段验收、第三方评估和持续改进的工程化评价框架，为全行业抗量子迁移项目验收与阶段规划提供衡量参考。

5. **构建分领域、可实操、重风控、能量化的全行业抗量子安全迁移实施体系：**依托通用技术范式与标准化实施流程，提出行业适配专属选型方案与推进节奏，实现顶层规划与行业落地的深度衔接。

6. **四大关键行业抗量子安全迁移呈现共性技术路径与差异化落地特征：**金融、运营商、能源、政务行业因业务属性、性能要求、安全底线不同，形成差异化迁移约束，同时聚焦高安全、高影响核心场景，构建了针对性抗量子安全防护体系；各行业典型案例验证了混合架构、基础设施先行、工业适配、轻量化普惠等落地模式；行业共性表现在采用“国密+ PQC +量子赋能”混合架构，面临报文膨胀、算力开销、终端碎片化、存量兼容难四大工程瓶颈；行业差异体现在技术路线、改造模式、防护重点，形成场景驱动、约束适配的分野特征；分层分级、混合架构、密码敏捷、生态协同是抗量子安全规模化落地的关键共识。

7. **国内抗量子安全产业已具备工程化落地基础与多元生态协同格局：**依托基础设施、密码、网安、芯片及新锐创新各生态圈企业，产业整体已处于技术试点向工程化规模化应用过渡阶段，整体应用呈现高端关基场景落地成熟、中小及普惠场景布局滞后的差异化发展现状，但受多重现实因素制约，规模化全域推进仍需补齐体系与应用短板，依托科学落地逻辑稳步实现产业纵深发展。

8. **抗量子安全产业的未来将进入中长期演进态势：**用户、供给、管理层面三方主体分工施策、梯度推进，面对多重发展短板、现状痛点与趋势差距，需划定分领域推进节奏，补齐技术、产业、制度各类发展弱项，逐步建成成熟完备的全域抗量子安全防护体系。

目录

第一章 背景概述

随着量子计算技术的强劲创新发展，作为其工程化落地的现实版量子计算机终会问世，或者说传统密码体系是否升级迁移并不能阻挡量子计算能力的发展和量子计算机的问世。因此，传统公钥密码体系必须面对日益现实的颠覆性威胁，而关键信息基础设施领域的重要数据也必须面对“先存储、后解密（HNDL）”的威胁挑战。

根据 NIST 首批 PQC FIPS 标准发布、NIST IR 8547 迁移时间线、NSA/CNSA 2.0 等规划以及关键信息基础设施密码迁移周期判断，2026-2035 年可视为全球密码系统向抗量子安全体系迁移的关键十年，也是最后有效解除风险的行动窗口。与此同时，这场密码体系的重构，并非简单的算法替换，而是涉及协议栈、证书体系、硬件兼容、密钥治理、业务连续性及供应链协同的系统性工程。因此，面向真实场景、聚焦落地过程、跟踪实践成效，开展抗量子安全应用迁移与落地实践研究，已成为当前重点行业必须提前规划、分阶段实施的重要课题。

当前，全球抗量子安全建设已进入标准落地、协议适配、产品验证与过渡期混合部署并行的关键阶段。国际上，NIST 已发布 FIPS 203、FIPS 204、FIPS 205，分别对应 ML-KEM、ML-DSA、SLH-DSA，产业界正围绕 TLS、IPSec、PKI、代码签名、设备身份等场景开展集成验证与分阶段试点；国内，国密后量子密码算法标准化稳步推进，政策导向明确，具有中国特色的“国密合规底座+PQC 规模化替换+QKD 高安全链路+QRNG 熵源增强”多元混合落地架构日渐清晰。在各行业中，金融领域试点最早、实践最深、案例最丰富；运营商、能源、政务等重点行业也陆续进入规划、验证和分级迁移阶段，成为抗量子安全迁移的重点领域。

2025 年，安全牛在业内首个抗量子安全主题研究报告——《后量子密码安全能力构建技术指南（2025 版）》中，率先指出重视量子计算威胁的必要性和紧迫性，并系统梳理出量子计算的演进发展给传统密码体系（尤其是非对称密码）带来的具体影响和重构挑战；2026 年，安全牛又在密码安全产业年度研究报告——《密码安全产业发展关键动因与竞争格局演变（2026 版）》中，从技术对抗维度重点阐述了量子计算发展与量子计算威胁分别为催生出量子安全和后量子密码安全的多元化抗量子安全领域技术路线和发展路径。为统一产业认知、厘清技术边界，该报告海以“抗量子安全”为整体框架，将量子安全与后量子密码安全纳入其中并给出明确定义，清晰界定了 QKD、PQC、QRNG 的技术定位、适用场景与互补关系，为产业提供了统一、清晰、可落地的概念基准。而本次报告则将以应用迁移与落地实践为核心视角，遵循“风险演进—技术锤炼—行业推行”的主线，系统呈现抗量子安全从算法到标准、从产品到各行业落地应用的现实迁移及规模化部署的推进过程，客观反映各行业在抗量子安全实践过程中的探索、突破与经验沉淀。

本报告既是对 2025 年后量子密码产业化进程的延续，也是对 2026 抗量子安全重塑阶段实践成果的系统总结，力求以务实、客观、可落地的研究内容，为行业用户、技术厂商及标准推进方提供参考，共同推动我国抗量子安全体系平稳、有序、高质量落地。

1.1 量子威胁现实化与产业范式重塑

近十年来，综合国内外市场发展热点与现状，以量子物理、量子通信、量子测量、量子计算等为代表的量子技术领域都在蓬勃发展，企业数量不断增多、技术成果不断迭代更新。其中量子物理和量子计算工程化进程的持续提速，使得量子计算机从实验室原型机走向规模化商用系统的步伐也在加快。

面对量子计算带来的安全威胁，全球网络安全的底层逻辑也在发生不可逆重构。传统密码体系赖以成立的数学安全假设——例如大整数分解、离散对数等计算难题——在量子计算范式下不再稳固，Shor 算法等量子攻击手段理论上可在多项式时间内破解现有非对称密码体系，这使得基于“计算复杂性”的传统信任基石出现裂痕。信息安全正从依赖单一加密算法的“算法安全”走向涵盖密码协议、系统架构、密钥管理、运行环境及持续监测的“体系安全”，防御思维也从静态的、边界式的保护转向动态的、内生式的弹性安全。整个密码安全产业因此面临一次由底层计算威胁驱动的全面升级与范式转移，后量子密码算法的标准化与迁移、量子密钥分发的网络化集成、抗量子攻击的安全协议设计，以及与之配套的芯片、软件和基础设施重构，正在形成新一轮技术与产业变革的核心主线。

需要说明的是，量子计算带来的具体安全威胁可参阅《后量子密码安全能力构建技术指南（2025 版）》研究报告，量子计算威胁带给密码安全产业的重大影响可参阅《密码安全产业发展关键动因与竞争格局演变（2026 版）》。

1.1.1 量子计算逼近实用化，传统公钥密码体系进入风险窗口期

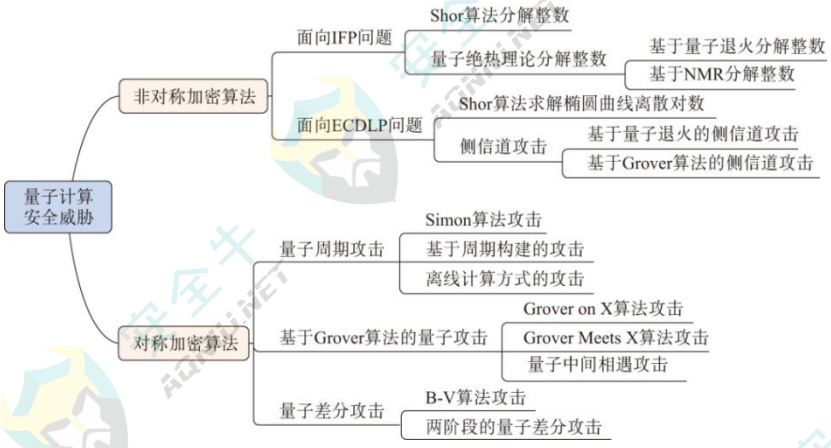
一方面，当前全球对量子计算的重视程度不断提升，正推动相关技术与产业快速发展。全球主要科技强国均将量子计算视为战略竞争制高点，纷纷通过国家战略引导与资本投入等方式展开布局竞争，现已形成多国角逐的发展格局。随着各国持续加大投入力度，量子计算领域的竞争态势预计将愈发激烈。量子计算领域的科研

探索与技术创新进展迅猛，科研论文与发明专利的数量均保持持续上升趋势。虽然产业整体认为，量子计算正处于“工程化实用化初期”或“工业应用探索阶段”，尚未进入大规模工业部署，但已超越纯实验室阶段、向产业化的关键路口迈进。

参考资料

《量子计算发展态势研究报告（2025 年）》（由中国信息通信研究院、中移（苏州）软件技术有限公司和北京玻色量子科技有限公司于 2025 年 9 月 24 日在 2025 中国国际信息通信展览会量子科技产业论坛上联合发布）指出，全球主要科技强国均将量子计算视为战略制高点，技术方面近年来在量子比特规模、逻辑门精度及退相干时间等关键指标上持续取得进展，量子计算正处于从理论研究向应用落地探索转化的关键阶段。在此过程中，跨行业、多场景的应用探索已成为推动应用落地突破的核心驱动力。报告认为量子计算正处于“工程化实用化初期”或“工业应用探索阶段”，尚未进入大规模工业部署，但已超越纯实验室阶段、向产业化的关键路口迈进。

另一方面，量子计算技术与发展的持续突破，正在动摇当代数字社会的安全根基。以 RSA、ECC 为代表的传统公钥密码体系，依托大数分解、离散对数等数学难题构建安全屏障，长期支撑身份认证、数据加密、交易防护、跨域信任等核心能力。随着超导量子、离子阱等主流技术路线不断走向工程化，传统公钥密码的安全假设已不再具备长期可靠性。



量子计算对传统加密体系的安全威胁

图片来源：《后量子密码升级迁移关键问题研究》

参考资料

1994 年 Shor 算法的提出首次从理论上确认了量子计算威胁，促使全球密码学家开始考虑如何对抗量子计算攻击。

美国国家标准与技术研究院（NIST）曾发布一份《后量子密码学》报告，预计最早可能在 2030 年出现首次密码泄露。

滑铁卢大学的另一位专家 Michele Mosca 博士则估计，到 2026 年基础公钥加密工具已经有七分之一的几率被破解，到 2031 年该几率将上升至 50%。

2025 年 5 月 21 日，谷歌量子人工智能部门（Google Quantum AI）在 arXiv 上发表以“How to factor 2048 bit RSA integers with less than a million noisy qubits”（如何利用不足 100 万个含噪量子比特分解 2048 位 RSA 整数）为题的论文。研究表明，采用不足

100 万个含噪量子比特的量子计算机，可在不到一周时间内破解 2048 位 RSA 加密密钥（当前网络数据安全的主流标准），这一数值仅为该团队在 2019 年预测的约 2000 万量子比特的 1/20！而在 2012 年，业内估算破解 2048 位 RSA 密钥需 10 亿个物理量子比特。该研究再次印证了遵循该时间表的紧迫性。

值得一提的是，该团队表示赞同 NIST 内部报告草案——“2030 年后逐步淘汰易受量子计算攻击的加密算法，并于 2035 年后全面禁用”的建议，并不是因为他们认为 2030 年前会出现足够强大的量子计算机，而是不愿将安全保障寄托于技术发展的迟缓。

对此，美国联邦调查局（FBI）相关业务人员在同期 AFCEA 会议上围绕抗量子安全应用迁移事务表示，“当前数据可能成为未来攻击武器，但过渡过程仍需审慎规划——这涉及全局性变革，时间压力虽大，但不可仓促决策。”另一位国务院战略专家也表示，我们只能警示‘若不行动，后果严重’，但决策者仍会质疑投资回报。

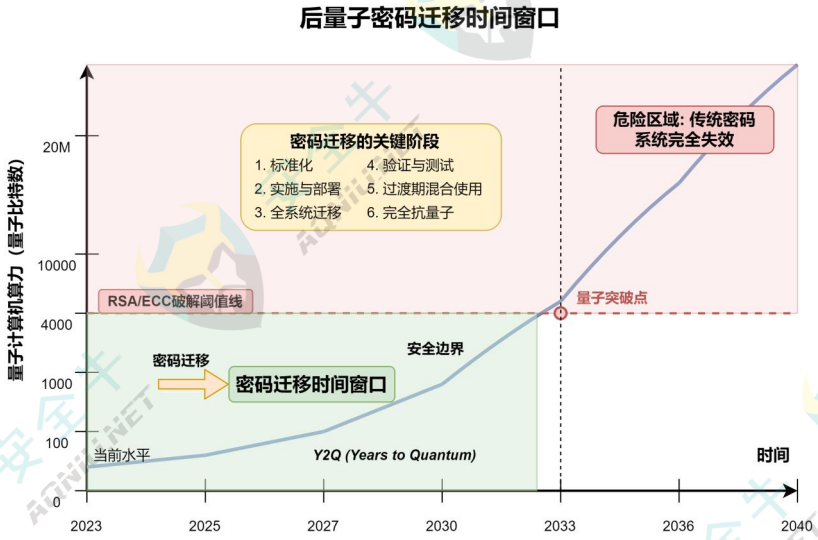
更为紧迫的是，“先存储、后解密（HNDL）”已从理论威胁演变为现实安全挑战。大量政务、金融、关键基础设施、核心隐私等长周期敏感数据，一旦被持续窃取并存储，即可在未来具备实用能力的量子计算机上被快速解密。对于安全周期远超系统迭代周期的关键行业而言，防御动作必须提前布局，抗量子能力建设已从远期规划变为现实刚需。

参考资料

《后量子密码安全能力构建技术指南（2025 版）》中指出：（1）传统计算机的发展一直遵循“摩尔定律”，即算力每 18 个月翻一番，而量子计算是基于量子力学原理的新型计算模式，其并行计算能力和指数级别的速度优势远远超过传统计算机，成为未来计算发展的重要方向，也给传统领域带来致命的攻击风险和安全威胁。（2）量子计算的威胁不仅在于未来可能破解现有的密码系统，更在于攻击者可以在现阶段收集和存储加密通信数据，等待量子计算机成熟后再进行解密。这种“存储今天，破解未来”的策略对敏感信息的长期保密性构成了严重威胁。

后量子密码算法的迁移时间主要是由以下因素决定的：算法标准化与成熟度验证、软硬件系统改造、行业应用适配与测试、用户习惯培养与生态构建等。

安全牛在《后量子密码安全能力构建技术指南（2025 版）》曾指出，抗量子安全算法的迁移是一个复杂而漫长的过程，周期通常为 10-15 年。虽然量子计算机的实用化尚需时日，但量子计算带给密码系统的破解风险以及长期风险都是确定的，并且密码迁移的周期长、复杂度高，留给应用迁移的时间窗口并不宽裕。如果等到量子计算机威胁迫在眉睫时再启动迁移，很可能为时已晚。



因此量子计算带来的安全威胁已经不容忽视，全球主要国家、标准化组织与产业界也已达成共识：应对量子计算挑战的密码体系升级早已不再是可选项，而是一项关乎国家安全、产业安全与数据安全的强制性、体系化任务。

1.1.2 抗量子迁移是系统性工程，而非单一算法替换

行业实践中普遍存在一个误区：将抗量子安全建设简单等同于“算法替换”。事实上，抗量子迁移是覆盖全技术栈、贯穿全生命周期、影响全业务流程的系统性工程，其复杂度、实施周期与协同要求远高于常规安全改造。

抗量子迁移涉及协议栈重构，需要完成 TLS、IPSec、证书体系、应用接口等全链路适配；涉及硬件兼容改造，需要推进加密卡、安全芯片、终端与网关设备的能力升级；涉及密钥管理体系重构，覆盖密钥生成、分发、存储、更新、注销等全生命周期管理机制；更涉及业务连续性保障，要求在不中断服务、不降低体验、不损失效率的前提下完成平滑过渡。

这意味着，抗量子迁移不是单点优化，而是架构级变革；不是一次性项目，而是长期演进能力；不是安全部门的独立任务，而是技术、业务、运维、管理多方协同的系统性工程。能否以工程化思路推进迁移，直接决定关键行业能否平稳度过量子安全过渡期。

参考资料

以 PQC 算法迁移为例，《抗量子密码升级迁移关键问题研究》中指出，PQC 升级迁移是应对量子计算威胁、保障信息安全的关键举措，但在技术标准、性能、安全、实施、行业协同等方面面临着诸多问题：一是性能优化问题。二是标准化和互操作性问题。三是密钥管理问题。四是升级迁移实施问题。五是行业协同与生态建设问题。

此外，自 2025 年施行的《关键信息基础设施商用密码使用管理规定》也明确要求，密码应用需进行全生命

周期、全栈式的合规改造，这涵盖了从规划、设计、实施到运维、评估及退役的各个阶段，并涉及硬件、软件、网络等所有技术层级。这一要求不仅强调了密码技术在关键信息基础设施中的基础性作用，还印证了其作为系统性工程的属性，凸显了改造工作需统筹协调、整体推进的复杂性和必要性。

1.1.3 2026 年成为关键拐点，产业进入抗量子安全重塑阶段

2025 年被安全牛定义为后量子密码产业化元年，其核心标志是算法方向明确、产品形态成型、试点项目启动，行业从理论探讨进入产品化准备阶段。进入 2026 年，随着国际标准落地、国内政策引导加强、关键行业试点成效显现，产业正式迈入全新阶段。

2026 年被安全牛称之为抗量子安全重塑元年，主要体现在三个方面：一是标准从制定阶段进入落地实施阶段，技术路线趋于稳定，产业不再需要在方向上反复试探；二是厂商从产品研发转向工程化交付，解决方案、部署模式、迁移路径逐步成熟，可复制性显著提升；三是行业用户从观望试点转向主动规划，金融、运营商、能源、政务等高优先级领域开始制定中长期路线图，投入、建设与目标更加明确。

参考资料

《后量子密码安全能力构建技术指南（2025 版）》中指出，2025 年作为“十四五”规划的收官之年，结合年初中美两国在后量子密码技术上的成果发布以及对国内密码领域主流厂商非常认可后量子密码技术研究和解决方案必须先行做好准备的调研情况，安全牛分析认为，2025 年可能成为中国后量子密码技术市场的启动年。预计未来 5-10 年内，该市场将逐步扩大，并在 2030 年和 2035 年分别迎来两个发展顶峰。

《密码安全产业发展关键动因与竞争格局演变（2026 版）》中指出，我国当前抗量子安全产品生态已经形成“物理 QKD 领跑、量子通信安全创新、国密与 PQC 叠加、国密与 QRNG 密钥协同”的多元化生态协同与行业应用范式，持续推动我国密码技术从“自主可靠”向“世界引领”跨越，向着下一代国际密码安全技术的标杆蓬勃发展的局面。面对量子计算带来的体系化安全威胁，全球主要经济体正加速战略布局。各国在制定量子密码标准时虽因应用场景和产业基础存在路径差异，但普遍遵循“标准引领、试点推进”的实施策略，重点推动关键信息基础设施的算法迁移工作。基于当前我国密码产业发展态势，安全牛将 2026 年定义为“抗量子安全重塑元年”。

从产业化元年到重塑元年，标志着后量子密码从技术概念走向真实部署，从安全能力补充走向核心基础设施升级，从单点试点走向体系化建设。这一拐点，也是本报告研究的重要时代背景与现实基础。

1.2 概念重构与抗量子安全技术体系边界

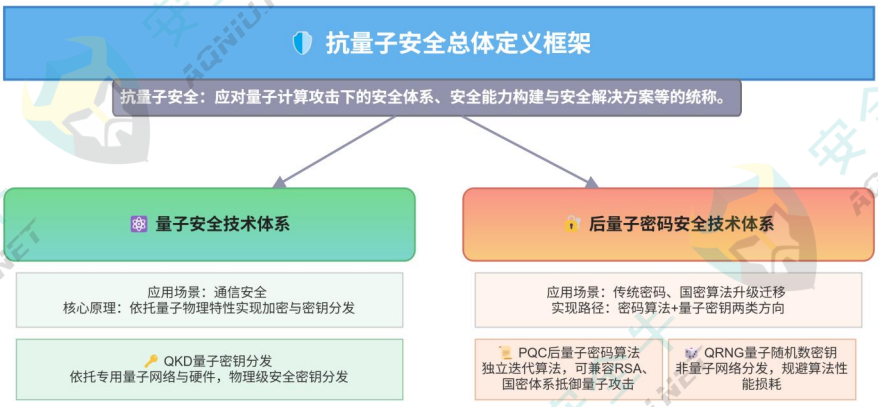
在产业快速推进过程中，概念混淆、路径不清、定位重叠等问题日益突出。为统一行业认知、明确技术边界、指导落地选型，本节节选《密码安全产业发展关键动因与竞争格局演变（2026 版）》中的定义，以“抗量子安全”为统一框架，对技术体系、能力定位、适用场景进行系统性重构，形成可理解、可执行、可推广的体系化认知。

表：抗量子安全相关核心概念统一释义对比

概念名称	权威定义（本报告统一口径）	技术属性	实现方式与环境依赖	与现有体系兼容性
抗量子安全	总体宏观概念，指为应对量子计算攻击所构建的整体安全能力、技术路线与解决方案总称	顶层架构	包含量子安全、后量子密码安全两大类技术路线	覆盖全场景、全架构
量子安全技术体系	专注通信传输安全，基于量子物理特性实现的无条件安全通信的技术体系	量子物理层安全	依赖专用量子传输设备与量子信道；纯物理 QKD	不兼容现有网络，需专用部署
量子密钥分发（QKD）	由量子物理特性生成的密钥并由量子通信网分发的密钥分发机制	量子物理层安全	量子通信网	不兼容现有网络，需专用部署
后量子密码安全技术体系	基于密码算法与密钥机制实现、可抵御量子攻击的密码技术体系	密码算法层安全	分为 PQC 与 QRNG 密钥两条路径	可无缝兼容现有网络与系统
后量子密码算法（PQC）	后量子密码安全的算法升级路线，可抵抗量子计算攻击的新型密码算法	算法迭代	纯软件/固件实现，无需量子物理硬件	可与 RSA、国密（SM 系列）共存、叠加，用户可根据需要选择、切换
量子随机数（QRNG）密钥	后量子密码安全的密钥机制路线，由量子随机数装置生成的密钥，并非量子通信网分发的密钥	密钥管理	仅指通过使用量子随机数装置生成的密钥，传输依托普通专线/现有网络	无需改造业务系统，适配现有 IT 架构

1.2.1 确立“抗量子安全”总体框架

长期以来，量子安全、抗量子安全以及后量子密码（PQC）常被引用混淆，导致指代不明、讨论背景不完整。为了去除混淆、统一概念和理解，安全牛在《密码安全产业发展关键动因与竞争格局演变（2026 版）》研究报告中做出以下定义。



- **抗量子安全：**这是一个总体宏观概念，主要是指应对量子计算攻击下的安全体系、安全能力构建以及安全解决方案等的统称。抗量子安全技术路线可以划分为量子安全技术体系和后量子密码安全技术体系：
  - ✧ **量子安全技术体系：**现主要服务于通信安全，借助量子物理特性和量子通信安全的原理与安全逻辑，通过量子安全专用传输材料和传输网络，完成通信传输过程中的加密和密钥分发，以此来保障量子计

算时代信息通信的安全。其中密钥分发的过程是具备物理安全的 QKD（量子密钥分发），需要借助量子物理环境实现分发。

- ✓ **QKD：量子密钥分发**，指由量子物理特性生成密钥并基于物理形态的量子通信网（专用硬件设备，可能包括专用光纤线路）实现分发的机制。其核心目标是利用量子力学原理，在通信双方之间安全地共享密钥。主流实现方式包括离散变量 QKD（DV-QKD，将信息编码在单个光子的离散量子态上，如偏振态或相位态）和连续变量 QKD（CV-QKD，将信息编码在光场的连续变量，如振幅和相位上，通常采用相干态或压缩态）。

✧ **后量子密码安全技术体系，**现主要服务于传统密码和国密体系的所有算法升级以及迁移。按照密码算法和密钥两类实现路径，可分为 QRNG（量子随机数生成器）密钥和 PQC（后量子密码算法）。

- ✓ **PQC：后量子密码算法，**是一套独立密码算法，凭借算法先进性对抗量子计算的攻击威胁。它是在非量子通信网的前提下，针对密码学、密码算法以及密码安全产业应对量子计算攻击下的密码算法的升级或迁移而形成的迭代密码算法技术体系。它可以与用户当前使用的 RSA 密码体系和国密体系共存、叠加，用户可根据安全要求、应用性能、安全级别等选择需要的密码算法。
- ✓ **QRNG 密钥：量子随机数生成器密钥，**是一套辅助生成量子密钥的系统装置，不同于量子安全中借助量子物理特性生成的量子密钥；此密钥在后量子密码安全技术体系中，依据不同的安全级别和要求，通过网络专线（非量子通信网）或者原网络环境实施分发。它可以在安全级别和要求适合且网络性能受限的系统中使用，相比 PQC 路径可以避免因 PQC 算法带来的性能和效率的损耗。

关键释义

安全牛在《量子安全能力构建技术指南（2025 版）》中所指的 QKD 对应本研究中的量子安全技术体系，PQC 则对应本研究中的后量子密码安全技术体系。两者在密钥生成部分都算量子密钥的范畴，但分发阶段的实现环境不同，因此出现了 QKD 在产业内被引用的混淆。

2025 年及以前，量子计算领域和密码安全领域对于 QKD 的引用和指代各有隐含的前提如下：

- ➢ 量子计算领域所指的 QKD 是由量子物理特性生成密钥并基于物理形态的量子通信网实现，
- ➢ 密码安全领域所指的 QKD 是由量子随机数发生器生成密钥并基于原有（非量子）通信网络实现。

也就是说，抗量子安全是面向量子计算威胁构建的全域安全体系，既包括基于数学算法的软件防御能力，也包括基于量子物理特性的硬件防御能力，二者共同构成完整的抗量子屏障。抗量子安全不是单一技术、单一算法、单一产品，而是覆盖密钥生成、密钥分发、数据加密、身份认证、信任构建、运行防护的全链条安全能力。它以长期安全为目标，以混合架构为过渡形态，以分层防御为实施逻辑，以业务可运行、可监管、可演进为落地原则，是支撑数字社会长期稳定的新一代安全底座。

通过统一“抗量子安全”框架，产业能够摆脱单一技术路线的局限，根据安全等级、业务场景、性能约束、合规要求灵活组合防御能力，真正实现按需部署、平滑迁移、持续演进。

1.2.2 量子安全技术体系：以 QKD 为核心的物理层安全能力

量子安全技术体系依托量子物理特性实现安全防护，核心代表为量子密钥分发（QKD）。QKD 基于量子不可克隆、不可窃听、测量扰动等基本原理，在通信双方之间建立理论上无法被破译的密钥分发通道，属于物理层可证明安全能力。

（一）适用场景和工程实现

在抗量子安全体系中，QKD 面向超高安全等级场景，提供长期稳定的链路级密钥分发保障。它不依赖数学难题，不受制于算力提升，特别适合政务骨干网、金融核心交易、电力调度、跨数据中心专线等对数据安全要求极高、安全周期极长的场景。

工程实现层面，QKD 已形成成熟技术路线，主要包括离散变量 QKD（DV-QKD）与连续变量 QKD（CV-QKD）两大方向，在传输距离、集成度、成本控制、组网能力等方面形成互补。随着量子城域网、城际网逐步建成，QKD 从实验室走向规模化部署，成为我国抗量子安全体系中的独特优势。

（二）生态表现

在应对量子威胁的前沿领域，我国始终秉持 QKD 与 PQC 的双轮驱动核心发展策略。其中 QKD 方面，由运营商牵头、量子计算厂商提供核心技术支撑的量子安全技术体系，持续稳居国际领先阵营。该体系以量子物理安全为核心特色，依托物理量子密钥分发（QKD）技术，在量子通信安全领域构筑起牢不可破的先发优势，目前已在多家运营商的多个省份骨干传输网络中实现规模化部署与广泛应用。

(1) 以运营商为主导，量子计算厂商提供核心支撑的量子安全技术体系，清晰彰显了基于“物理 QKD”的通信安全实现路径，具备高级安全属性，成为对量子安全有极高诉求的行业用户的优选方案；但该体系受限于距离与硬件条件，应用及推广范围目前仍局限于少数场景。

(2) 由量子计算厂商联合通信产业生态主导研发的安全通信创新设备（如中国电信与国盾量子联合打造的“量子密话”产品等）正陆续推出，这些设备的推出，为通信领域开辟了一条成熟且广泛应用的市场路径。

1.2.3 后量子密码安全体系：PQC 与 QRNG 协同互补

后量子密码安全体系面向传统 IT 环境，在不改变现有网络架构的前提下，通过算法与密钥能力升级实现抗量子防御，由 PQC 与 QRNG 构成，二者定位清晰、互补协同。

（一）适用场景和工程实现

后量子密码（PQC）是通用场景下的主力升级路径。它以新一代数学难题为基础，可在传统网络、通用设备、现有协议上运行，兼容国密体系与业务系统，适合大规模推广部署。PQC 覆盖广、成本低、易集成，能够支撑互联网接入、移动办公、开放接口、云端应用等海量场景的抗量子能力升级，是行业迁移的基础底座。

量子随机数生成器（QRNG）是密钥生成环节的增强方案。它利用量子物理噪声生成真随机数，提升密钥本

身的安全性，同时在性能受限、资源约束、低时延要求的场景中，可缓解 PQC 算法带来的计算开销、报文膨胀、时延上升等问题。QRNG 部署轻量、改造量小，可作为 PQC 的有效补充。

（二）生态表现

在应对量子威胁的前沿领域，我国始终秉持 QKD 与 PQC 的双轮驱动核心发展策略。其中 PQC 以及 QRNG 方面，由密码安全厂商主导并提供全链条技术支撑的后量子密码安全技术体系，基于量子随机数生成器（QRNG）密钥与后量子密码算法（PQC）两种路径落地，近年来发展全面提速：

(1) QRNG 密钥主要由量子通信厂商为密码厂商提供产品和技术支撑，其凭借灵活、便捷的可实现性，在诸多政务领域的试点及落地场景中得到广泛应用。

(2) 从国际标准看，PQC 已不再处于“标准待定”状态：NIST 已正式发布 FIPS 203（ML-KEM，来源于 CRYSTALS-Kyber）、FIPS 204（ML-DSA，来源于 CRYSTALS-Dilithium）和 FIPS 205（SLH-DSA，来源于 SPHINCS+）。从国内标准看，我国后量子密码算法征集、评估和国密融合适配仍在推进，产业界可在过渡期采用“国密+NIST PQC”混合方案开展非生产验证、试点部署和密码敏捷能力建设，但正式生产推广仍需结合国家密码主管部门标准、密评要求和行业监管口径稳妥实施。

(3) 以国内主流密码安全厂商为主导的后量子密码安全技术体系，呈现出“百花齐放、百家争鸣”的多元化技术实现特征。一方面，推进多算法并存的产品工程化实践，包括与 NIST 主流后量子密码算法与国密体系的融合方案已成功落地，同时产业界也已完成充分技术储备——待国内标准算法正式确立，全线密码产品可快速完成迭代发布，实现敏捷响应；另一方面，与量子计算厂商合作开发 QRNG 密钥，构建多元化抗量子安全技术路径，在各行业广泛应用中实现百花齐放、多元竞合的格局。

整体来看，PQC 负责通用抗量子能力覆盖，QRNG 负责密钥质量与性能优化，QKD 负责超高安全场景物理层保障，三者共同构成层次清晰、分工明确、协同高效的抗量子安全技术体系。当前抗量子安全产品生态已经形成“物理 QKD 领跑、量子通信安全创新、国密与 PQC 叠加、国密与 QRNG 密钥协同”的多元化生态协同与行业应用范式，持续推动我国密码技术从“自主可靠”向“世界引领”跨越，向着下一代国际密码安全技术的标杆蓬勃发展。

1.2.4 抗量子安全技术边界与误用风险

为避免抗量子安全建设中出现技术泛化和误用，本研究明确以下边界：PQC 是规模化替换现有公钥密码体系的主路径，适用于 TLS、IPSec、SSH、PKI、mTLS、API 认证、代码签名、设备身份等广泛场景；QKD 主要解决特定链路上的密钥分发问题，适用于专线、骨干网、数据中心互联、政务/金融/能源高安全链路等场景，但不直接替代身份认证、证书体系、访问控制、代码签名和数据静态加密；QRNG 的价值在于增强随机数和熵源质量，可用于密钥生成、Nonce、证书签发和终端安全芯片等环节，但不能被定位为独立替代 PQC 的抗量子迁移方案。

因此，“国密+PQC+QKD+QRNG”的混合部署不是简单叠加，而是按安全目标分工：国密解决国内合规与

现有信任体系基础，PQC 解决算法层抗量子替换，QKD 解决少数高价值链路的物理层密钥分发增强，QRNG 解决熵源质量和终端随机数可信问题。项目设计应以业务场景、数据生命周期、合规要求、性能约束和运维能力为约束条件，而不是以单一技术先进性作为选型依据。

1.3 宏观合规演进与中国路径选择

抗量子安全的推进，始终在全球标准竞争、国家战略引导、行业合规约束下开展。不同国家因技术基础、产业结构、安全战略不同，选择了差异化的发展路线。我国依托量子通信领域的积累优势与国密体系建设基础，形成了符合自身需求、兼顾安全与合规的独特发展路径。本节将节选《密码安全产业发展关键动因与竞争格局演变（2026 版）》中的相关图表内容进行关联阐述。

1.3.1 国际标准全面落地，全球进入工程化部署阶段

全球范围内，以美国 NIST 为代表的标准组织已完成首批后量子密码算法筛选与标准化工作。FIPS 203（ML-KEM）、FIPS 204（ML-DSA）、FIPS 205（SLH-DSA）正式发布，标志着国际 PQC 主干技术路线已经明确；但 TLS、IPSec、X.509 证书、代码签名、设备身份等具体应用协议和生态适配仍处于持续演进和工程验证阶段，全球产业正在进入集成验证、分阶段试点和风险管理式部署阶段。

其中：NIST FIPS 203 明确 ML-KEM 为基于 Module-LWE 问题的密钥封装机制，并定义 ML-KEM-512/768/1024 参数集；PQC 工程实践应遵循标准参数集和互操作要求，不应任意裁剪参数。IETF TLS 工作组关于 ML-KEM 用于 TLS 1.3 及混合密钥交换的文档仍以 Internet-Draft 形式持续演进，在相关工程报告中应区分正式标准、协议草案和厂商实现。

表：国际后量子密码算法标准化进程（NIST PQC）核心特征表

核心维度	具体特征
主导机构	美国国家标准与技术研究院（NIST）
聚焦方向	后量子密码安全技术体系（PQC 算法升级）
核心成果	完成首轮遴选，确定 CRYSTALS-Kyber（密钥封装）、CRYSTALS-Dilithium（数字签名）等标准算法
落地节奏	FIPS 草案推进，未来 5 年美国联邦系统将强制实施
技术特点	PQC 为独立算法，可与 RSA 等经典算法共存叠加
产业影响	形成全球技术风向标，构建隐形技术贸易壁垒，倒逼跨国企业适配
发展趋势	持续开展后续算法遴选，完善多场景 PQC 算法体系

参考资料

- **美国引领全球后量子密码算法标准与迁移规范。**美国在后量子密码相关技术领域一直保持了全球领先状态，1982 年美国物理学家费曼首先提出量子计算概念，1994 年美国科学家 Shor 提出首个量子计算攻击算法，1996 年美国密码学家 Ajtai 在后量子密码基础理论方面取得突破，2005 年美国密码学家 Regev 突破实用化后量子密码关键技术。依托其技术优势，美国在后量子密码标准制订方面率先行动，美国国家标准与技术研究院（NIST）于 2009 年发布了后量子密码进展综述，2012 年正式启动了后量子密码算法标准征集，2024 年完成首批美国后量子密码标准草案发布，计划于 2035 年完成后量子密码迁移工作。
- **欧洲后量子密码科研和应用国际领先。**欧洲具备丰厚的密码底蕴，在后量子密码科研和典型应用场景验证方面处于全球领先。在后量子密码算法设计和分析方面，欧洲“地平线 2020”计划于 2015 年开始资助多个后量子密码相关项目，其中 PQCRYPT 项目是全球后量子密码标准化领域影响力最大的旗舰项目，整合了欧洲优势科研力量，在美国后量子密码标准征集工作中提供或参与了半数以上的候选算法。在后量子密码典型应用场景落地方面，欧洲依托其在移动通信和金融领域的优势地位，2023 年率先通过全球移动通信系统协会 GSMA 推动后量子密码在蜂窝通信系统中的迁移工作；2024 年率先通过国际清算银行 BIS 启动金融领域后量子密码迁移验证工作。受限于其政治体制和组织模式，欧洲各国难以推出与美国竞争的后量子密码标准，但是通过积极参与美国后量子密码标准征集获得了该领域的国际领先影响力。在标准化推进方面，欧洲各国依托欧洲电信标准化协议 ETSI 组织了量子安全年度会议，自 2013 年开始打造欧洲的后量子密码技术体系，其底层算法采用美国后量子密码标准，基于此构建协议层、应用层标准，形成完整的后量子密码标准体系。
- **中国后量子密码快速追赶。**我国后量子密码技术研究工作与标准制订工作起步较晚，但通过快速追赶欧美，水平已取得长足进步。2015 年《中国密码学发展报告》指出，后量子密码是我国与国际差距最大的领域之一，同年推动国家重点研发计划、自然科学基金和国家密码管理局密码发展基金加大后量子密码领域的科研投入。2016 年美国面向全球征集后量子密码候选算法，我国科研团队提交了 3 个候选算法，占据全球 3：69 的比例，其中 1 个密码算法进入第二轮评估，占据 1：26 比例，也是亚洲范围内唯一进入第二轮评估工作的候选算法。经过 10 年的发展，目前我国科研团队已经取得多项单点突破，例如格密码底层困难问题 SVP/SIS 问题攻击、密码算法量子计算电路资源评估、量子随机预言机紧致归约、非 NTT 友好多项式快速计算、NTRU 类密码算法设计等。整体而言，我国在后量子密码基础困难问题、设计框架、攻击工具等开创性工作方面与欧美尚有差距，但是在实用化算法设计与分析方面已达到国际先进水平。2025 年 2 月我国商用密码研究院发布了包含后量子密码在内的我国新一代商用密码标准征集计划。
- **国际标准化组织的后量子密码标准竞争。**ISO/IEC JTC1 SC27 WG2，即国际标准化组织（ISO）和国际电工委员会（IEC）联合技术委员会（JTC1）信息安全与隐私保护分委员会（SC27）密码工作组（WG2）是最权威的密码算法国际标准制订机构。欧美在推动自己后量子密码标准制订工作的同时也在 ISO/IEC 推动其标准成为国际标准。ISO/IEC 于 2017-2020 完成了后量子密码标准预研工作，2020-2024 年完成了 XMSS/LMS 两类抗量子数字签名算法的标准制订；2022 年启动抗量子密钥封装算法标准制订工作，预计 2026 年完成；2025 年启动了抗量子数字签名标准化工作，预计未来 3 年完成。互联网工程任务组 IETF 是后量子密码协议国际规范的主阵地，主要包括链路层安全协议 MACSec，网络层安全协议 IPSec，传输层安全协议 TLS，应用层安全协议 HTTPS/LAMPS，点对点消息层安全协议 MLS，数字证书标准 X.509 等。除了在每类协议的专题工作组推进其后量子密码迁移，IETF 于 2023 年成立了 PQUIP 工作组推进共性后量子密码迁移标准。

伴随标准落地，美欧日韩等经济体相继发布国家层面迁移战略、实施指南与时间规划，推动政府、国防、金融、关键基础设施等领域逐步完成密码升级。国际云服务商、设备厂商、安全企业、CA 机构正推出 PQC 兼容产品，混合部署、灰度迁移、算法并行和密码敏捷成为过渡期主流实施模式。需要特别说明的是，IETF 等组织的若干 PQC 协议适配仍属于 Internet-Draft 或持续迭代状态。

参考资料

- **迁移规划方面：**美国 NIST 于 2024 年底发布了《向抗量子密码算法标准迁移》（简称 NIST IR 8547）的指导要求文件。NIST IR 8547 对后量子密码基础算法的安全类别、混合密码算法使用等提出了实际操作层面的细化建议。加拿大、英国和欧盟于 2025 年第二季度先后发布了后量子密码（PQC）迁移规划，加拿大拟在 2026 年 4 月之前，英国拟在 2028 年之前，欧盟成员国拟在 2026 年底之前，完成后量子密码迁移的初步规划及相关准备工作。
- **迁移时间方面：**围绕美国提出的 2035 年完成后量子密码迁移的目标，英国、欧盟、加拿大等国纷纷制定了具体实施方案，并细化了 2035 年之前的阶段性里程碑。2025 年 4 月，英国国家网络安全中心发布《抗量子密码迁移时间线》，明确提出后量子密码迁移计划里程碑；2025 年 6 月，欧盟委员会和欧盟成员国发布《向抗量子密码过渡的协调实施路线图》，提出向 PQC 迁移的明确时间表；加拿大在 2025 年 6 月发布了后量子密码迁移路线图，其中包含 4 个里程碑事件。
- **实施方面：**在数字基础设施方面，全球性互联网企业已率先启动后量子密码迁移。在 NIST 发布标准化的后量子密码算法之后，一些全球化的浏览器、操作系统、云服务平台、应用等互联网数字基础设施，快速推进向 PQC 密码算法迁移，大部分迁移工作的共同特点是都采用混合密码算法。
- **中国方面：**中国近年来在国家密码管理局的指导下科研机构及企业协同推进的研究团队持续开展协同推进后量子密码算法设计、安全性分析及基础理论创新等研究，并取得了一系列重要进展。重点围绕后量子密码算法（PQC）标准化、行业应用展开。

1.3.2 国内合规驱动力强劲，国密抗量子标准稳步推进

在我国，抗量子安全已成为密码战略、数据安全、关键信息基础设施保护的重要组成部分。国家层面高度重视前瞻性安全布局，相关法律法规、政策文件、标准规划均隐含对长周期敏感数据的前瞻性防护要求，推动行业提前布局抗量子能力。

表：中国密码安全领域核心政策演进与产业影响

时间	政策文件	核心合规要求	监管强度	对产业的核心影响
2020 年 1 月	《中华人民共和国密码法》	确立商用密码法律地位，建立“以评促改”制度	基础立法	行业进入法治化轨道，密码应用成为法定方向
2023 年 7 月	《商用密码管理条例》（修订）	密评强制化，覆盖全链条管理	强制监管	密评正式成为刚性要求，市场进入合规爆发期
2023 年 11 月	《商用密码应用安全性评估管理办法》	明确“三同步一评估”，关基 / 等保三级以上系统必须执行	严格执行	压实运营者责任，未合规将面临处罚
2025 年 6 月	《关键信息基础设施商用密码使用管理规定》	规范关键信息基础设施商用密码使用，保护关键信息基础设施安全	年度汇报	明确关基单位对商密应用的职责
2026 年 6 月	《商业秘密保护规定》	将数据、算法纳入保护，覆盖数字化、跨境场景	全域延伸	密码成为数据资产保护刚需，拓展长期应用空间

与此同时，国内抗量子标准体系稳步构建。2025 年密码行业标准化技术委员会正式对外公布启动后量子密码算法征集与评估，推动形成自主可靠、安全高效、适配国情的国密抗量子标准体系。在合规层面，国密合规是不可突破的底线，抗量子升级必须在国密框架内推进，实现“国密为基、抗量子为能力”的双重目标。

表：传统公钥体系/国密密码体系/后量子密码体系之间的技术路线对比

对比维度	传统公钥体系	国密密码体系	后量子密码算法体系（PQC）
代表算法	RSA、ECC、SHA-256	SM2、SM3、SM4、SM9	CRYSTALS-Kyber、Dilithium
技术特征	国际通用、成熟度高	我国自主可靠、全栈配套	抗量子攻击、代数格/编码理论基础
安全能力等级	高（经典环境下）	高（符合国家合规要求）	极高（抗量子+经典安全双重）
抗量子安全性	不安全（可被 Shor 算法破解）	经典安全、量子不安全	安全（可抵御量子计算攻击）
典型适用场景	通用系统、海外场景、存量系统	关基、政务、金融、能源、信创	长期密存、跨代通信、高敏感核心系统
产业落地阶段	大规模应用、逐步替代	全面强制落地	试点过渡、2025 产业化元年
核心定位	历史主流技术	当前合规底座	未来长期技术方向

对金融、运营商、能源、政务等重点行业而言，合规是当下约束，抗量子是必备底座。这种刚性合规需求，将持续推动迁移工作加速落地。

1.3.3 中国路径：混合架构为过渡，双轨并行成共识

结合我国量子通信领先优势、国密体系成熟基础、关键行业业务特点，行业已形成高度共识：中国抗量子安全建设，必须走符合国情的渐进式路径。

过渡期内，最务实、安全、合规的模式是采用“国密+PQC+QKD”混合架构。一方面坚守国密合规底线，保障信任体系、密码服务、密钥管理自主可靠；另一方面引入 PQC 实现大规模场景快速升级，借助 QKD 强化核心链路高安全防护，三者并行不悖、协同增效。

在此基础上，“双轨并行”成为我国落地实践的核心策略：以 PQC 为主体推进全行业算法与算力升级，实现通用场景广泛覆盖；以 QKD 为骨干强化高安全、长周期、跨域场景的物理层保障。双轨并行、分层施策、逐步收敛，既兼顾当前业务稳定运行，又实现面向未来的前瞻性防御。

这一路径既符合我国产业现状，也适配监管要求，同时能够充分发挥我国在量子通信领域的先发优势，是我国密码产业高质量发展的必然选择。

表：中国抗量子安全双轨融合创新发展核心特征表

核心维度	具体特征
发展策略	双轨并行+融合创新，兼顾量子安全技术体系与后量子密码安全技术体系
量子安全技术体系	聚焦 QKD 量子密钥分发，依托量子通信网实现物理级安全的密钥分发，适配高安全需求通信场景
后量子密码安全技术体系	当前以国密 SM 系列为主体，融合 PQC 算法；同步布局 QRNG 密钥，适配性能受限场景；同步自主研发并确立 PQC 标准
算法融合特点	国密+PQC 混合架构，非简单替代，保留国密基础并叠加抗量子安全能力
落地原则	研用结合、试点先行，在政务/金融等重点行业开展融合方案试点
核心要求	多算法体系（SM+PQC+QRNG）协同管理与动态调度能力
产业导向	打造自主可靠的中国特色量子安全能力体系，筑牢数字安全底层屏障

综上，量子威胁日趋现实，全球密码体系正迎来深刻的范式转移，2026-2035 年成为抗量子安全全面迁移的关键窗口期。在以“抗量子安全”为统一框架的前提下，量子安全与后量子密码安全的技术边界得以清晰界定，QKD、PQC、QRNG 的定位分工与协同互补关系形成明确共识。国际标准加速落地，国内国密后量子密码算法稳步推进，“国密+PQC+QKD”“国密+PQC+QRNG”等混合架构成为行业主流过渡形态。我国依托量子通信优势与国密合规基础，确立“混合架构过渡”的核心实践路径，为全行业抗量子安全工程化部署与规模化迁移筑牢认知根基、指明演进方向。

第二章 抗量子安全技术体系与多元混合落地框架设计

全球抗量子安全体系在发展起点、合规框架、数字基础设施、战略导向与产业生态等方面存在显著国别差异，本章将结合我国密码应用现状、量子技术禀赋与行业落地节奏，重点围绕我国抗量子安全技术体系工程化落地的总体逻辑展开系统性分析。

正如第一章所述，量子计算正推动密码安全产业进入范式转移阶段，2026-2035 年是全球密码体系向抗量子安全全面迁移的关键窗口期。当前国际层面已进入标准落地与过渡期融合并行的发展阶段，我国则依托国密体系成熟、量子通信领域领先的双重优势，形成了“混合架构过渡、双轨并行”的整体布局。

梳理以美国为代表的国际后量子密码标准竞争与技术演进格局可见：美国依托长期研发积累，已率先完成后量子密码的理论突破、技术验证、标准定型与迁移部署规划，形成了较为完整的顶层设计与产业生态，在全球范围内占据先发主导地位。从密码技术体系发展的客观规律来看，新一代密码体系从理论创新到成熟落地具有长周期、高复杂度、强迭代性特征，完整构建一套自主可靠、安全可靠、全域适配的新型密码技术体系，通常需要 20-30 年的持续演进，任何国家都难以在短时间内完成从零到一的全链条自主重构。此外在产业实践中，抗量子安全建设并非纯理论推导或标准先行的单向推进过程，而是需要依托真实业务场景完成技术验证、方案迭代与经验沉淀，再反向驱动标准完善与规模化推广。

综合国际竞争格局、技术发展规律与我国产业基础，本研究认为：我国抗量子安全体系建设，应坚持以应用为先导、以试点为抓手的务实推进路径，采用“先开展应用验证、再推动标准制定”的渐进式落地思路，优先在优势场景与关键领域开展试点，通过边试用边迭代、边推进标准化的方式，以实践经验沉淀形成标准规范的需求依据，结合前沿技术演进方向，逐步构建符合国情、适配产业、安全高效的自主可靠抗量子安全标准与技术体系。

2.1 顶层架构：从“单点替换”到“多元混合落地”的体系化重构

当前量子计算技术发展态势强劲，对基于大数分解、离散对数等数学难题的传统公钥密码体系形成确定性与颠覆性威胁，网络安全底层防御逻辑随之从算法安全向体系安全发生不可逆重构。

在早期应用实践中，行业内常将抗量子安全建设简单等同于“把 RSA、ECC 换成新型后量子密码算法”的单点替换，已在金融、政务、运营商等关键信息基础设施领域暴露出明显局限：既难以应对“先存储、后解密（HNDL）”带来的长周期数据泄露风险，也无法兼顾存量系统兼容、业务连续性运行与国密合规底线。

近年来的行业实践表明，抗量子安全迁移绝非局部优化，而是覆盖算法、硬件、密钥、协议、管控与业务流程的全链条系统化重构，必须从“单一技术防御”转向“数学安全与物理安全协同、通用覆盖与高安全兜底互补”的驱动架构，这也是我国平稳推进 2026-2035 年量子安全关键迁移期的核心顶层设计。

2.1.1 威胁倒逼与能力互补：PQC、QKD、QRNG 的技术边界与协同防御模型

量子计算对现有密码体系的威胁呈现分层穿透特征：Shor 算法可直接破解 RSA、ECC、SM2 等非对称密码所依赖的数学难题；Grover 算法可显著降低对称密码安全强度；而“先存储、后解密（HNDL）”模式，则可对政务、金融、能源等领域的长周期敏感数据形成跨代安全风险，此类数据一旦被窃取并存储，将在未来实用化量子计算机上面临被快速解密的隐患。

（一）应用实践中不同技术路线的分工

从应用落地现状来看，单一技术路线均存在场景覆盖盲区：PQC 在通用性、兼容性与部署成本上具备优势，但无法提供物理层无条件安全；QKD 可实现理论安全等级上限，但依赖专用硬件与量子信道，难以实现全域大规模铺开；QRNG 能够快速增强密钥熵源安全性，但无法独立构成完整的抗量子防御体系。

参考资料

- **后量子密码（PQC）**：是能够在现有计算机上运行，并能抵御未来量子计算机攻击的数学密码系统。优势是兼容性强（PQC 可通过混合密码机制与现有系统兼容，无需完全替换现有网络和设备，只需升级软硬件即可实现抗量子攻击）、成本低且部署高效；局限性是安全性依赖数学难题的可靠性、应用场景受限（目前最紧迫的应用是升级 HTTPS 加密，防止攻击者“先收集后解密”传统密码加密的数据）、以及影响业务性能（量子计算攻击使得后量子密码算法设计必须采用更复杂的结构，导致算法参数尺寸大幅增加。目前综合性能最具竞争力的格密码，其密钥和密文尺寸超过 0.5KB，其他算法甚至达到 100KB-1MB 量级，而现有工业标准中的椭圆曲线密码则仅有 32-64B 左右）。
- **量子密钥分发（QKD）**：是利用量子力学原理（如量子不可克隆定理和量子态叠加原理）进行密钥分发的技术，理论上可提供无条件安全；需要专用设备（如单光子源、探测器）和物理环境（如低温、真空），依赖专用光纤或卫星通信，通信距离受限（目前最远记录约 500 公里）；QKD 仅用于密钥分发，需结合传统密码算法（或 PQC 算法）加密数据，而传统算法已无法抗量子攻击；受限于硬件和部署成本，QKD 目前仅适用于对安全性要求极高的场景。QKD 已在实际中应用，例如中国“墨子号”量子卫星实现了千公里级量子密钥分发，但大规模部署仍面临挑战。为解决传统算法不抗量子的问题，QKD 需与 PQC 结合，例如用 PQC 加密 QKD 分发的密钥。

- **QRNG（量子随机数发生器）：**基于量子过程（如光子偏振、真空涨落）生成真随机数，作为密码系统中密钥生成、Nonce 等的熵源，提升随机性安全性，不直接用于加密或通信，而是支撑其他密码组件。优点是生成真随机数（不可预测，优于伪随机算法）、 熵源可靠（符合密码学严格随机性要求）；缺点是仅提供熵源（不能单独构成安全体系）、硬件依赖强（需专用量子器件，集成成本较高）、应用场景有限（主要用于密钥生成、初始化等环节）。

结合本研究调研成果，安全牛发现：基于威胁特征与技术特征差异，PQC、QKD、QRNG 三者已形成较为清晰的能力边界与互补关系。

(1) **后量子密码（PQC）作为算法层通用防御基座**：以格密码、编码理论等新一代数学难题为安全基础，无需专用量子硬件，可无缝兼容现有网络架构、通信协议与国密体系。目前 NIST FIPS 203/204/205 标准已进入工程化落地阶段，国内国密后量子密码算法研究与评估同步推进，CRYSTALS-Kyber、Dilithium 等算法与国密融合方案已在金融、政务等场景完成试点验证，承担全行业、全场景规模化抗量子覆盖的主体任务。

(2) **量子密钥分发（QKD）承担物理层高安全兜底能力**：依托量子不可克隆、测量扰动等基本物理原理实现理论无条件安全，不受算力突破影响。我国已建成“京沪干线”、合肥量子城域网、长三角量子通信环网等规模化基础设施，中国电信、中国联通联合金融机构开通跨省量子 OTN 专线，验证了 QKD 在运营商/政务骨干网、金融核心交易、电力调度、跨数据中心专线等超高安全等级、超长数据生命周期场景的工程可行性。

(3) **量子随机数（QRNG） 作为密钥质量增强与性能补位手段**：通过量子物理噪声生成真随机数，从源头提升密钥安全性，同时可缓解 PQC 算法在边缘终端、低性能设备上带来的计算开销与时延上升问题。目前 QRNG 已实现芯片化、模块化集成，可嵌入安全芯片、加密卡、智能终端与物联网设备中，为存量系统提供轻量化、低成本的抗量子能力补强路径。

三者协同构成“通用防御+高安全兜底+性能增强”的多元化落地方案：PQC 解决“全域规模化基本面”的覆盖，QKD 解决“核心链路重要节点”的极致安全，QRNG 解决“存量改造与性能约束场景”的兼容补位问题，共同应对量子计算带来的全维度、长周期安全威胁。

QKD 的部署前提是可获得可管理的量子链路、可信中继或密钥服务池，且其主要作用是密钥分发；QRNG 应被纳入密钥生成和熵源管理体系，无法独立成为后量子加密算法。对通用互联网、移动应用、API 网关、云原生服务和大规模终端接入而言，PQC 及其混合密钥交换/混合签名方案仍应作为主路径。

（二）未来确定性发展趋势

安全牛认为，从全球技术演进与产业落地态势看，抗量子安全技术体系正呈现四大确定性发展趋势：

(1) **一是标准收敛与生态融合加速**，NIST 首批标准已进入联邦系统强制部署阶段，国密后量子密码算法征集与评估工作稳步推进，多算法共存、混合架构成为行业普遍采用的过渡期主流形态；

(2) **二是工程化导向全面取代纯理论研究**，产业重心从算法设计转向报文膨胀优化、硬件加速卸载、协议兼容适配等真实落地难题，PQC 与 QKD 均朝着低成本、高集成、易部署、易运维方向持续演进；

(3) **三是管控平台走向中心化与服务化**，统一密钥管理、密码服务抽象化、量子密钥即服务（QKaaS）逐步成为行业标配，有效支撑多源密钥协同调度与算法热插拔能力；

(4) **四是场景化分层防御成为产业共识**，高安全域以 QKD 主导构建物理层安全，通用高并发域以 PQC 全面覆盖，边缘与物联网端以轻量“PQC+QRNG”增强，安全能力与业务需求精准匹配，推动抗量子安全从单点试点逐步走向规模化、常态化部署。

2.1.2 中国特色多元落地演进：国密打底+QKD 做后盾+PQC 加速跑+QRNG 补位

全球抗量子安全迁移不存在统一范式，各国均依据技术基础、产业生态与监管要求选择差异化发展路径——美国以 NIST PQC 为核心推进联邦系统强制迁移，欧盟侧重隐私与关键基础设施保护。我国依托国密体系成熟自主、量子通信部署规模全球领先的双重优势，逐步形成双轨并行、混合架构的渐进式演进态势，呈现为“国密算法打底+QKD 做后盾+PQC 加速跑+QRNG 补位”，这一路径已在金融、政务、运营商、能源等重点行业试点中得到实践验证。

- **国密算法打底**：以 SM2/SM3/SM4/SM9 等国密算法为合规底座，坚守密码自主可靠底线。《关键信息基础设施商用密码使用管理规定》明确要求关键信息基础设施运营者全生命周期合规使用商用密码，所有抗量子升级均在国密框架内实施，确保信任体系、密钥管理与密码服务全程合规、自主可靠。
- **QKD 做后盾**：充分发挥量子通信规模化部署的先发优势，将 QKD 作为核心链路与高安全域的物理层安全后盾。我国已建成天地一体化量子通信网络，骨干线路总长度超过万公里，量子密钥服务池化（QKaaS）模式逐步成熟，可为长周期、高敏感数据提供信息论安全保障，从根本上抵御“先存储，后解密（HNDL）”跨代解密威胁。
- **PQC 加速跑**：同步对接 NIST 国际标准与国密后量子密码算法发展方向，持续推进 PQC 与国密算法的深度融合适配。一大批国内主流密码厂商已在近两年陆续完成“国密+PQC”混合算法、混合证书链的技术储备，TLS 1.3、IPSec、国密 SSL 等协议适配方案也已趋于成熟，能够以软件化、轻量化方式实现全行业快速覆盖，有效压缩迁移周期、降低总体改造成本。
- **QRNG 补位**：面向存量系统改造难度大、边缘终端算力资源有限的场景，以 QRNG 快速增强密钥熵源。量子随机数发生器已实现小型化、低功耗、高稳定度工程化，可直接嵌入安全芯片、加密卡、物联网终端等设备，无需重构协议与硬件，即可实现低成本、即插即用式抗量子能力补强。

一方面上述路径贴合我国合规底线与产业现实，另一方面这一路径并非技术的简单叠加，而是合规要求、安全等级、部署成本、实施效率四者的综合最优解。国内多家运营商与密码企业联合推出的“QKD+PQC”分布式密码体系，已在跨省密话、金融专线、政务专网等场景实现商用验证，既规避了全盘替换带来的业务中断风险，又充分释放我国在量子通信与国密领域的技术禀赋，是适配国情、可长期稳定演进的最佳实践路径。

2.1.3 面向平滑迁移的核心基线：密码敏捷性架构要求与过渡期业务连续性保障

抗量子安全迁移是一项长达 10-15 年的系统性工程，期间将面临标准持续迭代、业务系统动态升级、量子威胁等级不断提升等多重变量。传统“一次性改造、静态部署”的架构模式，极易引发重复建设、业务中断、

合规滞后、投资浪费等问题。国际上，法国央行、美联储、谷歌、微软等机构均将密码敏捷性列为过渡期架构的核心原则；我国金融、政务、运营商等行业试点实践也证实，密码敏捷性是保障业务连续性的关键前提。

密码敏捷性架构以解耦、兼容、动态、可演进为核心要求，相关设计已在国内关键行业落地应用：

- **算法与协议深度解耦**：通过抽象密码服务层将密码能力从业务系统、应用逻辑与通信协议中尽量剥离。多家商业银行试点项目中采用该架构，可降低核心业务系统改造范围，并支持国密、PQC、混合算法的灰度切换和分阶段验证。需要强调的是，PQC 与国密/传统算法的密钥结构、公钥长度、签名长度、返回码、异常类型和证书字段差异明显，并非简单“无感切换”，必须经过接口契约、强类型校验和业务回归测试。
- **多体系并行兼容**：支持传统密码、国密、PQC、QKD 密钥共存运行，通过混合证书链、双算法协商、多协议兼容等机制，保障新老系统、新旧设备无缝互通，彻底消除迁移过程中的业务断层。
- **灰度切换与动态调度**：支持按场景重要性、风险等级、业务敏感度实施分批次、灰度式迁移，逐步收敛传统密码算法。国内运营商在骨干网迁移中普遍采用该模式，确保核心业务 7*24 小时不间断运行，非核心业务先行试点、逐步推广。
- **全生命周期可演进**：架构预留标准迭代、技术升级、设备扩展接口，可适配国密抗量子标准发布、新型 PQC 算法落地、QKD 组网扩容等长期演进需求。统一密钥管理平台支持多源密钥统一纳管与协同调度，避免重复投入与架构重构。

业务连续性是密码敏捷性架构的最终目标。迁移全过程需实现服务不中断、体验不下降、效率不损失、合规不突破，我国金融行业量子 OTN 专线、政务量子城域网等实践表明，以敏捷架构将大规模体系化重构转化为用户无感、业务平稳的渐进式升级，可实现抗量子安全建设与业务数字化转型同步推进、相互支撑，成为全行业规模化迁移提供可复制、可推广的工程范式。

2.2 迁移实施体系全流程技术框架

抗量子安全迁移并非简单的算法替换，而是覆盖密码资产梳理、量子风险研判、抗量子安全技术适配、全方位业务流管控重构的系统性工程，其落地成效迁移成效不仅取决于顶层架构设计的科学性，更取决于落地实施过程中基础工作的扎实程度、核心技术的工程化适配能力，以及异构资源的统筹管控水平。本章 2.1 已明确我国“国密算法打底、PQC 加速跑、QKD 做后盾、QRNG 补位”的多元落地架构，本节将围绕“资产盘点、脆弱性评估、算法落地、物理层融合、密钥管控”五个核心环节，阐述从“迁什么”到“怎么迁、怎么管”的抗量子安全迁移实施技术框架，旨在为行业场景化落地提供技术范式与实践指引的参考。

第一步，建立密码资产清单；第二步，形成 CBOM/密码物料清单；第三步，开展量子脆弱性评估；第四步，确定迁移优先级；第五步，设计混合过渡架构；第六步，在非生产环境开展互操作和性能测试；第七步，分批上线、灰度切换和应急回退；第八步，纳入统一密钥、证书、SOC/SIEM、变更管理和供应商路线图的常态化运营。

上述每一步均应形成明确交付物：资产清单、CBOM、风险评分表、迁移批次表、混合架构设计、测试报告、上线回退方案、运营监控指标和验收证据包。只有形成上述交付闭环，抗量子安全迁移才可从“技术方案”转

化为“工程项目”和“可审计过程”。

2.2.1 迁移起点：密码资产盘点与量子脆弱性评估

抗量子安全迁移的首要前提是摸清存量密码资产底数、识别量子安全风险敞口，避免盲目改造或遗漏高风险节点。当前多数行业存量系统存在密码调用分散、算法依赖复杂、资产台账缺失、跨系统依赖不清等问题，传统人工梳理方式效率低、易出错、覆盖不全，难以适配大规模、异构化系统的盘点需求。基于此，自动化、体系化的资产盘点与脆弱性评估成为迁移工作的核心起点与基础保障。

（一）存量密码资产自动化发现与依赖图谱构建

存量密码资产涵盖算法、密钥、证书、加密组件、密码服务接口等全类型资源，广泛分布于主机、网络设备、安全设备、业务系统、终端、批处理平台、灾备系统、主机/小型机、老旧中间件和第三方接口中，且与业务流程深度耦合。自动化资产发现是必要手段，但不能作为唯一迁移起点。对大型银行、运营商、能源央企和政务平台而言，日常流量分析、代码扫描、配置审计和接口探测只能覆盖活跃路径，容易遗漏年度决算、灾备切换、跨境特殊清算、熔断回退、离线批处理等低频“冷资产”。因此，本报告将资产发现明确为“自动化白盒/黑盒测绘+运行时动态插桩+灾备/沙箱触发验证+历史蓝图人工审计”的三位一体方法。

其中：

- 对“冷资产”和历史架构，应在季度或年度灾备演练、沙箱仿真、回退链路演练、异常清算流程演练中人为触发低频业务路径，使隐藏的 RSA/ECC/SM2 调用、硬编码密钥、旧版证书链和非标准加密组件在日志、流量或调用栈中显形。
- 对无法充分触发的老旧系统，应结合历史设计蓝图、接口文档、变更记录、批处理脚本、主机作业调度、运维手册和供应商交付文档开展人工审计。
- 对白盒扫描难以覆盖的非标准企业框架、老旧中间件、COBOL/PLSQL/脚本混合系统、二进制组件和闭源 SDK，应补充抽象语法树（AST）依赖追踪、二进制符号识别、运行时探针、eBPF/系统调用观测、密钥/证书文件特征扫描和第三方组件访谈。

- 资产清单应标注“自动发现资产”“人工确认资产”“未验证疑似资产”“冷路径触发资产”四类证据等级，避免以自动化工具输出替代审计结论。

从具体实施层面来看，自动化发现可从三个层面同步推进：

- 网络层：通过解析 TLS、IPSec、国密 SSL 等协议握手流量，识别加密算法套件、证书类型、密钥交换机制；
- 系统层：扫描操作系统、数据库、中间件内置加密模块与密钥存储路径，定位底层加密依赖；
- 应用层：深度检测业务代码中的密码接口调用、硬编码密钥、第三方加密组件依赖，明确应用侧密码使用情况。

在完成自动化识别后，需进一步构建密码资产依赖图谱。该图谱以“资产节点-依赖关系-业务链路”为核心维度，清晰呈现算法与组件、组件与系统、系统与业务的关联逻辑。图谱不仅需标注 RSA、ECC、SM2、AES 等算法的分布位置、使用频次、部署版本，还需明确密码资产的上下游依赖关系、业务优先级、数据流转路径，精准定位核心业务依赖的关键密码节点，为后续脆弱性评估与优先级排序提供数据支撑。金融、运营商行业试点实践显示，依赖图谱可将存量密码资产梳理效率大幅提升，从而有效规避人工盘点导致的资产遗漏、关系不清等问题。

（二）量子脆弱性风险评估模型与分级判定

量子脆弱性评估聚焦传统密码算法、密钥机制、加密链路对量子攻击的抵御能力，结合量子计算技术演进态势与“先存储、后解密（HNDL）”威胁特征，构建科学、可量化的风险评估模型。本研究认为，评估模型可以“算法安全强度、密钥生命周期、数据敏感度、攻击暴露面”为核心指标，采用定性与定量相结合的方式，实现脆弱性的精准分级判定，避免单一维度评估导致的风险误判。

- **算法安全强度维度：**结合 NIST、国密算法安全规范，将传统密码算法可划分为“高脆弱、中脆弱、低脆弱、安全”四个等级。
  - ✧ RSA、ECC 等非对称密码因可被 Shor 算法破解，归为高脆弱等级；
  - ✧ DES、3DES 等弱对称密码易被 Grover 算法降低安全强度，归为中脆弱等级；
  - ✧ SM4、AES-256 等高强度对称密码在量子环境下安全强度可控，归为低脆弱等级；
  - ✧ 国密 SM2 算法虽具备经典安全能力，但不具备抗量子特性，仍归为高脆弱等级。

表：量子脆弱性算法分级对照表

脆弱性等级	典型算法	量子威胁	风险描述
高脆弱	RSA、ECC、SM2	可被 Shor 算法破解	量子威胁明确，需优先迁移
中脆弱	DES、3DES	Grover 算法降低强度	需中期替换，降低暴露风险
低脆弱	SM4、AES-256	强度可控、威胁有限	长期运维优化，无需紧急迁移

脆弱性等级	典型算法	量子威胁	风险描述
安全	国密抗量子、PQC	可抵御量子攻击	长期安全，优先推广

- **密钥生命周期维度**：密钥有效期越长、数据存储周期越久，HNDL 威胁风险越高，脆弱性等级相应提升；
- **数据敏感度维度：**政务机密、金融核心交易、能源调度指令等高敏感数据对应的加密链路，脆弱性等级高于普通业务数据链路；
- **攻击暴露面维度：**互联网公开接口、跨域共享链路等暴露面广的场景，脆弱性等级高于内网封闭场景。

由此，基于多维度指标加权计算，可最终形成四级量子脆弱性分级标准：一级（极高风险）、二级（高风险）、三级（中风险）、四级（低风险）。分级结果直接指导后续迁移工作，一级、二级脆弱性资产需优先纳入迁移清单，三级资产纳入中期改造计划，四级资产可纳入长期运维优化范围，从而实现风险精准管控与资源合理分配。

（三）迁移优先级排序：基于数据生命周期与 HNDL 威胁的量化分析

迁移优先级排序是在资产盘点与脆弱性评估基础上，解决 “先迁什么、后迁什么” 关键问题的核心环节。结合调研，本研究认为迁移优先级排序需综合考量风险等级、数据生命周期、业务重要性、改造成本等多重因素，重点聚焦 HNDL 跨代解密威胁。为避免平均用力或本末倒置，本研究基于行业迁移实践调研，构建了一个量化排序模型，确保有限资源优先投入到高风险、高价值场景。

(1) 量化排序三大核心原则

HNDL 威胁的核心特征是“当下存储、未来解密”，数据生命周期越长、安全周期要求越高，量子威胁的紧迫性越强，迁移优先级自然越高。基于此，量化排序需遵循三大核心原则：

- **高风险优先：**一级、二级脆弱性资产优先于三级、四级资产；
- **长周期优先：**数据生命周期超过 5 年、安全周期要求超过 10 年的资产优先迁移；
- **高价值优先：**核心业务、高敏感数据对应的密码资产优先于普通业务资产。

具体量化过程中，可为各指标赋予差异化权重。如：风险等级权重 40%、数据生命周期权重 30%、业务重要性权重 20%、改造成本权重 10%，通过加权得分计算资产优先级排序值，形成分批次、分阶段的迁移清单。

(2) CBOM 与 AI 辅助资产发现要求

本研究建议在密码资产盘点阶段引入 CBOM（Crypto Bill of Materials，密码物料清单）机制。CBOM 应记录系统名称、业务负责人、算法类型、密钥长度、协议版本、证书链、密码库版本、HSM/KMS 位置、数据保密期限、外部暴露面、供应商、替换复杂度和迁移批次等字段，并与 CMDB、SBOM、证书管理平台、代码仓库、流量探针和 KMS/HSM 台账交叉校验。

此外还可引入 AI 辅助密码资产发现和依赖图谱构建，如利用代码语义分析、配置解析、日志分析、流量特征识别定位 RSA/ECC/SM2 调用、硬编码密钥、弱算法库、过期证书和第三方组件依赖。但 AI 工具不得接触私钥、生产密钥、核心证书私密材料和敏感系统配置；AI 输出结果必须由密码专家、系统负责人和审计/合规人员复核，不能直接作为上线依据。

参考资料

类似量化排序模型的排序方法已在多家银行、政务平台试点应用，有效提升迁移资源利用效率，优先保障高价值、高风险场景的安全升级。例如，金融行业核心交易系统中的 RSA 签名证书，风险等级为一级、数据生命周期 10 年、业务重要性极高，优先级排序值最高，纳入首批迁移清单；政务内网普通办公系统中的 SM2 加密模块，风险等级为一级，但数据生命周期 1 年、业务重要性较低，纳入中期迁移清单；互联网公开页面的 AES-256 加密链路，风险等级为四级、数据生命周期短，纳入长期运维优化范围。

2.2.2 算法层落地：PQC 工程优化与协议兼容适配

后量子密码（PQC）作为抗量子安全迁移的主力技术路线，承担全行业、全场景规模化覆盖任务，其工程化落地直接决定迁移进度与效果。NIST 首批 PQC 标准（FIPS 203/204/205）已正式发布，国内国密后量子密码算法标准也在追赶推进中。综合来看，PQC 算法理论安全性已得到验证，但在实际落地中，“密钥尺寸大、签名长度长、计算开销高、协议兼容性差”等工程化痛点突出，直接导致报文膨胀、握手时延增加、系统性能下降，制约 PQC 大规模推广应用。本节将从标准对标、性能优化、硬件加速、协议适配四个维度，提出 PQC 算法层落地的工程化解决方案，为产业破解性能瓶颈、实现平滑兼容落地提供参考。

PQC 落地不能仅以“支持算法”为验收标准，应建立面向业务场景的性能测试基线。测试对象应覆盖 TLS 1.3、IPSec、SSH、VPN、API 网关、mTLS、国密 SSL、电子签章、代码签名和设备身份认证；测试算法至少覆盖 ML-KEM-768、ML-KEM-1024、ML-DSA-65、ML-DSA-87、SLH-DSA 典型参数集，以及“国密+PQC”“ECDHE+ML-KEM”等混合组合。

测试指标应包括握手时延 p50/p95/p99、吞吐量、CPU 占用、内存占用、证书链大小、报文分片率、连接失败率、重传率、证书验证耗时、签名验签 TPS、密钥轮换耗时和回退成功率。金融场景应强化低时延和账务一致性测试；运营商场景应强化全网规模和终端兼容测试；能源工控场景应强化弱网、长周期、确定性时延和离线可运行测试；政务场景应强化跨域互认、电子证照和合规审计测试。

（一）标准层面：NIST FIPS 标准与中国“国密+抗量子”路线对标分析是前提

面对 NIST 主导的全球 PQC 标准，中国采取了兼容并蓄的策略，既紧跟和适配 NIST 的 PQC 标准，同时追赶并推进国密自主的 PQC 算法及标准。国内外这两套标准路径在算法选型、技术路线、应用场景上既有共性，也存在一定的差异，因此对标分析是 PQC 工程化落地的前提。

- **NIST PQC 标准：**历经四轮遴选，从 2016 年发起、至 2024 年发布的是 CRYSTALS-Kyber（密钥封装）、CRYSTALS-Dilithium（数字签名）、SPHINCS+（哈希签名）三大类算法，在此基础上还在继续收集和更

新，预计会在未来 1-2 年发布下一个新的 PQC 算法标准，其核心优势是“通用性强、国际兼容性好、产业生态成熟”，因此而成为全球通用和国际互联场景 PQC 迁移的主流选择。

- **中国国密自主的 PQC 算法及标准**：坚持“自主可靠、安全适配、国密兼容”的原则，依托国密算法成熟体系，开展 PQC 算法征集、评估与标准化工作，重点研发适配国内场景、兼容国密 SM 系列算法、性能更优的自主 PQC 算法。与 NIST 标准相比，国密 PQC 算法的核心特点是“合规性优先、场景适配性强、安全冗余度高”，重点聚焦政务、金融、能源、关键信息基础设施等国内核心领域，强调与国密体系的深度融合，避免单一依赖国际标准带来的安全风险与合规隐患。

表：NIST 与国密 PQC 标准对标

对比维度	NIST PQC 标准	中国“国密+抗量子”路线
核心算法	CRYSTALS-Kyber、Dilithium、SPHINCS+	自主研发后量子密码算法（征集评估中）
技术特点	通用性强、国际兼容性好	自主可靠、国密深度融合、合规优先
适用场景	通用互联网、国际互联、云原生场景	政务、金融、能源、关基等国内核心场景
生态成熟度	全球厂商适配、生态完善	国内试点推进、生态快速构建

两套算法标准并行并非相互排斥，而是优势互补、协同推进：通用场景、国际互联场景优先采用 NIST 标准算法，保障互联互通；国内核心场景、高安全场景优先采用国密 PQC 算法，坚守自主可靠的底线；当前国内标准尚未公布前，产业在过渡期则采用“国密+NIST PQC”混合算法架构，实现双标准兼容、平滑过渡。据本研究调研发现，国内主流密码厂商已经纷纷完成对 NIST PQC 标准算法的适配，并且在聚焦研发密码迁移工程的敏捷性，使得不同场景需求下能够灵活切换，为双标准并行落地提供技术支撑。

（二）核心痛点破局：报文膨胀与计算时延的握手优化、协议压缩策略

PQC 算法的核心工程化痛点是“报文膨胀与计算时延”：以 ML-KEM、ML-DSA 等算法为例，其公钥、密文或签名尺寸相较传统 ECC 通常明显增大，可能导致 TLS、IPSec 等协议握手报文体积增加、证书链增大、分片和重传概率上升；同时，格密码、哈希签名等算法的计算路径与传统 RSA/ECC 不同，在高并发、低时延、弱终端场景中可能引入 CPU、内存和网络开销。具体开销不宜用单一固定倍数概括，应通过场景化测试给出 p50/p95/p99 时延、吞吐量、CPU 占用、失败率和回退成功率等实测指标。

针对上述痛点，本研究提出从握手流程优化、协议数据压缩、算法参数调优三个层面制定优化策略。

- **握手流程优化：聚焦减少 PQC 算法调用频次、简化握手交互步骤**

✧ 采用“预共享密钥（PSK）+PQC”混合握手模式，首次握手完成 PQC 密钥协商后，后续握手复用 PSK，

避免重复执行 PQC 复杂运算；

- ✧ 优化 TLS 1.3 握手流程，将 PQC 密钥封装、签名验证等操作并行处理，缩短握手交互时间；
- ✧ 采用会话复用、会话 ticket 机制，减少频繁握手带来的性能损耗。

- **协议级报文体积控制：针对证书链、握手频次、分片风险与会话恢复机制**

  - ✧ ML-KEM、ML-DSA 等 PQC 公钥、密文和签名在设计上接近高熵伪随机数据，通用 LZ 类压缩算法通常难以获得稳定压缩收益，甚至可能因压缩头、分块元数据和失败回退造成报文反向膨胀。
  - ✧ PQC 报文膨胀治理应转向协议级和工程级措施：减少完整握手频次、缩短证书链、优化证书携带方式、会话恢复、缓存可信证书、控制混合算法组合数量、评估 MTU/分片/重传影响，并通过实测给出不同链路下的报文增量和失败率。
  - ✧ 证书与握手优化应采用标准化、可互操作的方法：首次连接可完整传输传统/国密与 PQC 复合证书链，后续连接优先采用 TLS 1.3 会话恢复、PSK、会话 Ticket、证书缓存、证书链最小化和必要场景下的标准化证书压缩机制；对必须传输的 PQC 公钥、密文或签名，只能采用算法标准、协议标准或实现规范允许的编码规整方式，禁止为了压缩体积进行任意截断、舍入或非标准字段省略。任何“格元素截断”“参数精简”均须经过标准兼容性、安全性和互操作性验证，不得作为通用工程建议直接推广。

- **算法参数调优：以保障安全强度为前提**

算法参数不得以“降低密钥冗余度、压缩多项式精度”等非标准方式擅自调整。PQC 工程优化应优先选择已标准化参数集、经过验证的实现优化、常量时间实现、向量化/硬件加速、批处理、会话复用、证书链最小化和协议级规整。若确需采用轻量化参数或专用编码，必须经过算法安全评估、标准符合性审查、互操作测试和监管/密评口径确认。

（三）算力瓶颈突破：FPGA/ASIC 硬件加速与软硬协同卸载机制

对于金融核心交易、云平台、高并发互联网服务等算力密集型场景，仅靠软件优化难以彻底解决 PQC 算法算力瓶颈，“硬件加速与软硬协同卸载”就成为核心解决方案。硬件加速是指依托 FPGA、ASIC 等专用芯片，将 PQC 算法中计算密集型模块（如多项式乘法、模运算、哈希运算）固化为硬件逻辑，利用芯片并行计算能力大幅提升运算效率，降低 CPU 占用率。

从硬件类型来看，两种方案各有优势：

- **硬件加速**

  - ✧ FPGA 加速：具备灵活性高、开发周期短、适配性强的优势，可支持 PQC 算法参数动态调整、多算法兼容切换，适合试点验证、中小规模部署场景；

- ASIC 加速：具备性能高、功耗低、成本低的优势，可针对特定 PQC 算法进行定制化设计，运算效率约是 CPU 软件实现的 10-20 倍，适合大规模、高并发场景规模化部署。

参考资料

国内多家芯片厂商已推出 PQC 加速 FPGA 卡、ASIC 芯片或相关密码加速能力，部分 PoC 或实验室测试显示可提升 ML-KEM、ML-DSA 等算法吞吐并降低 CPU 占用。但此类数据必须区分“算法裸跑吞吐”“协议握手性能”“业务端到端时延”和“微突发尾部时延”，不得以理想环境聚合吞吐直接替代金融核心交易、证券低时延链路或运营商大规模现网的生产验收。

- **软硬协同卸载机制：**可构建“CPU+硬件加速卡”协同运算架构，将 PQC 算法分为“控制逻辑层”与“计算密集层”。其中：
  - 控制逻辑层（如参数配置、数据收发、结果校验）由 CPU 负责；
  - 计算密集层（如密钥生成、封装、签名、验签）卸载至硬件加速卡执行，实现算力合理分配。
  - 同时构建统一加速接口，支持不同厂商、不同类型加速设备兼容适配，降低硬件依赖风险；优化调度算法，根据系统负载动态分配算力资源，保障高并发场景下的稳定运行。

（四）协议栈平滑演进：TLS 1.3/IPSec/国密 SSL 的混合证书链与向后兼容设计

PQC 算法大规模落地需解决与现有协议栈、传统密码体系的兼容问题，避免改造过程中业务中断、新老系统无法互通。当前主流通信协议（TLS、IPSec、国密 SSL）、证书体系均基于 RSA、ECC、SM2 等传统密码算法设计，直接替换为 PQC 算法会导致兼容性故障，本研究认为，“混合证书链、双算法协商、向后兼容设计”将成为协议栈平滑演进的核心路径。

- **混合证书链：**主要指的是采用“传统算法证书+PQC 算法证书”双证书并行模式，证书中同时包含 RSA/ECC/SM2 公钥与 PQC 公钥，支持传统客户端与 PQC 客户端同时接入：
  - 传统客户端通过传统算法完成身份认证与密钥协商，PQC 客户端通过 PQC 算法完成安全交互，实现新老客户端无缝兼容。
  - 国内多家主流 CA 机构已推出国密+PQC、RSA+PQC 混合证书，支持 TLS、国密 SSL 协议适配，已在政务网站、金融 APP、云平台等场景部署应用。
- **双算法协商机制：**优化 TLS 1.3、IPSec、国密 SSL 协议握手流程，支持传统算法与 PQC 算法动态协商：
  - 握手阶段双方交换算法支持列表，优先协商 PQC 算法；
  - 若对方不支持 PQC 算法，自动降级为传统算法，保障互通性。
  - 协议栈改造可采用模块化、插件化设计，将密码算法模块从协议核心逻辑中剥离，同时需要支持 PQC 算法插件灵活插拔、动态加载，从而无需重构协议核心代码即可完成算法升级，降低改造难度与风险。
- **向后兼容设计：**
  - 遵循“兼容存量、平滑过渡、逐步升级”的原则，协议栈保留传统算法支持能力，不强制下线传统算

法；

- ✧ 采用灰度部署策略，先在非核心业务、边缘节点部署 PQC 算法，逐步扩大覆盖范围；
- ✧ 构建兼容性测试体系，全面验证 PQC 算法与现有系统、设备、终端的兼容性，提前发现并解决适配问题，保障协议栈平滑演进、业务无中断升级。

2.2.3 物理层落地：QKD 与 QRNG 高安全互补融合

量子密钥分发（QKD）与量子随机数（QRNG）作为抗量子安全体系的物理层核心技术，与 PQC 算法形成“通用覆盖+高安全兜底+性能增强”的互补格局：QKD 依托纯量子物理特性提供理论无条件安全，适用于超高安全等级场景；QRNG 通过量子真随机数增强密钥安全性、优化性能，适用于存量改造与资源受限场景；两者均不替代 PQC 算法，而是在特定场景提供安全补强，构建多层次、立体化抗量子防御体系。本节将从 QKD 工程化破局、QRNG 轻量化适配、混合架构实践三个维度，提出物理层技术落地路径与融合方案。

（一）QKD 的工程边界与破局：距离衰减、中继信任模型与量子密钥服务池化（QKaaS）

(1) **QKD 工程化落地挑战：**作为量子物理层高安全技术，其工程化落地面临“距离衰减、中继信任、成本高昂、组网复杂”四大核心挑战，明确工程边界、突破技术瓶颈、创新部署模式，是 QKD 规模化应用的关键。

- QKD 基于光子传输实现密钥分发，光子在光纤中传输时存在固有损耗，导致密钥生成速率随传输距离增加呈指数级下降，传统点对点 QKD 系统有效传输距离通常不超过 100 公里，难以满足广域骨干网、跨城通信等长距离场景需求；
- 长距离传输需引入中继节点，而传统中继节点需对量子信号进行测量、转发，存在密钥泄露、窃听攻击风险，中继信任问题成为制约 QKD 组网的核心瓶颈；
- 同时，QKD 专用设备（量子发射机、接收机、光纤链路）成本高昂，部署维护复杂度高，难以大规模普及。

(2) **QKD 工程化破局：**可从技术优化、信任模型创新、部署模式升级三方面推进：

- **技术优化：**
  - ✧ **采用高灵敏度探测器、低损耗光纤、量子信号放大技术：**提升光子传输效率，将点对点 QKD 有效传输距离可提升至 200 公里以上；
  - ✧ **引入量子中继技术：**通过量子纠缠交换实现远距离密钥分发，无需测量量子信号，规避中继节点窃听风险，目前我国已完成千公里级量子中继技术验证，为广域组网奠定基础。
- **信任模型创新：**可构建“可信中继+量子密钥池”混合信任模型，核心骨干网采用量子中继保障无条件安全，城域网、接入网采用可信中继降低部署成本，中继节点密钥统一汇入量子密钥池，实现密钥集中管理、按需分发，平衡安全与成本。
- **部署模式升级：**可采用量子密钥服务池化（QKaaS），将 QKD 从专用硬件系统升级为云化服务，依托现有量子通信网络构建分布式密钥服务池，用户无需自建 QKD 专用链路与设备，通过网络接口按需获取量子密钥，从而实现按需调用、弹性扩展、低成本接入。QKaaS 模式将可大幅降低 QKD 应用门槛，推动 QKD

从政务、金融核心场景向能源、交通、工业互联网等领域延伸，我国运营商已建成多个省级量子密钥服务池，为行业用户提供标准化量子密钥服务。

参考资料

QKaaS 和量子密钥池应补充容量规划与枯竭保护。QKD 物理链路的成码率、密钥池补充速率、链路可用率和突发业务密钥消耗速率之间可能存在数量级差异；如果将 QKD 密钥误用于高频一次一密式业务数据加密，密钥池很容易在突发流量下被快速消耗。工程上应优先将 QKD 密钥作为会话密钥更新、根密钥派生或高安全链路密钥材料，而不是直接承载万兆级业务流量的逐包密钥消耗。

建议量子密钥池设置水位管理、配额控制、业务分级、密钥预取、限流策略和安全降级策略：高水位正常调度，中水位限制低优先级业务调用，低水位触发 PQC/国密混合密钥协商兜底，枯竭状态进入保护模式并保留最小关键业务密钥预算。降级过程中必须同步启用密钥序列号、时间戳、Nonce、重放窗口、链路绑定和审计日志，防止密钥复用、降级攻击和重放攻击。

（二）QRNG 的即插即用价值：存量系统熵源增强与芯片化/低功耗改造路径

量子随机数（QRNG）基于量子物理噪声（如真空零点能、光子散粒噪声）生成真随机数，与传统伪随机数（PRNG）相比，具备不可预测、不可重复、无规律的特征，可从源头提升密钥、证书、加密数据的安全性，同时缓解 PQC 算法在资源受限场景的性能损耗，是存量系统轻量化升级抗量子安全的最优选择。QRNG 无需专用量子信道，不依赖复杂组网，具备即插即用、改造量小、适配性强的核心优势，适用于终端、物联网设备、安全芯片、加密卡等各类存量系统。

- **存量系统熵源增强是 QRNG 的核心应用场景：**传统密码系统依赖伪随机数生成密钥，伪随机数基于算法生成，存在可预测、可破解风险，尤其在量子计算威胁下，伪随机数安全性进一步降低。QRNG 通过硬件模块直接生成真随机数，替代传统伪随机数发生器，为密钥生成、证书签发、数据加密提供高熵值随机源，从根源提升密码系统抗量子攻击能力。改造过程无需重构业务系统与通信协议，仅需替换或新增 QRNG 模块，对接现有密钥管理接口，从而可实现低成本、无感知、快速化的安全升级，金融 POS 机、智能卡、物联网终端等设备已广泛集成 QRNG 模块。
- **芯片化、低功耗改造是 QRNG 规模化普及的关键：**传统 QRNG 设备体积大、功耗高、成本高，难以嵌入小型化、低功耗终端设备。当前 QRNG 技术已实现芯片化集成、低功耗设计、小型化封装，单芯片尺寸可缩小至毫米级，功耗降至毫瓦级，成本大幅降低，可嵌入安全芯片、MCU、加密卡、手机、物联网传感器等各类终端设备。国内芯片厂商已推出多款国产 QRNG 芯片，支持国密算法、PQC 算法适配，已在政务终端、金融 IC 卡、工业物联网设备中批量应用，为海量存量终端提供轻量化抗量子安全解决方案。

（三）混合架构实践：PQC 软件协商+QKD 物理分发的高可用冗余与双轨密钥冗余机制

PQC 算法与 QKD 技术并非相互替代，而是优势互补、协同增效，构建“PQC 软件协商+QKD 物理分发”的混合架构，可实现安全等级叠加、可用性互补、风险冗余备份，是高安全、高可靠场景的最优部署模式。混合架构结合 PQC 算法的通用性、兼容性与 QKD 的无条件安全性，同时引入 QRNG 增强密钥熵源，形成多层次、高冗余的抗量子防御体系，已在金融核心交易、政务骨干网、跨数据中心专线等场景试点应用。

- **高可用冗余设计聚焦“避免单点故障、保障业务连续性”：**
  - ✧ 核心通信链路可同时部署 PQC 加密通道与 QKD 增强密钥分发通道。PQC 通道承担通用业务数据传输保护，具备部署灵活、成本较低、兼容性较好的优势；QKD 通道或量子密钥服务池可作为高安全链路的密钥分发增强与冗余来源，保护核心敏感数据传输所需的会话密钥。若 PQC 通道出现性能故障、兼容性问题或安全策略触发，系统应按照预设策略切换至备用通道或传统合规通道，确保业务连续性。
  - ✧ 同时，通用业务链路以 PQC/国密混合密钥协商和对称加密保护为主，高安全链路可引入 QKD 密钥池作为密钥材料增强或高安全域冗余来源；当 QKD 密钥池水位不足、链路中断或调度异常时，应按预设策略切换至 PQC/国密混合协商，并记录降级原因、密钥序列和审计证据。
- **双轨密钥冗余机制构建“PQC 软件密钥+QKD 物理密钥+QRNG 随机密钥”三重密钥体系：**
  - ✧ PQC 密钥由软件算法生成，用于通用场景数据加密；
  - ✧ QKD 密钥由量子通信网物理分发，用于核心敏感数据加密；
  - ✧ QRNG 密钥由量子随机数芯片生成，作为密钥熵源补充，提升密钥安全性。
  - ✧ 三重密钥相互独立、冗余备份，即使某一密钥体系被破解，其他密钥体系仍能保障数据安全；同时，密钥采用动态轮换、交叉校验机制，定期更新密钥，防止密钥泄露、复用，构建无死角、高冗余的密钥安全防线。该机制已在政务涉密网络、能源调度系统中部署，有效抵御 HNDL 跨代解密威胁与量子攻击。

2.2.4 管控中枢：统一密钥管理与敏捷调度机制

抗量子安全迁移涉及国密密钥、PQC 软件密钥、QKD 物理密钥、QRNG 随机密钥等多源异构密钥，密钥类型多样、生成机制不同、分发路径差异大，传统分散式密钥管理模式存在管控混乱、调度低效、安全风险高、合规性差等问题，难以适配多源密钥协同管理需求。

本研究基于密钥管控体系调研与行业落地实践认为，应构建统一密钥管理中枢，实现多源密钥统一纳管、敏捷调度、全生命周期安全管控，同时也是保障抗量子安全体系高效运行、防范密钥安全风险、满足合规要求的核心支撑。本节将从多源密钥纳管、敏捷切换机制、全生命周期管控三个维度，阐述管控中枢的构建逻辑与核心能力。

（一）多源密钥统一纳管架构：PQC 软件密钥、QKD 物理密钥与国密密钥的协同调度

多源密钥统一纳管架构以集中管理、分布式部署、标准化接口为核心设计理念，打破不同密钥体系的技术壁垒，构建“国密密钥、PQC 密钥、QKD 密钥、QRNG 密钥”一体化管理平台，实现密钥的统一生成、分发、存储、更新、注销与监控。

该架构可采用分层设计，分为接入层、核心层、应用层，其中：接入层提供标准化适配接口，兼容国密 KMS、PQC 密钥服务、QKD 密钥池、QRNG 模块等各类密钥源，支持不同厂商、不同类型密钥无缝接入；核心层负责

密钥统一存储、权限管控、策略配置、调度决策，构建全局密钥视图，实时监控密钥状态；应用层对接业务系统、加密设备、终端，提供密钥按需分发、动态调用服务，支撑各类业务场景密钥应用。

基于此，协同调度机制可基于场景安全等级、业务优先级、密钥可用性构建智能调度引擎，实现多源密钥动态匹配、最优分配：

- 高安全场景（政务机密、金融核心交易）优先调度 QKD 物理密钥，辅以 PQC 密钥备份；
- 通用场景（互联网服务、办公系统）优先调度 PQC 软件密钥，兼顾成本与兼容性；
- 资源受限场景（物联网终端、边缘设备）优先调度 QRNG 密钥，优化性能损耗；
- 国密合规场景强制调度国密密钥，坚守合规底线。
- 同时，调度引擎须支持策略自定义配置，根据行业规范、安全需求、业务特性灵活调整调度规则；支持密钥负载均衡，避免单一密钥过度使用导致的安全风险；支持密钥故障自动切换，保障业务连续性。

（二）敏捷切换机制：算法热插拔、抽象密码服务层设计与双标自适应路由

抗量子安全迁移周期长达 10-15 年，期间 PQC、国密算法标准持续迭代，量子威胁动态升级，传统静态密钥管理模式难以适配算法更新、策略调整需求。敏捷切换机制成为调研中呼声最强烈的一项需求，但敏捷切换机制的目标不是“一键无感”，而是在严格接口契约、版本治理、影子测试、灰度发布、回退策略和审计留痕基础上，实现可控、可验证、可回退的算法、密钥和策略更新。

敏捷切换机制依托算法热插拔、抽象密码服务层、双标自适应路由三大核心设计，有效化解标准迭代、技术升级带来的反复改造风险。

- **算法热插拔须支持 PQC、国密、传统密码算法插件化管理和动态加载：**
  - ✧ 管控中枢可将各类密码算法封装为标准化插件，与业务系统解耦，无需重构业务代码即可完成算法新增、更新、下线；
  - ✧ 可支持算法灰度切换，先在部分业务节点试点新算法，验证稳定后逐步扩大覆盖范围；
  - ✧ 可支持算法并行运行，新老算法同时在线，保障切换过程中业务互通、无中断。

参考资料

算法热插拔须支持 PQC、国密、传统密码算法插件化管理和动态加载，但必须限定在经兼容性验证的接口契约内运行。每一种算法插件均应声明版本号、参数集、公钥/私钥/密文/签名字段长度、编码方式、错误码、异常类型和回退策略，业务侧不得直接解析未知二进制流或未登记结构体。

因此，建议在抽象密码服务层（CaaS）与业务应用层之间增加 Sidecar/动态代理或服务网格式适配层。代理层负责算法路由、结构体版本转换、强类型 JSON/Protobuf/ASN.1 校验、字段长度校验、异常隔离和日志审计，避免 PQC 密钥结构、签名长度或证书字段变化直接冲击主业务线程。

此外，算法版本切换前必须执行影子测试（Shadow Testing）和契约测试：新算法返回的字符串、二进制流、证书链、签名、错误码先由代理层预解析并与旧链路并行比对；一旦发现字段长度不匹配、类型溢出、证书链解析失败、验签失败率异常或业务状态机污染风险，应自动进入沙箱隔离，并按预案降级至存量合规国密链路或传统受控链路，严禁将异常扩散到主交易、主清算或主调度流程。

- **抽象密码服务层（CaaS）可构建统一密码服务接口，屏蔽底层算法、密钥、设备差异：**
  - ✧ 业务系统仅需对接标准接口，无需感知底层技术细节；
  - ✧ 服务层可支持多算法、多密钥、多协议兼容适配，实现“一次对接、全场景适配”，大幅降低业务系统改造难度。

- **双标自适应路由须适配国密标准与 NIST PQC 标准双套标准需求，构建双标准兼容路由体系：**
  - ✧ 管控中枢须根据业务场景、对接对象、合规要求自动匹配标准，国内合规场景优先路由国密算法链路，国际互联场景优先路由 NIST PQC 算法链路；
  - ✧ 须支持双标准链路并行传输、数据同步，保障新老系统、国内外节点无缝互通；
  - ✧ 须支持标准策略动态调整，系统可根据政策更新、安全态势灵活切换标准优先级，平衡合规性、安全性与兼容性。

（三）密钥全生命周期安全：跨域路由隔离规范与量子密钥分发合规性审计

密钥全生命周期安全管控覆盖密钥生成、分发、存储、使用、更新、注销、销毁全环节，从而构建闭环安全防护体系，防范密钥泄露、篡改、滥用、丢失等安全风险。主要通过跨域路由隔离规范和量子密钥分发合规性审计来实现：

- **跨域路由隔离规范：**针对密钥跨域传输、跨网共享场景，明确密钥路由路径、访问权限、安全防护要求：
  - ✧ 如采用专用密钥传输通道、加密隧道隔离、访问控制列表（ACL）等技术，隔离不同安全域、不同网络区域的密钥流量，防止密钥跨域泄露、非法访问；
  - ✧ 严格管控密钥跨域分发权限，遵循“最小权限、按需分发”原则，仅授权合法节点获取对应密钥；
  - ✧ 采用密钥分片、多副本存储、异地备份等机制，保障密钥跨域传输过程中的完整性、可用性。
- **量子密钥分发合规性审计：**聚焦 QKD、PQC、国密密钥的全流程合规管控，构建自动化、常态化审计体系，满足《密码法》《商用密码管理条例》《关键信息基础设施商用密码使用管理规定》等法律法规要求。其审计内容涵盖密钥生成合规性、分发路径合规性、存储安全合规性、使用权限合规性、更新注销合规性：
  - ✧ 核查 QKD 密钥分发是否遵循量子通信安全规范，PQC、国密密钥生成是否符合算法标准要求；
  - ✧ 审计密钥分发记录、访问日志、操作轨迹，追踪密钥全生命周期流转；
  - ✧ 定期开展密钥安全评估、漏洞检测、合规检查，及时发现并整改安全隐患；
  - ✧ 生成标准化审计报告，留存审计记录，满足监管审查、合规验收需求。

2.3 场景分层落地范式与抗量子就绪度评估

抗量子安全迁移的最终目标，是在不同业务场景中实现安全、可用、可控、合规的平衡，而非采用单一标准、单一架构进行一刀切式改造。我国“国密打底、QKD 做后盾、PQC 加速跑、QRNG 补位”的多元落地路径，

天然决定了落地模式必须场景化、差异化、分层化推进。不同场景在数据敏感度、生命周期、并发规模、算力条件、合规等级上差异显著，对应的技术选型、部署策略、安全目标必然不同，无法用一套方案覆盖所有场景。

基于行业实践与场景特征，本研究提出分层落地范式与就绪度评估体系，针对极高安全、通用高并发、边缘物联网三类典型场景，明确差异化技术组合、部署策略与安全目标；并建立抗量子就绪度（PQR）指标体系与阶梯式成熟度模型，为迁移成效提供可量化、可验收、可迭代的判定标准，从根本上解决“做成什么样、做到什么程度、效果如何衡量”的交付痛点，为全行业迁移提供目标指引与验收参考。

2.3.1 极高安全场景：QKD 主导+PQC 应急+零信任融合

极高安全场景是国家关键信息基础设施与核心敏感数据的集中承载区域，主要包括政务涉密网络、国防通信链路、金融核心交易骨干、关键能源调度专网、跨域涉密数据交换节点等。这类场景的核心特征是：数据生命周期长达 10 年以上、敏感度极高、安全周期要求远超系统迭代周期、面临明确的 HNDL 跨代解密威胁、必须达到信息论级安全保障、合规约束极为严格。单纯依赖算法安全已无法抵御量子级威胁，必须构建“物理安全+算法安全+身份安全”三位一体的信息论安全闭环，实现端到端、全链路、无死角的安全防护。

（一）技术组合范式：QKD 主导、PQC 应急、零信任融合

本研究基于高安全场景实践总结，确立如下技术组合范式：

- **QKD 为高安全链路密钥分发增强能力：**核心链路可采用量子密钥分发机制，为特定通信链路提供高安全等级密钥分发保障，从物理层面降低密钥分发被窃听和被中间人攻击的风险。需要强调的是，QKD 不直接替代应用身份认证、访问控制、证书生命周期、代码签名和数据静态加密，仍需与国密、PQC、PKI/证书体系和零信任访问控制协同使用。
- **PQC 为应急与规模化覆盖能力：**当 QKD 链路中断、量子密钥池水位不足、网络不可达或业务突发流量超过密钥供给能力时，系统应按策略切换至 PQC/国密混合密钥协商通道，并同步启用重放防护、降级审计、密钥序列校验和会话绑定机制。该切换应经过演练和性能验证，不能简单设想为天然“无缝”。

- **零信任架构深度融合**：在身份认证、访问控制、权限动态校验、行为审计等层面全面叠加零信任机制，严格遵循“永不信任、始终验证、最小权限、动态授权”原则，构建端到端可信链路，杜绝非法接入、越权访问、内部泄露风险。

（二）安全目标：构建信息论安全闭环

本场景的最终安全目标，是实现抗量子、防截获、防篡改、防泄露、防越权、全链路可信的信息论安全闭环，具体涵盖四大维度：

- **密钥分发安全**：由 QKD 提供理论不可破译、不可窃听、不可篡改的密钥分发保障；
- **数据传输安全**：采用 PQC + 国密 + QKD 三重加密防护，同时抵御量子破解与传统网络攻击；
- **访问控制安全**：零信任架构实现细粒度、动态化、持续化权限控制，全程验证、最小授权；
- **全链路审计安全**：密钥、算法、访问、操作全程可追溯、可审计、可追责，满足最高级合规要求。

（三）典型应用特征

- **数据生命周期**：10 年以上；
- **安全等级**：最高级（信息论安全）；
- **改造重点**：骨干链路、核心节点、跨域通道、涉密数据交换节点；
- **实施难点**：链路专用、设备成本高、运维体系复杂、合规约束强、需长期稳定运行。

2.3.2 通用高并发场景：PQC 全面替换+QRNG 增强

通用高并发场景是数字经济的主流承载区域，涵盖互联网平台、云原生应用、企业核心业务系统、运营商城域网、公共服务平台、移动互联网服务等。这类场景的核心特征是：用户规模庞大、并发量极高、业务时延敏感、算力资源紧张、改造预算有限、存量系统规模大、兼容需求强、数据敏感度中等。此类场景无法承担 QKD 的高部署成本，也难以接受过高的算力开销，必须在安全强度、系统可用性、算力损耗、部署成本、存量兼容性之间找到最优平衡点，实现安全升级与业务稳定并行。

（一）技术组合范式：PQC 全面替换、QRNG 熵源增强、国密并行

本研究基于大规模场景迁移实践，提出如下技术组合范式：

- **PQC 为主力加密算法**：全链路替换 RSA/ECC 等高脆弱传统算法，优先采用 NIST 标准 PQC 算法（如 CRYSTALS-Kyber、Dilithium），实现全域抗量子覆盖，彻底消除量子破解风险；
- **QRNG 增强密钥熵源**：在密钥生成、证书签发、会话密钥生成、随机数调用等关键环节引入量子随机数，从源头提升密钥本源安全性，同时有效缓解 PQC 算法带来的性能压力；
- **国密并行兼容**：保留国密算法作为合规底线，形成“国密+PQC”双算法共存架构，兼顾合规要求与抗量子安全能力；
- **轻量优化策略**：全面采用握手优化、会话复用、协议压缩、参数精简、硬件加速等工程化手段，严格控制

报文膨胀与算力损耗，保障高并发场景稳定运行。

（二）安全目标：抗量子全覆盖、高可用、低损耗

本场景的核心目标，是在可接受性能损耗前提下，实现全链路抗量子、高并发稳定、业务无感、兼容存量、成本可控，具体包括四大核心：

- **算法安全：**全面消除 RSA/ECC 等高脆弱算法风险，有效抵御 Shor 算法破解；
- **性能可控：**PQC 改造后，时延、带宽占用、CPU 负载控制在业务可接受范围，不影响用户体验；
- **兼容性强：**与传统系统平滑互通，支持灰度切换、逐步升级，避免业务中断；
- **密钥安全：**QRNG 大幅提升密钥不可预测性，降低密钥被破解、泄露风险。

（三）典型应用特征

- **数据生命周期：**1-5 年；
- **安全等级：**中高；
- **改造重点：**应用层、网络层、证书体系、密钥生成环节、云平台加密服务；
- **实施难点：**高并发下性能压力、大规模系统兼容、灰度切换控制、算力资源优化。

2.3.3 边缘与物联网场景：轻量级 PQC+绿色计算优化

边缘与物联网场景是数字化转型的末梢神经，包括工业物联网终端、智能传感器、车载终端、智能家居设备、低功耗边缘网关、海量物联网终端等。这类场景的核心特征是：终端数量极为庞大、算力极弱、功耗极低、存储资源有限、网络不稳定、成本高度敏感、部署环境复杂、设备生命周期长达 5-15 年。传统标准 PQC 算法密钥尺寸大、运算复杂度高、算力开销大，直接部署难以适配终端资源约束，必须采用轻量化裁剪、软硬协同、绿色计算优化的定制化路径，在资源受限条件下实现抗量子安全能力。

（一）技术组合范式：轻量级 PQC、QRNG 芯片化、软硬协同优化

本研究基于海量终端适配调研，确立如下技术组合范式：

- **轻量级 PQC 算法裁剪：**在严格保证抗量子安全强度前提下，对标准 PQC 算法（如 Kyber、Dilithium）进行参数精简、运算简化、代码深度优化，大幅降低密钥长度、签名尺寸与计算复杂度，适配终端弱算力、低存储约束；
- **QRNG 芯片化集成：**采用低功耗、小型化、低成本的量子随机数芯片，嵌入终端安全模块，提供高熵值密钥源，替代不安全的伪随机数生成器，从源头提升密钥安全性；
- **软硬协同卸载：**将 PQC 算法核心运算固化在终端安全芯片或硬件安全模块中，由硬件高效完成加密运算，MCU 仅处理控制逻辑，大幅降低终端 CPU 占用与功耗；
- **绿色计算优化：**采用低功耗时钟、动态调频、休眠调度、轻量化协议栈、数据精简传输等策略，适配电池供电、长期在线、资源受限场景，平衡安全、功耗与续航。

（二）安全目标：轻量抗量子、低功耗、长续航、高可靠

本场景的安全目标，是在极低算力、极低功耗、极小体积的严格约束下，实现终端侧抗量子、密钥安全、数据防篡改、低能耗、高稳定、长生命周期安全：

- **算法安全：**轻量级 PQC 有效抵御量子攻击，适配终端资源约束；
- **密钥安全：**QRNG 提供真随机数，防止密钥被预测、破解；
- **功耗控制：**加密运算功耗降至毫瓦级，大幅延长终端续航时间；
- **可靠性：**适应弱网、断网、恶劣环境，长期稳定运行，保障数据安全传输。

（三）典型应用特征

- **数据生命周期：**5-15 年；
- **安全等级：**中；
- **改造重点：**终端安全芯片、加密模块、密钥生成、轻量协议栈、边缘网关；
- **实施难点：**算力限制、功耗敏感、成本控制、大规模批量适配、长期稳定性保障。

2.3.4 迁移成效判定：抗量子就绪度（PQR）指标与阶梯式成熟度模型

为解决迁移成效“无法量化、无法验收、无法对比、模糊主观”的痛点，本研究基于行业迁移实践与安全评估框架，构建抗量子就绪度（PQR）指标体系与阶梯式成熟度模型，实现从定性描述到定量评估、从经验判断到数据驱动、从模糊验收到达标判定，为全行业迁移提供成效判定的参考。

（一）抗量子就绪度（PQR）指标体系

PQR 指标体系全面覆盖资产、算法、密钥、协议、管控、合规、运维、成效八大核心维度，采用定量为主、定性为辅、加权评分、综合判定的方式，客观衡量抗量子安全迁移的整体成效。

综合得分（满分 100）对应就绪度等级：PQR 90-100：完全就绪；PQR 75-89：高度就绪；PQR 60-74：基本就绪；PQR 40-59：部分就绪；PQR 0-39：未就绪。

其中：

- **资产维度（20%）：**密码资产覆盖率、高脆弱算法清除率、资产图谱完整度、资产风险分级准确率；
- **算法维度（20%）：**PQC 覆盖率、国密合规率、算法兼容性达标率、算法性能达标率；
- **密钥维度（15%）：**密钥熵源安全率、密钥轮换及时率、密钥泄露风险率、多源密钥协同调度率；
- **协议维度（10%）：**TLS/IPSec/国密 SSL 适配率、混合证书链部署率、握手优化达标率；
- **管控维度（15%）：**统一密钥管理覆盖率、算法热插拔能力、密钥审计完整率、权限管控合规率；
- **合规维度（10%）：**密码法/商密条例合规率、关基合规达标率、等保合规达标率；
- **运维维度（5%）：**运维自动化率、故障恢复效率、安全监控覆盖率、应急响应处置率；
- **成效维度（5%）：**性能损耗达标率、业务中断率、安全事件发生率、用户体验满意度。

表：抗量子就绪度（PQR）指标体系权重与分级

一级维度	权重	核心二级指标	就绪度分级判定标准
资产维度	20%	密码资产覆盖率、高脆弱算法清除率、资产图谱完整度、资产风险分级准确率	90-100：全覆盖、高脆弱清零、图谱完整、分级精准 75-89：≥80%覆盖、高脆弱清除≥80%、图谱较完整、分级较准 60-74：≥60%覆盖、高脆弱清除≥50%、图谱基本完整、分级合理 40-59：≥40%覆盖、高脆弱清除≥30%、图谱部分缺失、分级粗略 0-39：＜40%覆盖、高脆弱清除＜30%、图谱缺失、无分级
算法维度	20%	PQC 覆盖率、国密合规率、算法兼容性达标率、算法性能达标率	90-100：PQC 全覆盖、国密 100%合规、兼容/性能全达标 75-89：PQC≥80%、国密≥90%合规、兼容/性能≥80%达标 60-74：PQC≥60%、国密≥75%合规、兼容/性能≥60%达标 40-59：PQC≥40%、国密≥50%合规、兼容/性能≥40%达标 0-39：PQC＜40%、国密＜50%合规、兼容/性能＜40%达标
密钥维度	15%	密钥熵源安全率、密钥轮换及时率、密钥泄露风险率、多源密钥协同调度率	90-100：熵源 100%安全、轮换 100%及时、零泄露风险、调度全协同 75-89：熵源≥80%安全、轮换≥80%及时、低风险、调度≥80%协同 60-74：熵源≥60%安全、轮换≥60%及时、中风险、调度≥60%协同 40-59：熵源≥40%安全、轮换≥40%及时、较高风险、调度≥40%协同 0-39：熵源＜40%安全、轮换＜40%及时、高风险、调度＜40%协同
协议维度	10%	TLS/IPsec/ 国密 SSL 适配率、混合证书链部署率、握手优化达标率	90-100：全适配、全部署、优化全达标 75-89：≥80%适配、≥80%部署、优化≥80%达标 60-74：≥60%适配、≥60%部署、优化≥60%达标 40-59：≥40%适配、≥40%部署、优化≥40%达标 0-39：＜40%适配、＜40%部署、优化＜40%达标
管控维度	15%	统一密钥管理覆盖率、算法热插拔能力、密钥审计完整率、权限管控合规率	90-100：全覆盖、全支持、审计完整、100%合规 75-89：≥80%覆盖、支持、审计较完整、≥80%合规 60-74：≥60%覆盖、基本支持、审计基本完整、≥60%合规 40-59：≥40%覆盖、部分支持、审计部分缺失、≥40%合规 0-39：＜40%覆盖、不支持、审计缺失、＜40%合规
合规维度	10%	密码法 / 商密条例合规率、关基合规达标率、等保合规达标率	90-100：100%合规、全达标、全达标 75-89：≥90%合规、≥90%达标、≥90%达标 60-74：≥75%合规、≥75%达标、≥75%达标 40-59：≥50%合规、≥50%达标、≥50%达标 0-39：＜50%合规、＜50%达标、＜50%达标
运维维度	5%	运维自动化率、故障恢复效率、安全监控覆盖率、应急响应处置率	90-100：全自动化、高效、全覆盖、全达标 75-89：≥80%自动化、较高效、≥80%覆盖、≥80%达标 60-74：≥60%自动化、基本高效、≥60%覆盖、≥60%达标 40-59：≥40%自动化、一般、≥40%覆盖、≥40%达标 0-39：＜40%自动化、低效、＜40%覆盖、＜40%达标
成效维度	5%	性能损耗达标率、业务中断率、安全事件发生率、用户体验满意度	90-100：损耗全达标、零中断、零事件、高满意 75-89：≥80%达标、低中断、低事件、较满意 60-74：≥60%达标、偶发中断、偶发事件、基本满意 40-59：≥40%达标、较多中断、较多事件、一般 0-39：＜40%达标、频繁中断、频发事件、不满意

（二）阶梯式成熟度模型

本研究基于迁移周期规律与行业阶段特征，提出五级阶梯式成熟度模型，由此刻画从基础摸底到持续演进的完整迁移路径：

- **一级：资产摸底期**——完成密码资产全面盘点、依赖图谱构建、量子脆弱性评估、迁移优先级排序，摸清家底、识别风险；
- **二级：试点验证期**——完成核心场景试点部署、算法适配验证、性能测试优化、混合架构可行性验证，验证方案、积累经验；
- **三级：全面替代期**——高脆弱算法清零、PQC 规模化部署、密钥体系全面升级、协议栈兼容改造，全域覆盖、消除风险；
- **四级：管控融合期**——统一密钥管理中枢建成、算法热插拔常态化、多源密钥协同调度、合规审计常态化，体系成型、管控闭环；
- **五级：持续演进期**——安全能力常态化迭代、标准动态适配、性能持续优化、风险闭环管控、形成长效机制，能力成熟、持续领先。

（三）成效判定原则

- **分层达标：**不同场景设置差异化达标线（如极高安全场景≥90、通用场景≥75、边缘场景≥60），避免一刀切；
- **动态迭代：**就绪度与成熟度随标准更新、技术演进、风险变化持续调整，保持评估时效性；
- **可落地、可验收、可追溯：**指标可量化、数据可采集、过程可追溯、结果可复核，杜绝主观判定；
- **安全与业务平衡：**优先保障安全底线，兼顾业务性能、稳定性与成本，实现安全、业务、成本的最优平衡。

2.4 重点行业抗量子安全迁移实施与全域行动建议

如前文所述，我国已在抗量子安全建设领域形成“国密打底、QKD 做后盾、PQC 加速跑、QRNG 补位”的多元落地路径。本章前述小节已提出覆盖全流程的完整设计体系，包含从前期资产盘点、摸排评估、算法工程适配、物理层技术融合、全域密钥统筹管控，到分层场景落地、就绪度成效评判各环节，在此基础上，不同行业还应结合自身业务架构、安全防护等级、网络运行模式、监管约束要求以及业务承载规模，开展差异化落地实施。

为此，本研究聚焦政务、金融、能源电力、通信运营商四大重点行业，结合各类业务运行特征完成方案裁剪、优先级调整与实施节奏适配，形成兼具统一建设设计与行业差异化特征的落地实施建议。同时梳理全行业通用实施流程、共性工程痛点解决路径、分级业务风控兜底机制，搭建适配行业特性的成效评价体系，并面向产业链各类参与主体提出协同发展建议，推动抗量子安全建设从顶层规划设计全面转向行业实地落地执行。

2.4.1 分行业业务分层选型决策建议

针对极高安全防护、通用高并发运行、边缘物联网轻量化三类基础场景，依据业务涉密等级、数据流转属性、运行实时性、业务连续性要求调整技术方案侧重方向，从部署场景、技术侧重、防护强度三个维度凸显行业选型的核心差异。

（一）政务领域选型适配

政务领域应整体遵循涉密优先、纵向贯通、合规前置的核心建设原则，严格按照内网涉密等级划分差异化建设方案。例如：

- 党政涉密内网、跨层级机要数据交换链路、涉密公文传输系统等高等级业务场景，应全面采用“QKD 主导+PQC 应急+零信任融合”的极高安全建设模式，从物理密钥分发、数据加密传输到全域访问权限管控搭建全维度信息安全闭环，以便契合党政机要信息最高等级防护与涉密合规管理要求。
- 政务外网、便民政务服务平台、线上办事大厅等面向社会公众的普惠服务类业务，应采用“PQC 全面替换+QRNG 熵源增强”的通用高并发建设思路，在筑牢抗量子安全底线的基础上，充分兼顾海量群众访问并发压力与政务平台日常运行流畅度。
- 基层政务感知采集终端、乡镇级边缘数据采集设备等末梢节点，应选用经过深度裁剪优化的轻量级 PQC 算法完成安全改造，以极低资源消耗适配基层终端算力弱、部署分散的现实条件。

（二）金融行业选型适配

金融行业应以资金交易绝对安全、全链路业务连续运行、金融监管全面达标为核心建设目标，依据交易层级、资金体量划分梯度化选型标准。例如：

- 央行跨行资金清算链路、商业银行核心账务系统、大额资金划转骨干网络等金融核心命脉业务，应全面落地最高等级多元协同落地路径，依托 QKD 实现骨干专网密钥安全分发，依靠 PQC 完成业务应用层加密应急兜底，从根源规避量子算法破解引发的资金交易窃取、篡改风险。
- 线上零售支付、互联网理财、普惠金融服务等面向大众的高频交互业务，应以全域标准化 PQC 算法迭代替换为核心改造方向，搭配 QRNG 优化全链路密钥生成机制，精准平衡交易加密安全等级与金融业务响应时

延。

- 银行线下自助设备、网点业务终端、社区便民金融终端等分散式终端设备，应统一部署轻量化抗量子安全加密模块，在严控终端改造成本的前提下，补齐金融末梢终端安全防护短板。

（三）能源电力行业选型适配

能源电力行业具备工控网与信息网物理隔离、野外设备部署范围广、工业系统运行周期久、生产业务零容错的显著行业特征，选型工作应严格区分生产控制类业务与办公信息化类业务。例如：

- 电网跨省调度主站、电力负荷控制专网、新能源并网核心控制链路等直接关系能源生产输送稳定的工控核心业务，应沿用极高安全防护架构，兼顾工业通信协议适配性与抗量子攻击能力，严防调度控制指令遭到窃取、篡改与劫持。
- 电力企业内部办公系统、客户用电营销服务平台、线上缴费服务系统等非生产信息化业务，应采用标准化 PQC 替换改造模式，快速完成 RSA、ECC 等高危脆弱密码算法清零。
- 配电台区智能传感器、野外电力监测终端、分布式能源采集设备等海量边缘终端，应全面推行绿色轻量化抗量子改造方案，深度适配野外场景低功耗、弱网络、无人值守、长周期稳定运行的特殊部署环境。

（四）通信运营商行业选型适配

通信行业具备全网覆盖范围广、用户并发体量庞大、云边协同架构普及度高、终端设备海量下沉的行业特点，技术选型重点应兼顾全网统一迭代性与不同层级网络节点适配性。例如：

- 全国骨干承载传输网、核心信令交互网络、全域云网协同调度平台等全网核心枢纽设施，应搭建高可用抗量子安全体系，保障国家基础通信骨干链路长期稳定、安全可控。
- 公众移动通信业务、家庭宽带网络服务、中小微企业通用政企专线等大众化通信服务业务，应严格按照行业统一技术标准完成全网 PQC 规模化迭代升级，依托成熟产业生态压缩全网整体改造周期与实施难度。
- 城市基站边缘计算节点、海量物联网接入模组、户外通信监测终端等末梢网络设施，应精简抗量子安全配置项，采用极简轻量化部署模式完成规模化批量改造，充分适配通信行业海量终端低成本、快落地的改造需求。

表：四类重点行业业务分层技术选型差异化对照

行业类型	极高安全核心业务方案	通用并发业务方案	边缘末梢终端方案	核心选型差异化侧重
政务领域	QKD 主导 + PQC 应急 + 零信任	PQC 全域替换 + QRNG 增强	轻量裁剪 PQC	涉密合规优先，纵向层级贯通防护
金融行业	PQC+QKD 双轨并行加密防护	标准 PQC 迭代 + 密钥优化	终端轻量化加密模块	交易时延严控，资金链路零中断
能源电力	PQC+QKD 双轨并行适配工	标准化 PQC 算法替换	低功耗绿色轻量 PQC	工控协议兼容，野外低耗长效

行业类型	极高安全核心业务方案	通用并发业务方案	边缘末梢终端方案	核心选型差异化侧重
	控高安全			运行
通信运营商	骨干网高可用采用 QKD 架构	全网统一 PQC 规模化升级	极简配置轻量化部署	全网统筹迭代，海量终端降本落地

2.4.2 分行业四阶段迁移实施建议

在明确各行业差异化技术选型方案的基础上，可制定全行业通用、逻辑连贯的标准化抗量子安全迁移实施流程，整体划分为“资产摸底盘点、场景试点验证、全域规模推广、安全体系固化”四个阶段。该流程保持顶层框架完全统一，仅结合不同行业的管理架构、业务运行模式、审批管理要求，差异化调整实施推进节奏、试点选取范围与优先改造顺序，最终实现通用流程标准化与行业落地灵活化的深度结合。

（一）**第一阶段为资产摸底盘点阶段：**各行业可沿用 2.2 确立的密码资产自动化梳理、脆弱性分级评估方法，完成全域密码资产台账建立、高危算法排查、业务安全等级划分与整体迁移优先级排序。其中：

- 政务领域须重点聚焦涉密网络专属加密资产，优先梳理机要业务改造清单；
- 金融行业须聚焦核心交易系统内置加密组件，精准锁定影响资金流转的关键密码应用点位；
- 能源行业须将排查重心放在工控系统嵌入式加密模块；
- 通信行业须以全网网络设备、通信链路加密配置为主要摸排对象。

（二）**第二阶段为场景试点验证阶段：**各行业可选取贴合自身业务属性的代表性场景开展小范围落地测试，完成算法适配调试、全维度性能压力测试与新旧业务系统兼容性校验。

- 金融行业可优先选取区域性分支银行小额高频交易场景开展试点；
- 政务领域可优先选取单一地市政务服务一体化平台作为试点载体；
- 能源行业可选取区域配电网调度体系完成试点试运行；
- 通信行业可选取局部地市城域网开展试点落地，在验证技术可行性的同时沉淀行业专属落地经验与运维方案。

（三）**第三阶段为全域规模推广阶段：**在试点运行稳定、各项性能与安全指标全部达标的前提下，依照前期划定的优先级分批、分片、分领域开展全域改造。

- 政务领域须遵循自上而下逐级下沉的推进节奏，从省级核心平台逐步延伸至基层服务节点；
- 金融行业须严格执行核心先行、外围后置原则，优先完成核心交易系统升级，再迭代优化各类外围服务渠道；
- 能源行业须严格划分生产控制区与信息办公区，优先保障生产调度领域安全升级；
- 通信行业须采用圈层式分批迭代模式，从核心城区骨干网络逐步向偏远末梢网络延伸覆盖。

（四）**第四阶段为安全体系固化阶段：**全面完成存量高危脆弱算法清零工作，搭建适配行业业务特征的常态化运维管理机制，将抗量子安全管控、密钥运维、算法迭代管理等要求，全面融入行业现有网络安全、数据

安全管理制度体系之中，完成从项目化专项改造向常态化安全运营的平稳过渡。

表：四类重点行业分四阶段实施举措对照

阶段	通用核心动作	政务领域	金融行业	能源电力行业	通信运营商行业
一、资产摸底盘点（优先级排序）	1. 密码资产全量测绘 2. 脆弱算法（RSA/ECC）定位 3. 按安全等级/影响范围排序	·重点：涉密内网、机要链路、公文传输系统 ·优先：涉密业务→外网服务→末梢终端 ·合规：同步对标等保/密评要求	·重点：核心账务、清算链路、大额交易系统 ·优先：资金链路→客户认证→外围渠道 ·合规：对接监管审计口径	·重点：调度主站、工控专网、PLC/RTU加密模块 ·优先：生产控制区→信息区→野外终端 ·合规：兼顾电力监控系统安全规范	·重点：骨干网、信令网、云网协同平台 ·优先：核心网→城域网→接入网/IoT 模组 ·合规：同步考虑网安与数据合规
二、场景试点验证（小范围落地）	1. 选典型场景做PQC/QKD 适配 2. 性能/兼容性/稳定性压测 3. 形成行业试点规范与回退预案	·试点：单一地市政务服务平台+涉密文传链路 ·重点：涉密环境零泄漏、跨层级互通 ·验收：合规优先、性能适度容忍	·试点：省级分行小额高频交易+网银/APP 认证 ·重点：交易时延、吞吐、账务一致性 ·验收：性能+安全双红线	·试点：区域配电网调度 + 变电站远动通信 ·重点：工控协议兼容、毫秒级控制不中断 ·验收：稳定性>性能	·试点：本地城域网+边缘基站/物联网接入 ·重点：大并发、低开销、海量终端兼容 ·验收：规模化适配+成本可控
三、全域规模推广（分批落地）	1. 按优先级分批次割接 2. 灰度/双轨运行、新旧算法并存 3. 全网监控、问题快速闭环	·节奏：自上而下（省→市→县→乡镇） ·路径：涉密网全替换→外网分批→末梢轻量改造 ·策略：强合规、强审批、慢推进、零风险	·节奏：核心先行、外围后置 ·路径：清算/核心账务→渠道→数据中心→终端 ·策略：双轨热备、交易零中断、快速回退	·节奏：生产优先、分区隔离 ·路径：调度/工控→发电/配电→营销/办公→野外终端 ·策略：物理隔离区独立推进、严控跨区影响	·节奏：圈层迭代、全网统筹 ·路径：骨干→城域→接入→IoT/边缘节点 ·策略：标准化批量部署、集中管控、成本最优
四、安全体系固化（常态化运营）	1. 脆弱算法清零、证书/密钥全生命周期管理 2. 运维流程嵌入现有体系 3. 建立持续监测、审计、迭代机制	·重点：涉密密钥管理、分级审批、痕迹可追溯 ·制度：融入保密管理、密码管理、等保制度	·重点：交易密钥隔离、灾难恢复、审计留痕 ·制度：纳入资金安全、运维审计、应急响应流程	·重点：工控密钥离线管理、设备远程安全运维 ·制度：嵌入电力监控系统安全运维规程	·重点：全网密钥统一管控、终端可信接入、异常监测 ·制度：纳入通信网安、数据安全、IoT 管理体系

2.4.3 针对共性工程化痛点的标准化统筹方案建议

针对前文提及的 PQC 落地四大核心工程痛点，即报文体积膨胀、算力资源消耗偏高、新旧架构协议兼容性不足、技术架构迭代灵活性偏弱，本节提出全行业通用的标准化优化解决范式：基础优化技术路径全行业统一，同时依据不同行业核心业务的运行指标阈值，划定差异化的优化优先级与管控标准，避免通用优化方案与行业

实际业务运行标准产生冲突。

（一）**针对 PQC 应用带来的报文膨胀问题：**各行业不应寄希望于对 PQC 公钥、密文和签名进行通用字节级压缩。通用治理措施应调整为：握手流程精简优化、会话恢复/PSK/会话 Ticket、证书链最小化、证书缓存、标准化证书压缩（仅针对可压缩的证书元数据和链路结构，不能承诺压缩高熵 PQC 字段）、MTU/分片/重传治理、混合算法组合数量控制以及终端证书解析能力验证。金融行业应把端到端时延、尾部时延和交易失败率作为首要指标；通信行业应关注大流量下的分片、重传和链路利用率；政务、能源行业应在合规完整性和业务连续性基础上进行稳健优化。

（二）**针对加密运算带来的算力损耗问题：**软件层面统一优化算法运行参数、精简冗余运算逻辑，硬件层面沿用 FPGA、ASIC 硬件加速搭配软硬协同卸载的成熟落地路径。例如：通信行业可依托庞大网络架构，侧重采用集群算力分摊模式平衡全网运算压力；金融行业可在核心交易节点集中部署高性能硬件加速设备，保障核心业务算力充足稳定；政务与能源行业可结合现有设备算力配置，灵活搭配软件轻量化优化与低成本硬件升级两种模式。

（三）**针对老旧系统、异构网络带来的协议兼容难题**：各行业可统一推行混合证书链部署、双算法自适应协商、模块化加密插件解耦三大兼容方案。例如：能源电力行业存量工业协议繁杂、系统迭代周期漫长，可将协议兼容性适配作为核心优化重点；政务领域可重点做好新旧政务业务系统跨版本算法兼容对接；金融、通信行业则可依托自身系统迭代能力，快速完成老旧通信协议、加密协议替换调试。

（四）**针对抗量子标准持续更新带来的架构迭代需求：**各行业可统一搭建抽象密码服务中间层，实现底层加密算法与上层业务应用完全解耦。如政务领域可紧跟国家密码政策与行业标准更新节奏，重点强化架构快速适配调整能力；其余行业则可依托解耦架构，平稳完成后续算法版本迭代、技术路线微调升级。

表：四大共性工程化痛点 vs.各行业优化侧重对照

痛点类别	通用解决方案	政务领域优化侧重	金融行业优化侧重	能源电力行业优化侧重	通信运营商行业优化侧重
报文膨胀（带宽占用↑）	1. 会话恢复/PSK/会话 Ticket 2. 证书链最小化与证书缓存 3. MTU/分片/重传治理 4. 仅采用标准允许的编码规整，禁止通用压缩神话	保障加密完整性与合规性，适度优化	首要优化：严控交易时延与报文体积	保障工控指令传输完整性，适度优化	批量压缩：骨干链路大流量数据压缩
算力损耗（CPU占用↑）	1.软件参数调优 2.硬件加速（FPGA/ASIC） 3. 软硬协同卸载	灵活搭配软件优化与低成本硬件升级	核心节点加速：高性能硬件保障交易算力	低功耗优先：适配野外设备，软件优化为主	集群分摊：全网算力负载均衡，降低单点压力
协议兼容（新旧	1.混合证书链	核心优化：新旧	快速替换老旧	首要优化：存量工	快速完成全网统一

痛点类别	通用解决方案	政务领域优化侧重	金融行业优化侧重	能源电力行业优化侧重	通信运营商行业优化侧重
系统不通）	2.双算法协商 3. 模块化插件解耦	政务系统跨版本兼容对接	协议，保障交易连续性	业协议适配与改造	协议升级与兼容调试
架构迭代（标准更新快）	1.抽象密码服务层（CaaS） 2.算法热插拔 3. 双标自适应路由	重点强化：快速适配政策与标准更新	平稳完成算法版本迭代与技术路线微调	保障工控系统长期稳定，避免频繁迭代	依托解耦架构，平滑完成全网技术升级

2.4.4 针对业务平稳迁移风控的分级适配型兜底策略建议

为全面保障抗量子安全改造全过程不干扰原有核心业务正常运转，坚守行业业务运行底线，全行业需统一确立“业务运行不中断、改造方案可回退、全链路运行可观测”三大核心风控总原则，同时结合 2.3 章节划分的三类应用安全场景，匹配分级分类的差异化兜底防护策略，按照业务安全等级配置对应强度的风险防控与应急保障手段。

（一）**面向涉密政务骨干链路、金融核心交易专网、电网调度控制专网等高等级核心业务：**可部署双加密链路热备份兜底架构，搭载策略化可回退切换机制。日常业务可优先运行经验证的新型抗量子加密体系；一旦出现运行异常、兼容故障、密钥池水位不足、性能波动或解析错误，应按照预案切换至存量合规安全链路或备用抗量子链路。切换前应经过影子测试、灰度验证和回退演练，不能预设为“无感瞬时切换”；同时搭建全域实时监测体系，对加密运行状态、密钥水位、数据传输状态、业务响应状态实行 7×24 小时动态观测，实现风险早发现、早处置。

（二）**面向政务外网公共服务、大众线上金融支付、运营商公众民用网络等中等级通用业务：**可采用灰度流量分批切分的渐进式改造模式，逐步将业务流量平稳迁移至新加密架构，配套完善全版本平滑回滚机制，若批量改造出现大面积适配问题，可按照业务批次有序回退至原有运行模式，依托系统运行日志、业务行为数据完成运行状态溯源分析与问题定位。

（三）**面向各类边缘感知终端、基层数据采集设备等低等级末梢业务：**可推行离线安全兜底运行机制，在网络中断、云端密钥调度服务异常等场景下，依靠终端本地缓存安全密钥完成基础加密防护工作，搭配极简轻量化运行状态监测模式，在严控终端改造成本的前提下，保障末梢设备基础安全运行能力。

表：四个重点行业风控兜底策略差异化对照

防护等级	通用兜底策略	政务领域	金融行业	能源电力行业	通信运营商行业
高等级核心业务（双链路热备）	双加密链路热备份；策略化可回退切换；影子测试/灰度验证；7×24小时全域实时监测；故障按预案切换	涉密专网双轨加密，严格涉密隔离；全程审计留痕，满足保密合规；禁止外网互通，物理隔离兜底	资金清算链路冗余备份；交易一致性校验；毫秒级切换，杜绝资金错乱；金融审计全程留痕	调度专网工控双链路；指令完整性校验；杜绝篡改劫持；工控故障自锁、防止误操作	骨干承载网、信令网双链路冗余；保障通信无中断；全网流量实时监控、异常流量阻断
中等级通用业务（灰度渐进改造）	灰度流量分批切分；批次化版本回退；日志溯源观测；小范围风险隔离	政务外网分批灰度上线；公众服务业务柔性切换；以服务不中断为底线，严控访问异常	线上支付、理财业务流量灰度切分；交易批次隔离，故障批量回退；保障用户交易体验	电力营销、办公信息系统渐进改造；隔离办公区与生产区，避免风险传导	公众移动通信、宽带业务分批迭代；大流量平滑迁移，规避全网波动卡顿
低等级末梢业务（离线兜底运行）	本地密钥缓存；离线安全加密；极简状态监测；低成本容错运行	基层采集终端本地缓存密钥；断网情况下正常数据采集，保障基层数据不间断上报	线下自助终端本地密钥备份；断网可完成基础刷卡、查询等简易业务	野外电力传感器离线兜底；无人值守状态下自主加密、数据留存	基站边缘终端、物联网模组本地秘钥驻留；弱网环境保持基础通信加密能力
行业风控核心侧重	统一底线：不中断、可回退、可观测	合规优先、涉密可控、全程可追溯	交易稳定、资金安全、零账务差错	工控隔离、指令安全、生产零事故	全网通畅、海量兼容、波动最小化

2.4.5 针对多维落地成效评价的行业适配型细则建议

各行业迁移成效评价体系以 2.3.4 章节构建的抗量子就绪度（PQR）通用指标体系为核心基础，沿用安全防护能力、合规建设水平、业务运行性能、整体建设成本、长期运维能力五个核心评价维度，统一五级就绪度等级划分标准与综合评分规则，在此基础上结合四个重点行业的核心发展诉求与考核重点，差异化调整各维度权重占比，可形成通用框架统一、考核权重细分、行业标准适配的落地成效评判体系。

（一）**政务领域成效评价应大幅上调合规建设维度权重，**将党政密码管理条例落实情况、涉密网络安全管控达标情况作为核心考核依据，其次应侧重考核全域密码资产安全覆盖水平，适度放宽非核心业务性能损耗与整体建设成本考核标准，从而匹配政务建设合规为先的核心导向。

（二）**金融行业成效评价应重点抬高安全防护能力与业务运行性能两大维度权重，**核心考核资金交易链路安全等级、加密交易时延控制水平、全业务运行稳定率，严格约束改造后各类金融服务核心运行指标，全力保障金融交易业务平稳有序开展。

（三）**能源电力行业应侧重提升工控系统适配度与长期运维能力评价权重，**重点考核抗量子安全体系与现有工业控制系统的融合适配效果，以及野外分布式终端、偏远站点设备长期安全运维保障能力，贴合能源行业重稳定、长周期、少迭代的运行特征。

（四）**通信运营商行业应侧重优化全网规模化适配效果与整体建设成本维度权重，**重点考核全网统一改造兼容覆盖率、海量终端批量改造成本管控水平，兼顾全网整体性能损耗管控，适配通信行业全网统筹、批量落

地的改造特征。

各行业最终综合得分可沿用前文既定五级就绪度判定标准，同时结合行业专属权重测算得出结果后，从而判定行业整体抗量子安全建设成熟层级，作为后续体系优化升级、下一阶段建设规划编制的核心量化依据。

表：四类重点行业落地成效评价维度及权重示例差异化对照

评价维度	通用基础权重	政务领域（合规优先）	金融行业（安全优先）	能源电力（运维优先）	通信运营商（成本优先）
安全防护能力	20%	22%涉密链路安全、访问权限管控、防窃取篡改	30%资金链路防护、交易隔离、抗攻击能力	25%工控指令防护、内网隔离、终端安全加固	18%骨干网防护、异常流量拦截、接入可信校验
合规建设水平	20%	30%密评、等保、涉密管理、党政合规审查	20%金融监管、交易审计、资金留存规范	18%电力安防规范、工控安全合规备案	17%通信安全、数据安全行业合规要求
业务运行性能	20%	15%适度容忍时延，不苛求极致性能	25%严控交易时延、高吞吐、零抖动、低报错率	22%工业控制低延迟、指令传输稳定可靠	25%大并发承载、全网吞吐、带宽损耗可控
整体建设成本	20%	13%财政预算管控，成本容忍度较高	12%核心业务不计成本，严控改造成本浪费	15%分期投入，优先保障生产区域建设	25%海量终端批量降本，严控全网改造投入
长期运维能力	20%	20%层级化运维、全程审计、痕迹留存	13%自动化运维、交易日志留存、故障快速恢复	20%野外设备长效运维、低维护频率、离线管控	15%全网统一运维、批量监控、远程管控
行业评价核心导向	均衡综合评判	合规为王、涉密可控	资金安全、交易稳定	生产稳定、长效运维	规模化落地、成本最优

2.4.6 对产业链多方主体协同推进的行动建议

抗量子安全体系规模化落地是覆盖政策、技术、产品、应用、运维的系统性产业工程，无法依靠单一行业、单一市场主体独立完成，需要行业终端使用方、安全产业研发厂商、国家及行业标准组织三方主体各司其职、协同联动。本节结合前文梳理的行业落地痛点、技术演进趋势、现存建设短板，依托整体双轨发展路线，针对不同主体职能定位，提出精准务实、贴合产业实际的差异化行动推进建议。

（一）**从行业终端用户层面而言，**各级政企行业用户需率先完成内部安全认知升级，充分研判长期量子安全威胁带来的业务风险，结合自身现有网络架构、业务布局提前编制中长期分阶段迁移建设规划，杜绝盲目大规模跟风改造。高安全等级行业应优先完成核心业务安全加固与风险隔离，普通行业用户应优先完成存量高危密码资产排查清理，循序渐进推进分级改造；同时主动对接产业技术资源，立足自身行业业务痛点提出定制化建设需求，避免通用化产品与方案盲目落地。

（二）**从安全产业研发厂商层面而言，**市场研发企业需坚定立足国内自主可靠发展大局，紧扣“国密打底、QKD 做后盾、PQC 加速跑”的多元化发展思路，一方面持续迭代优化通用型 PQC 软硬件安全产品，全面提升产品高并发适配能力与长期运行稳定性；另一方面深耕政务、金融、能源、通信垂直细分赛道，针对性研发适

配金融低时延交易、能源工控协议兼容、政务涉密高防护、通信海量终端轻量化部署的定制化安全产品与一体化落地解决方案，同步强化老旧存量设备兼容适配技术研发，持续压降全行业整体迁移改造成本。

（三）**从各级标准组织层面而言**，需加快补齐国内自主后量子密码算法应用体系，加速推进金融、政务、能源、通信等分行业专项应用规范、落地实施细则编制发布，填补当前细分领域场景化应用标准空白。统筹协调国际通用 PQC 算法与国内自主后量子密码的融合应用规则，平衡自主技术推广与跨境业务算法兼容需求；统一报文优化、硬件加速、业务风险兜底等通用工程化改造技术规范，为全行业规范化、标准化、有序化开展抗量子安全迁移建设筑牢制度与标准根基。

综上所述，本章围绕顶层架构、实施框架、场景范式以及成效评估详细阐述了抗量子安全技术体系与双轨落地逻辑，明确我国“国密打底、QKD 做后盾、PQC 加速跑、QRNG 补位” 的多元落地实践路径，系统阐述资产盘点、脆弱性评估、算法工程化、物理层融合及统一管控五大实施环节；针对极高安全、通用高并发、边缘物联网三类场景，提出分层落地范式；并建立可量化的抗量子就绪度（PQR）指标与阶梯式成熟度模型。

在此基础上，本章还进一步细化到重点行业的实操层面，聚焦政务、金融、能源、通信四类重点行业，在统一技术架构与通用实施流程的基础上，结合行业业务特征、安全要求与运维条件制定差异化落地策略，从业务选型、阶段推进、工程优化、风险兜底、成效评价五个维度细化行业适配方案，并配套多类行业对照分析表明确差异化实施细则，同时面向用户、厂商、标准组织提出协同发展建议，整体提出了一套完整、连贯、可落地、可验收的抗量子安全迁移体系建议，为行业提供了可落地、可验收的迁移指引，支撑我国抗量子安全体系在各行业落地实践的平稳有序、高质量推进。

第三章 重点行业抗量子安全迁移与落地实践研究

随着量子威胁由远期风险演变为现实挑战，抗量子安全建设随之进入工程化落地关键期。国内各关键信息基础设施行业结合自身业务特性、安全基线与监管要求，正逐步探索出差异化迁移路径，形成各具特色的实践模式。本章聚焦金融、通信、能源、政务四类重点行业，围绕案例、工程难点、落地范式等开展系统性实践研究。

当前国内抗量子安全迁移呈现出清晰的行业节奏差异：金融行业因资金高敏感、交易高频化及强监管约束，先行先试、率先形成标杆实践；通信运营商依托全网规模优势，聚焦量子城域网、5G 安全底座推进规模化改造；能源行业立足工控核心命脉，坚守生产零中断底线，坚持稳健稳妥推进；政务领域以分级合规为首要前提，采取审慎渐进、分级落地策略，筑牢民生与治理安全根基。

同时，四类重点行业的场景需求也各有侧重：金融行业聚焦交易连续性，以极致低时延、高吞吐量为刚性约束；通信行业面向海量终端与全网流量，重点攻克高并发承载、规模化兼容难题；能源行业保障工控稳定运行，强调确定性时延、长周期运行可靠性；政务领域锚定合规底线，突出分级管控、全程可审计要求。

本章将通过复盘头部机构典型项目，拆解一线工程痛点与适配方案，提炼可复制的行业落地范式，旨在验证理论框架的可行性，总结行业共性规律与差异化经验，为后续跨行业推广、标准细化与生态完善提供实证依据，支撑我国抗量子安全体系从顶层设计走向全面落地。

3.1 金融行业：高并发交易驱动下的标杆实践

金融行业作为国家关键信息基础设施的核心组成，其交易链路、资金清算、客户数据与身份认证体系高度依赖公钥密码技术，是量子威胁暴露面最广、安全影响最直接、迁移紧迫性最高的领域。伴随 NIST PQC 标准落地、国内算法征集启动及监管合规持续强化，金融行业率先进入抗量子安全迁移先行试点与规模化验证阶段，形成具有行业标杆价值的实践模式。

3.1.1 行业迁移约束：金融监管、交易 SLA 与高敏感数据防护

金融行业抗量子安全迁移受强监管、高 SLA、高敏感数据三重刚性约束叠加，构成区别于其他行业的核心迁移边界。

（一）**在监管合规层面：**金融行业密码应用体系严格遵循《密码法》《金融数据安全 数据安全分级指南》及商用密码应用安全性评估（密评）等规范，跨境支付、资金清算、客户身份认证等核心场景已明确纳入量子安全合规审查范围。监管要求迁移过程不降低原有安全等级、不中断业务连续性、不新增系统性风险，合规审查覆盖算法选型、协议改造、证书体系、密钥管理、审计追溯全链路。

（二）**在交易连续性层面：**金融核心系统普遍要求毫秒级响应、7×24 小时不间断运行、零账务差错的严苛 SLA。支付清算、跨行结算、证券交易、手机银行等高频场景日交易峰值可达数十万笔/秒，任何因算法替换、协议变更、密钥更新导致的时延增加、吞吐下降或业务中断，都将直接影响资金安全与市场稳定，构成迁移不可逾越的刚性底线。

（三）**在数据安全层面：**金融行业集中存储与传输资金账户、交易记录、客户身份、征信数据、跨境清算指令等高敏感信息，数据保密周期长达 20–50 年，面临“先采集、后破解”（HNDL）长期潜伏式量子攻击风险。一旦传统密码体系被量子计算攻破，将引发数据泄露、交易伪造、资金挪用等系统性金融风险，因此迁移必须兼顾当前安全与长期量子韧性双重目标。

表：金融行业抗量子安全迁移核心约束对照

约束维度	核心要求	具体表现	迁移刚性影响
监管合规约束	密码法、密评、金融数据分级合规全覆盖	算法选型、协议改造、密钥管理、审计追溯全链路审查	不可降安全、不可断业务、新增风险零容忍
交易 SLA 约束	毫秒级响应、7×24 小时、零差错	支付峰值数十万笔/秒、清算零中断、账务无差错	时延敏感、吞吐受限、灰度回退机制必建
高敏感数据约束	20–50 年长周期保密、HNDL 高风险	账户、征信、清算指令、交易记录长期留存	抗量子强度必须最高、数据全链路加密

3.1.2 核心业务场景解构：清算、账务、支付与跨境结算

金融行业密码应用高度集中于资金清算、核心账务、移动支付、跨境结算四大核心场景，各场景业务逻辑、密码依赖、性能敏感度与量子暴露面差异显著，构成差异化技术选型与迁移优先级的核心依据。

（一）核心清算与跨行结算场景

涵盖央行大额支付系统、商业银行跨行清算、证券登记结算、债券交易结算等关键基础设施，是金融体系的“大动脉”。核心密码应用包括交易报文签名、清算指令加密、对账数据验签、资金划转授权等，依赖高强度、高稳定性公钥算法。该场景交易规模大、影响范围广、安全等级最高，量子暴露面最集中，迁移优先级最高，对算法安全性、密钥一致性、交易原子性要求极强。

（二）核心账务系统场景

包括银行核心账务、客户账户管理、资产负债核算、交易记账与对账等后台核心系统，是资金安全的“数据中枢”。密码应用覆盖账户认证、交易验签、敏感字段加密、批量对账数据完整性保护，对算法稳定性、数据一致性、长期保密性要求极高，属于高价值、长周期量子威胁重点防护对象。

（三）移动支付与线上交易场景

涵盖手机银行、网上银行、第三方支付、证券交易 APP 等高并发用户端场景，是金融行业最大规模的公钥应用场景。密码应用集中于用户身份认证、TLS 握手加密、交易签名、敏感参数保护，具有并发量极大、终端类型多样、时延敏感、兼容性要求高等特征，需重点平衡安全强度、响应速度与终端适配能力。

（四）跨境结算与跨境支付场景

包括 SWIFT 报文、跨境清算、外汇交易、跨境资金划转等跨境金融链路，涉及境内外多机构、多协议、多证书体系互联。密码应用涵盖跨境报文签名、跨境密钥协商、跨机构身份互认，需兼顾国内国密合规与国际 PQC

标准兼容，面临算法互操作、证书跨域、跨境审计等特有挑战，迁移复杂度最高。

表：金融行业核心业务场景密码应用特征对照

业务场景	核心密码应用	性能敏感度	量子暴露面	迁移优先级
核心清算/跨行结算	报文签名、清算指令加密、对账验签	极高（毫秒级）	最高	★★★★★
核心账务系统	账户认证、交易验签、敏感字段加密	高	高	★★★★
移动支付/线上交易	TLS 握手、身份认证、交易签名	极高	中高	★★★
跨境结算/支付	SWIFT 签名、跨境密钥协商、跨域认证	中高	高	★★★

3.1.3 头部金融机构典型案例复盘

金融行业作为量子威胁暴露面最广、安全影响最直接、迁移紧迫性最高的领域，叠加监管合规刚性、交易连续性极致要求、高敏感数据长期保密三重约束，已率先进入工程化验证与规模化落地阶段。本节选取金融行业权威媒体《金融电子化》中银行和证券领域的代表性头部机构实践，从背景动因、核心诉求、工程难点、改造路径、实测成效、行业经验等进行全链路复盘，由此形成可复用、可复制、可验证的金融行业迁移实证范式。

（一）大型国有银行：国密+PQC+QKD 混合架构与敏捷迁移实践

(1) 交通银行布局 QKD 与 PQC 双轨并行实践

- **方案概述：**交通银行积极响应国家战略部署，将量子技术纳入数字金融行动方案，坚持“场景落地”“技术突破”双轮驱动。在量子安全通信领域，开展量子密钥分发应用试点，构建异地数据中心间的量子保密通信网络，提升跨地域、跨管理域的数据传输安全性，进而加固总分行间 5G 链路的安全防护体系。在抗量子攻击领域，持续追踪国内外后量子密码标准制定进程，夯实后量子密码（PQC）算法技术储备，开展 PQC 非对称密码算法的研究试用。
- **QKD 方案的建设周期及成果：**
  - ✧ 2024 年在充分调研的基础上，确定 QKD 网络的两大核心应用场景，即总行数据中心间的数据加密传输和总分行 5G 链路的安全加固，优先推进“两地三中心”QKD 网络的可行性论证和规划。
  - ✧ 2025 年上半年，完成 QKD 网络的建设方案制定及实验室环境的技术验证；10 月至 11 月，完成上海至武汉的异地数据中心间 QKD 网络建设，提供跨地域的高安全加密传输能力；12 月，完成上海至合肥的量子加密网络建设，为试点分行提供 5G 链路的高安全防护。
  - ✧ 通过整合国家量子骨干网资源及配套软硬件，交通银行成功构建了具备三大核心能力的量子保密通信网络体系：首先，提供“两地三中心”QKD 网络。基于 QKD 基础设施覆盖总行各数据中心，可为关

键业务数据的跨域传输提供端到端高安全加密能力。其次，提供总分行间 5G 链路量子加密网络。利用总行至分行的安全专线实现量子密钥的动态注入，创新融合 5G 技术与量子加密技术，打通总分行间的高安全加密无线传输通道。第三，提供统一量子密钥管理平台。实现跨不同应用场景的量子密钥全生命周期集中管控，构建全行统一的量子密钥分发平台，核心设备实现 100%自主可靠，密钥分发效率从 200 毫秒级大幅优化至 20 毫秒级，在保障安全的同时实现了成本节约与运营效率的双提升。

- **QKD 方案的挑战：**
  - ✧ 一是信道损耗与距离限制，量子信号在光纤传输和传统中继过程中显著衰减，制约长距离传输应用，难以满足广域骨干网的覆盖需求；
  - ✧ 二是量子源质量和器件性能限制，导致密钥生成速率（成码率）低，商用系统的成码率通常仅为 kbps 级别，难以满足高速通信的业务需求。
- **PQC 的建设周期及成果：**
  - ✧ 交通银行在 QKD 网络的支持下，已在测试环境试点使用 PQC 与 SM4 的混合加密方案，通过统一的密钥管理平台，整合量子密钥与传统密钥的运维流程，有效降低多系统并行的成本，同时支持密钥池容量弹性扩展，满足业务增长的需求。
  - ✧ 此外，交通银行与网联清算公司共同开展 PQC“两把锁”方案验证。双方聚焦非实时对账文件的数字信封场景，通过测试环境联调来完整验证算法兼容性与流程可行性。具体采用抗量子签名算法（ML-DSA，基于格的数字签名算法）完成签名、验签操作，采用抗量子密钥封装算法（ML-KEM，基于格的密钥封装机制）完成密钥交换，与国密算法（SM4-CBC）混合部署，成功覆盖证书申请、数字签名、数字信封等密码应用核心环节。
- **PQC 路径的挑战：**
  - ✧ 首先，资源消耗增长——公钥、私钥及数字签名长度的增加，要求相应扩充密钥存储空间与报文字段容量，进而扩大加解密和签名验签的内存开销及传输环节的网络带宽需求。
  - ✧ 其次，性能表现分化——ML-KEM 在密钥封装环节的效率较优，但 ML-DSA 的签名生成与验签效率却明显低于 SM2 算法。系统迁移前相关算法的性能瓶颈需要重点突破，尤其在处理高频、低延时交易场景时需针对性优化架构设计。
- **未来展望：**着力扩大量子保密通信网络覆盖范围，推广分行通过 5G 链路的量子加密传输应用，探索延伸至境外分支机构专线链路量子加密传输；开展 PQC 算法的验证与迁移，按场景的安全威胁级别和迁移复杂度制定密码迁移规划。

参考资料

2025 年 10 月，《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》将量子科技列为六大未来产业之首，推动成为新的经济增长点，明确提出“探索多元技术路线、典型应用场景、可行商业模式、市场监管规则”的系统性要求。这一顶层设计，标志着量子科技在构建安全、高效、绿色、智能的新型金融基础设施，支持数字金融高质量发展中具有广阔应用前景。

量子技术为金融基础设施破局增效开辟新的路径。量子技术既是锋利的“矛”，又是坚固的“盾”，在攻防两端都对金融基础设

施的演进带来深远影响。一方面，量子保密通信和后量子密码，为抵御量子算法对传统金融密码体系的攻击破解提供了新的“安全防护墙”。另一方面，量子算法在金融投资组合优化、资产定价、风控建模等场景中展现出巨大的计算加速潜力，突破了传统金融基础设施的“算力天花板”。量子技术对金融基础设施的作用将从局部“加固加速”转向整体“融合重塑”，未来的金融基础设施有望演进为“量子-经典”混合智能体，在安全等级、计算范式、能效标准等方面实现跨越式提升。

(2) 中国邮政储蓄银行密码敏捷迁移实践

- **方案核心与目标：**邮储银行在开展量子密钥分发和后量子密码算法技术融合研究中，尝试构建浏览器-TLS 协议-业务系统全链路试点方案，以验证密钥敏捷迁移技术的可行性。方案以算法扩展和混合加密为核心，确保协议兼容性并通过双重密钥机制抵御量子威胁，为敏捷迁移提供可复用示范案例。
- **各环节具体设计：**
  - ✧ 浏览器为自主研发，采用密钥封装机制混合抗量子密钥协议的方式，通过公钥加密实现量子安全的密钥协商。
  - ✧ TLS 协议层将后量子密码算法伪装为“新椭圆曲线”，复用 TLS 原有框架，并通过组合设计模式实现混合密钥交换。
  - ✧ CA 体系设计复合证书或非复合证书两种模式，通过扩展字段或连接存储算法信息，平衡兼容性与存储开销。
  - ✧ 业务系统通过对密码服务中心接口抽象化、密码运算单元引擎化、密码服务配置模板化改造，支持多密码算法栈并行运行与智能切换。
- **面临的挑战：**
  - ✧ 后量子密码算法复杂度与系统开销高：存储压力增大，后量子密码算法数字证书存储空间由现有的不超过 2kb（SM2 算法）增长到最高 50kb(SPHINCS+算法），混合算法数据量更大；性能瓶颈，数据量变大导致运算中解析操作（如证书序列化）需优化；传输负载加大，网络开销随数据膨胀需优化。
  - ✧ 银行客户端生态改造复杂：银行业务涉及大量客户端终端，数量庞大、生态复杂，算法与协议更新需兼容老版本，终端改造难度大，无法短时间内全面更新，迁移复杂度高。
  - ✧ 基础设施敏捷性支持不足：银行现有密码设备普遍不支持新算法，硬件密码模块需升级；专用中间件扩展性差，难以快速适配敏捷密码需求，限制整体方案落地。
- **相关建议：**
  - ✧ 分阶段推进迁移：优先在外联系统、低频交易系统部署后量子密码进行试点，并逐步迁移至核心系统。
  - ✧ 提升密码服务中台敏捷能力：构建以策略控制、算法热插拔、密钥统一管理为核心的“密码即服务”平台，为未来算法演化提供基础支撑。
  - ✧ 联合生态伙伴共同推进：与软硬件厂商合作，推动密码安全厂商、TLS 协议栈、CA 机构支持后量子密码算法，实现上下游协同敏捷创新。
  - ✧ 建议单独设置“终端生态迁移子项目”：建立终端型号、固件版本、安全芯片/HSM 能力、证书链支持能力、远程升级能力、内存与功耗约束清单；将“可软件升级、需现场升级、需硬件更换、需长期

隔离兼容”四类终端分批纳入预算和工期；对无法升级的终端设置交易限额、网络隔离、网关代理转换、到期退役和风险接受审批机制。

- **成果总结：**本案例从银行信息系统对后量子密码迁移的迫切需求出发，提出了面向银行应用的敏捷迁移策略，以及密码算法敏捷设计、协议敏捷迁移、应用无感热迁移等多种关键支撑技术，确保系统具备一键无感知切换能力，有效控制迁移风险与业务影响。
- **实践意义与展望：**尽管当前后量子密码算法在性能与生态方面仍有挑战，但通过合理的架构设计和迁移策略，银行可以实现平滑、可控、渐进的迁移过程，为未来构建量子安全金融基础设施打下坚实基础。

参考资料

密码迁移要全面考虑算法安全性、算法性能、实施的便利性、合规性等多种因素，是一项极为复杂的长期系统性工程，需要耗费相当长的时间。以往密码安全体系的迁移工作历时往往达到 10 年以上，相比之下，后量子密码的过渡更为复杂，周期可能更长。密码体系的安全是保障银行信息安全的基础，尽快开展银行后量子密码迁移技术研究势在必行。迁移过程中要求银行 IT 系统能快速敏捷地适应新的加密标准，在调整加密措施后仍保持对其他系统的稳定性，尽量避免对基础设施进行大规模更改。

根据 NIST 的后量子密码迁移白皮书，后量子密码迁移包括两个阶段：前期准备和迁移实施。前期准备通常包括密码相关资产的盘点与迁移计划的制定。迁移实施则是结合迁移清单和迁移方案具体执行。按照分层设计思路，敏捷迁移可分为三步开展。

首先，构建敏捷密码服务层，通过抽象化密码算法接口、统一调用标准以及插件化设计，实现对传统密码算法与后量子密码算法接口的并行支持。通过算法策略管理，控制密码算法配置，可无缝切换并兼容经典算法和后量子密码算法。这样系统能够在现有服务不变的前提下，引入后量子密码算法进行沙箱验证，为后续敏捷切换打下基础。

其次是关键协议的敏捷切换支持，通过改造 TLS/HTTPS 等通信协议，使其兼容商密系列与后量子密码算法，尤其是引入支持双签名机制的中间件架构。同时，数字证书格式的扩展与兼容性处理也尤为关键，在不中断服务的情况下实现新旧算法的交替运行。

最后实现业务无感热迁移，在此阶段，通过引入代理层或中间件组件，配合灰度发布与服务热更新能力，系统可实现业务“一键无感”切换，达到不中断服务的热迁移能力。

（二）头部证券机构：交易链路与数据存储全链路抗量子安全实践

- **案例单位：国泰海通证券**
- **背景概述：**证券业关基系统复杂，业务连续性强、性能要求高，存在后量子密码算法选择困难，系统中易受量子计算攻击的密码算法位置识别不易，系统内密码迁移优先级风险评估标准不确定、应用部署及推广难度大等问题。
- **核心诉求：**当前，国泰海通证券交易系统客户端通过 SDK 与安全认证网关建立 SSL-VPN 加密通道，交易数据经网关路由至集中交易系统后安全落库存储，系统采用 CPU 内部的可信密码模块，为上层的密码应用提供基于商密的密码计算和密钥存储功能。而量子计算对现有依赖商密算法建立的网络传输层单向、双向通信通道，以及数据库中的用户敏感数据造成的威胁正逐步加剧。从安全性角度出发，优先聚焦于网络传输和数据存储模块的安全增强。
- **实施策略：**因后量子密码技术在国内仍处于标准制定和推广过渡期，尚无统一的国家标准发布，结合前期国泰海通证券在商用密码算法研究与应用方面积累的丰富经验，方案采用了后量子密码与商用密码结合的混合密码模式。在保障平稳过渡的基础上，加强证券行业网上交易系统互联网通信链路的安全防护，同时提升集中交易系统关键数据在数据库中的加密存储安全，实现用户交易数据从传输到存储的全链路抗量子

安全防护。

- **方案设计与实施：**在前期密码应用方案基础上，本方案使用后量子密码技术，升级安全认证网关为抗量子商密网关，重建数字证书系统，使其支持抗量子证书管理和下载功能，部署数据库加密服务，并使用后量子密码对密钥进行加密保护和存储。后量子密码迁移方案包括三方面设计：
  - ✧ 一是通信链路的安全加固。客户端到接入网关数据传输，通过使用“商密+后量子密码”相结合的方式，升级握手协议，对交易通道进行安全加固。
  - ✧ 二是数据库关键数据的加密存储。通过后量子密码算法保护加密密钥，从而对落盘的数据进行全密态加密，对本地数据进行安全加固。
  - ✧ 三是数字证书系统安全加固。提供支持后量子密码的数字证书系统，支持抗量子证书下载和管理功能，加强交易身份安全。
  - ✧ 算法选型：在后量子密码算法中，基于格的 Kyber 算法在性能、安全性以及认可度上相对更优，在软硬件实现方面展现出良好的应用前景。因此本方案中选用 Kyber 算法和商密算法结合的方式，对网上交易系统的通信链路和集中交易系统关键数据的加密存储进行安全加固实践。

- **方案成效：**
  - ✧ 有效应对量子计算攻击威胁；
  - ✧ 安全加固覆盖交易链路全流程，包括网络通信、数据存储、用户身份认证三个维度；
  - ✧ 可实现后量子密码平稳迁移，主要利用基于密码芯片商密应用方案提供的高性能、易使用优势，弥补新算法应用初期存在的性能短板；
  - ✧ 新算法满足证券交易对对低延迟、高并发以及快速响应的业务要求和性能需求。

- **未来展望：**
  - ✧ 一方面，深入钻研后量子密码在 CPU 内部实现原理，利用信创 CPU 芯片提升后量子密码计算速度，从而提高整体密码服务性能；
  - ✧ 另一方面，继续推进后量子密码在集中交易系统数据库加密场景的实施与落地，加大对数据库透明加密方案的研究，将数据库自身加密引擎和 CPU 芯片内部的加密技术结合，实现应用层免改造且时延低的加密方案。

3.1.4 金融行业案例实践特征及启示

综合上述交通银行、邮储银行、国泰海通证券头部金融机构的抗量子安全迁移实践，可清晰梳理出当前金融行业在量子安全建设中的共性特征、差异化路径及核心启示，为行业规模化推广提供可借鉴的实践规律。

表：金融行业抗量子安全实践共性与差异化特征对比

对比维度	共性特征	差异化特征
技术路线	均采用“国密+PQC”混合架构，兼顾合规、量子安全与兼容性	国有银行：叠加 QKD，构建“国密+PQC+QKD”全栈架构； 证券/股份制银行：侧重“国密+PQC”轻量化方案
迁移策略	均遵循分阶段试点、双轨并行、灰度推进、熔断回退原则，保障零中断	国有银行：先跨域/跨境高敏感场景； 证券机构：优先高频交易/在线接入场景； 股份制银行：优先移动端/外联场景
场景导向	均聚焦交易、数据、身份三大核心安全域	国有银行：侧重长周期、高敏感、跨域传输场景； 证券机构：侧重低时延、高并发交易场景； 股份制银行：侧重移动端高频接入场景
工程挑战	均面临算法开销、终端异构、存量设备适配、标准适配四大挑战	国有银行：重点攻克长距离链路衰减、跨域密钥同步； 证券机构：重点优化握手时延、CPU/并发性能； 股份制银行：重点解决终端兼容、灰度适配

（一）行业实践共性特征

(1) **一是坚持国密、PQC、QKD 的多元融合技术路线。**国有银行、股份制银行、证券机构均以国密算法为存量兼容基础，以 PQC 应对算法层量子威胁，高安全链路叠加 QKD 物理防护，形成“算法安全+物理安全+兼容安全”三位一体防护模式，实现合规、安全、性能的综合平衡。

(2) **二是采用分阶段试点、灰度推进、双轨并行、异常回退的平滑迁移策略。**所有机构均避免一刀切式改造，优先在外联、低频、非核心场景开展试点验证，再逐步向核心系统延伸；通过双栈并行、流量染色、灰度推送、熔断回退等机制，确保业务零中断、用户无感知，有效控制迁移风险。

(3) **三是突出场景驱动、性能优先、安全适配的工程化导向。**银行业、证券业均根据业务安全等级、并发压力、时延要求选择适配技术方案，高安全长周期场景强化量子防护，高频并发场景优先优化性能，所有改造均以业务连续性为底线，避免安全升级影响用户体验。

(4) **四是普遍面临算法开销、终端生态、基础设施、标准适配四大共性工程挑战。**PQC 算法证书体积增大、运算与带宽开销上升；终端类型异构、碎片化严重；存量密码机、中间件不支持新算法；国内标准尚未完全定型，跨厂商互操作难度高，成为行业共同痛点。

（二）行业实践差异化特征

(1) **一是技术路线侧重不同。**大型国有银行依托基础设施优势，采用“国密+PQC+QKD”全栈混合架构，兼顾算法安全、物理安全与广域传输高可靠；股份制银行、证券机构聚焦高频交易与互联网接入场景，侧重“国密+PQC”轻量化混合方案，降低部署复杂度与性能损耗。

(2) **二是迁移优先级不同。**国有银行优先推进跨域数据中心、总分行专线、跨境清算等高敏感、长保密周期场景；证券机构优先升级网上交易、集中交易、电子签章等高并发、低时延场景；股份制银行侧重移动端、第

三方对接等外联高频场景，形成与业务风险、性能约束高度匹配的优先级策略。

(3) **三是工程攻坚重点不同。**国有银行重点攻克长距离链路衰减、跨域密钥同步、广域高可用切换等广域网络难题；证券机构重点优化握手耗时、CPU 占用、并发承载能力等高频交易瓶颈；股份制银行重点解决终端兼容、灰度推送、用户无感知迁移等前端适配问题。

（三）行业实践核心启示

(1) **一是混合架构是过渡期最优解。**国密、PQC、QKD 不存在单一最优路线，需结合场景安全等级、性能要求、成本约束灵活组合；混合模式兼顾国密合规、量子安全、性能平衡与平滑过渡，是当前阶段最可行、风险最低的迁移路径。

(2) **二是密码敏捷能力是迁移成功关键。**通过密码服务抽象层、协议扩展、复合证书、算法可插拔、灰度回退等设计，实现算法策略化切换、协议兼容适配、业务无感知升级，有效降低改造风险、缩短迁移周期，是大型存量系统平滑过渡的核心支撑。

(3) **三是场景分层分级是高效迁移前提。**高安全长周期场景优先采用“QKD+PQC”双保险；高频并发场景侧重轻量化 PQC 优化；边缘终端场景简化算法组合，实现安全、性能、成本的精准匹配，避免一刀切式资源浪费。

(4) **四是生态协同是规模化落地基础。**密码设备厂商、终端厂商、CA 机构、行业主管部门需协同推进算法适配、硬件升级、标准统一、互操作测试，破解终端碎片化、基础设施不兼容、标准未定型等共性难题，构建全链路、全生态量子安全支撑体系。

3.2 运营商：广域承载网与 5G 安全底座融合实践

运营商作为国家数字基础设施的核心承载主体，网络覆盖范围广、节点数量庞大、业务类型复杂，是抗量子安全防护的关键领域。其网络承载海量公众通信、政企专线、跨域数据交互等业务，长期运行、全网互联、高并发传输等特征突出，量子威胁影响范围广、传导链路长、系统性风险高。近年来，国内头部运营商率先启动量子安全网络建设与后量子密码迁移试点，形成规模化、体系化、可复制的广域网络安全升级模式。

3.2.1 行业迁移约束：网络规模、带宽承载与跨域互信要求

运营商网络规模庞大、拓扑复杂、设备异构、承载业务多元，叠加高并发承载、全网互联、跨域互信、7×24 小时稳定运行等刚性要求，形成区别于其他行业的多重迁移约束。

（一）**在网络规模约束方面，**骨干网、城域网、接入网层级多，网元数量达数十万级，涵盖路由器、交换机、基站、传输设备、安全网关等异构硬件，存量设备型号复杂、更新周期长，大规模升级改造成本高、周期长，需避免全网同步停机。

（二）**在带宽承载约束方面，**骨干网单链路带宽达 Tbps 级，城域网与 5G 核心网承载百万级并发连接，抗量子安全改造需避免引入过大带宽开销与传输时延，否则将影响公众上网、视频业务、政企专线体验，必须维持原有带宽利用率与转发效率。

（三）**在跨域互信约束方面，**运营商网络跨地域、跨省份、跨厂商互联，密钥协商、身份认证、路由协议依赖传统公钥体系，抗量子安全改造需保障跨省、跨运营商、跨设备的互操作性，不能打破现有全网信任链。

（四）**在稳定性约束方面，**公众通信、应急通信、政务专线、工业互联网等业务全年无中断，抗量子安全改造需采用旁路部署、双栈并行、灰度割接模式，确保网络转发、会话建立、信令交互全程无感知、无中断。

表：运营商行业抗量子安全迁移约束对照

约束维度	核心要求	具体表现	迁移刚性影响
网络规模约束	网元异构、数量庞大、更新周期长	骨干/城域网设备数十万级、型号复杂、升级成本高	无法全网同步改造，必须分域分批实施
带宽承载约束	Tbps 级带宽、百万级并发、低时延	骨干单链路高吞吐、5G 短包密集转发	PQC 报文膨胀易致带宽拥堵，需严格控时延
跨域互信约束	跨省/跨厂商全网互信、密钥统一	路由/认证依赖传统公钥，跨域信任	需国密 + PQC 双证书，保障全网互操作性

约束维度	核心要求	具体表现	迁移刚性影响
		链复杂	
稳定运行约束	7×24 小时、全网无中断、高可靠	公众/应急/政企业务全年不可停	必须旁路部署、双栈并行、灰度回退

3.2.2 核心场景解构：量子城域网、5G 安全底座与政企专线

运营商抗量子安全迁移聚焦广域承载、移动通信、政企服务三大核心业务域，重点覆盖量子城域网、5G 安全底座、边缘计算安全、政企专线、工业互联网接入五大高价值场景，各场景网络拓扑、流量特征、安全需求差异显著，迁移优先级与技术路线各有侧重。

（一）量子城域网

作为城市级骨干量子安全承载网，覆盖省会及重点城市核心节点，承载跨城数据互联、政务云互联、金融专线、能源调度数据等长距离、高安全传输业务，是运营商量子安全基础设施核心载体。核心安全需求为跨城链路量子加密、密钥动态分发、跨域互信，流量特征为长包、大带宽、低时延，迁移优先级最高。

（二）安全底座

涵盖 5G 核心网、边缘计算节点、基站、5G CPE 等，承载公众移动通信、工业互联网、车联网、远程医疗、高清视频等高并发、低时延业务，量子威胁暴露面最大。核心安全需求为基站-核心网信令加密、用户面数据抗量子防护、边缘节点轻量化认证，流量特征为短包、高并发、超低时延，需平衡安全与终端性能。

（三）政企专线

面向政府、金融、能源、工业企业提供专用加密传输通道，承载涉密数据、交易数据、生产指令等高敏感业务，安全等级最高。核心安全需求为端到端量子加密、设备可信接入、数据长期保密，流量特征为稳定带宽、长连接、低抖动，需兼顾国密合规与量子安全。

（四）边缘计算安全

覆盖城域边缘、园区边缘、基站边缘等计算节点，承载工业控制、视频监控、物联网数据等就近处理业务，终端数量多、算力有限。核心安全需求为轻量化后量子密码认证、数据加密、边缘-云端安全传输，需适配低功耗、弱网环境。

（五）工业互联网接入

对接工业企业内网，承载生产控制、设备监控、远程运维等业务，实时性、稳定性要求极高。核心安全需求为工业协议抗量子加固、设备可信接入、控制指令完整性保护，需兼容工业私有协议与存量设备。

表：运营商核心场景特征对照

核心场景	安全等级	流量特征	核心诉求	迁移优先级
量子城域网	最高	长包、大带宽、低时延	跨城量子加密、动态密钥、跨域互信	★★★★★
5G 安全底座	高	短包、高并发、超低时延	信令加密、轻量化认证、边缘防护	★★★★
政企专线	最高	稳定带宽、长连接、低抖动	端到端加密、数据长期保密、可信接入	★★★★
边缘计算安全	中高	小数据、弱网、低功耗	轻量化 PQC、边缘 - 云端安全传输	★★★
工业互联网接入	高	实时流、工业协议、高稳定	协议加固、指令完整性、设备可信	★★★

3.2.3 头部运营商典型案例复盘

运营商作为数字基础设施核心建设与运营主体，在量子安全领域布局早、投入大、覆盖广，已在量子城域网、政企专线、5G 安全底座等关键场景形成体系化落地成果。本节选取中国电信、中国移动两大头部运营商公开实践，从战略布局、体系建设、落地路径、现存挑战与未来方向等维度复盘，提炼运营商抗量子安全迁移的标杆范式与行业共识。

（一）中国电信：量子城域网与政企抗量子安全规模化实践

- **战略定位与方案概述：**中国电信将量子科技纳入集团核心战略，构建“量子基础设施+密码服务平台+行业应用”三位一体体系，以“QKD+PQC 融合”技术为核心，打造规模化量子城域网，面向政务、金融、能源等高安全需求行业，提供端到端量子安全传输服务，筑牢数字基础设施安全底座。合肥、上海、北京、广州等城市量子城域网已相继建成，重点城市间初步实现互联互通。量子安全基础设施，正成为中国电信打造“量子+”产业新动能的关键底座。
- **建设路径与核心进展：**坚持统筹规划、分步实施、规模覆盖原则推进网络建设。
  - ✧ 先期完成核心技术验证与试点落地，逐步扩展至全国重点城市，形成规模化量子基础设施布局。
  - ✧ 技术层面，创新构建融合 QKD 与 PQC 的分布式密码体系，实现量子物理安全与后量子算法安全双重防护，该成果已入选央企科技创新成果目录。
  - ✧ 依托 OTN 光网优势，推出量子加密专线，为跨域高敏感数据传输提供“超大容量、超低时延、超高安全”通道。
  - ✧ 推出“量子+通话”“量子+云网”“量子+平台”等一系列创新产品。目前，已有 20 多款“量子+”产品逐步走向市场，覆盖政务、政法、应急、金融、医疗、制造等十余个行业。
- **现存挑战：**
  - ✧ 一是量子信号传输物理限制，长距离传输存在信号衰减问题，成码能力受环境与设备约束，难以完全

匹配超高速骨干网的全域覆盖需求；

✧ 二是存量设备兼容适配难度大，现有光传输、路由设备与量子加密模块融合组网复杂度高，改造与运维成本偏高。

- **未来方向：**

持续扩大量子城域网覆盖广度，延伸至更多省会与重点城市；深化 QKD 与 PQC 技术融合，优化密钥分发与管理机制；面向金融、政务、能源等行业推出定制化量子安全解决方案，构建“量子+行业”融合生态。

参考资料

近日，山东海洋集团联合山东电信、中电信量子集团共同打造的全国首个内河船闸 OTN（光传送网）量子加密专线项目在京杭运河山东段船闸正式建成投运。该项目成功将量子加密技术应用于内河船闸运营管理的 OTN 专网，实现了该项技术的首次商业化应用，为京杭运河山东段沿线船闸关键数据传输构筑起“物理隔离+量子加密”的双重安全防线，标志着我国智慧水运基础设施安全建设迈入新的阶段。

山东水运作为山东省内河水运项目投融资与运营管理平台，承担京杭运河山东段八里湾、邓楼、长沟、嘉祥等 12 座船闸的运营管理工作。随着智慧船闸、远程调度、视频监控等数字化业务深度应用，船闸数据传输对网络安全性、可靠性、低时延提出严苛要求。为此，中国电信充分发挥网络与技术优势，为山东水运量身定制量子 OTN 专线升级方案，在保留 OTN 精品专线大带宽、低时延、高可靠特性的基础上，深度融合量子安全基础设施，实现安全能力跃升。

此次全国首个船闸量子 OTN 专线项目的成功落地，不仅全面提升山东内河船闸通信网络防窃听、抗攻击、保畅通核心能力，为京杭运河“黄金水道”数字化、智能化运营夯实安全根基，更形成可复制、可推广的内河航运量子安全标准化解决方案，为全国内河航运、水利枢纽等关键基础设施网络安全建设提供示范范本。

（二）中国移动：量子科技与抗量子安全落地实践

- **战略定位与方案概述：**中国移动锚定“打造国际一流量子通信技术能力、基础设施、产品应用，成为量子领域国家战略科技力量”这一核心目标，聚焦“融入国家大局、科研攻关、设施建设、打造产品、引领生态”五大主线，加速量子科技创新与产业创新深度融合，联合全球合作伙伴共同推动量子通信规模化应用。
- **建设路径与核心进展：**
  - ✧ 一是突破量子密钥“随用充注”、通量一体等核心技术，在安徽率先完成国内通量一体现网试验；
  - ✧ 二是启动“点亮百城”量子试验网，成立量子生态联盟，加速超 10 省量子通信基础设施建设；
  - ✧ 三是投产量子密码服务平台，打造量子密话、量子密讯等多款量子通信产品，赋能政务、司法、公安等超 10 个领域,服务用户规模超百万；
  - ✧ 四是深化产学研协同，与国科量子合资成立信通数智量子科技有限公司，与头部设备厂商联合研发通量一体板卡及设备。
- **产业及生态倡议：**
  - ✧ 一是共同攻关核心技术，助力我国量子科技高水平自立自强。
  - ✧ 二是共推行业标准体系，提升跨行业、跨主体、跨路线的互联互通水平。
  - ✧ 三是共拓普惠应用，推动量子通信向更大范围拓展、更深程度渗透、更高层次演进。

- **未来方向：**与产业各方一道，共同推动量子通信产业化、商业化、规模化发展,加速服务千家万户、赋能千行百业。

参考资料

近日，广东移动联合中移互联网公司，携手中山市政务服务和数据管理局、应急管理局，成功落地“5G+量子加密”安全通信专线。这是广东移动量子城域网在中山政务领域的首次实战应用，为政务安全通信打造可复制、可推广的实践样板。

突发应急事件中，现场指挥车与后方指挥中心需实时传输高清画面、环境监测数据、调度指令，这直接关系救援黄金时间。而传统传输方式难以同时满足高速低时延与敏感信息保护的双重需求。针对这一痛点，广东移动量身打造解决方案：在应急指挥车和电子政务外网核心机房部署量子安全加密设备，依托 5G 政务专网实现量子加密传输，构筑应急通信安全与效率双重保障。

该专线采用“后量子密码算法+量子密钥+国密算法”三重加密技术，对接量子安全服务平台实现“一次一密”。密钥随机生成、用完即废，确保敏感信息从发送到接收全程加密，从源头防范窃听、篡改风险。

在传输层面，高带宽性能稳定承载大流量信息交互，满足多类型数据同步传输需求；在响应层面，端到端加密时延极低，保障应急指挥指令实时下达、高效响应。中山市应急管理局相关负责人表示：“量子加密让每一条应急指挥指令、每一帧现场图像都有了物理级安全保障。”

去年 10 月，在 2025 中国移动全球合作伙伴大会上，中国移动与中国电科、中国信科等十余家生态伙伴代表共同启动“点亮百城”量子试验网并正式发布量子生态联盟。作为量子试验网建设的重要成果，今年 3 月中旬，广东移动量子城域网顺利开通。中山“5G+量子加密”项目正是基于量子城域网打造。

目前，广东移动已搭建起“量子网络+量子平台+量子应用”一体化量子通信服务体系，为量子技术从实验室走向应用场景奠定了坚实基础。下一步，将持续推动量子技术深度赋能全省更多政务及产业应用场景，加快量子加密应用规模化普及。

3.2.4 运营商行业实践特征及启示

综合中国电信、中国移动两大头部运营商在量子城域网、政企专线、5G 安全底座、轻量化终端等领域的抗量子安全实践，本节梳理阐述运营商行业在量子安全建设中的共性特征、差异化路径及核心启示，为通信行业规模化推广提供可借鉴的实践规律。

表：运营商行业抗量子安全实践共性与差异化特征对比

对比维度	共性特征	差异化特征
技术路线	均采用 QKD+PQC 融合架构，叠加国密兼容，构建多重防护	中国电信：侧重广域骨干 QKD+PQC 融合； 中国移动：侧重轻量化 PQC + 量子随机数
推进模式	战略引领、体系化布局、规模化落地，产品化输出安全能力	中国电信：优先骨干网、跨域专线、高安全行业； 中国移动：优先移动端、边缘节点、普惠场景
成果与生态	均布局量子基础设施与行业应用	中国电信：重基础设施落地、推出量子密信/密话产品、暂未发布系统性白皮书； 中国移动：发布技术/迁移白皮书、牵头生态联盟
产品形态	均形成量子专线、加密通信、密码服务等产品矩阵	中国电信：基础设施级量子专线、行业方案、量子密信/密话； 中国移动：轻量化终端、SIM 卡、加密应用
核心挑战	均面临物理传输限制、存量设备兼容、终端生态碎片化	中国电信：骨干网传输衰减、大型设备改造难； 中国移动：海量终端适配、轻量化优化难

（一）行业实践共性特征

(1) **一是坚持战略引领、体系化布局、规模化落地的顶层推进模式。**头部运营商均将量子安全纳入集团核心战略，构建“量子基础设施+密码服务平台+行业应用”三位一体架构，以“QKD+PQC 融合”技术为核心，统筹推进网络、平台、产品、生态全链条建设，优先在重点城市、重点行业形成规模化覆盖，体现出基础设施型企业的系统性思维与规模化推进能力。

(2) **二是采用技术融合、分层防护、场景适配的安全架构设计。**普遍以 QKD 提供物理层安全、PQC 提供算法层安全、国密提供兼容层安全为核心逻辑，构建多重防护体系；同时根据广域骨干、城域接入、政企专线、移动终端等不同场景特性，差异化配置安全能力，兼顾安全强度、传输效率与适配成本。

(3) **三是突出网云协同、产品化输出、行业赋能的业务导向。**依托自身 OTN 光网、5G 网络、云平台资源，将量子安全能力封装为标准化产品，形成量子专线、量子密信、量子密话、量子超级 SIM 卡等产品矩阵，面向政务、金融、能源、工业、水运等行业提供定制化解决方案，实现安全能力的规模化对外输出。

(4) **四是面临物理传输限制、存量设备兼容、终端生态碎片化三大共性工程挑战。**量子信号长距离传输存在衰减问题，成码能力受限；现有光传输、路由设备与量子加密模块融合难度大，改造运维成本高；海量存量终端不支持 PQC 算法，规模化升级周期长、协调难度大，成为行业共同痛点。

（二）行业实践差异化特征

(1) **一是技术路线侧重不同。**中国电信侧重“广域骨干网+QKD+PQC”融合，聚焦量子城域网、跨域政企专线等大带宽、高安全场景，强化物理层与算法层双重防护；中国移动侧重“轻量化终端+PQC+量子随机数”，聚焦移动端、边缘侧、物联网等低功耗、广覆盖场景，以超级 SIM 卡、轻量化芯片为载体，突出普惠化、易部署特性。

(2) **二是成果发布与生态方式不同。**中国移动更侧重标准引领、白皮书发布、生态联盟共建，先后发布《通量一体技术白皮书》《抗量子密码敏捷技术白皮书》《抗量子密码迁移白皮书》，牵头成立量子生态联盟，推动行业共识与标准建设；中国电信聚焦基础设施建设、场景落地、产品创新，同样推出量子密信、量子密话等终端加密产品，但暂未公开系统性行业白皮书，实践导向更突出。

(3) **三是场景覆盖优先级不同。**中国电信优先布局省会及重点城市量子城域网、跨省市政企专线、行业专网，服务高安全等级的政务、金融、能源、水运等行业；中国移动优先覆盖政务、司法、公安等移动端加密通信、5G 边缘节点、中小微政企轻量化专线，侧重民生与普惠型安全应用。

(4) **四是产品化形态不同。**中国电信以量子 OTN 专线、量子云网、行业定制化解决方案为主，强调大带宽、低时延、高可靠的基础设施级安全能力；同时同步推出量子密信、量子密话等终端加密应用，完善端到端安全覆盖。中国移动以量子密讯、量子超级 SIM 卡、轻量化密码芯片为主，强调终端侧、用户侧的轻量化、易用化安全能力，适配海量终端与移动场景。

（三）行业实践核心启示

(1) **一是网基先行、分层防护是运营商量子安全的核心路径。**依托通信网络天然的广覆盖、大带宽优势，优

先建设量子城域网等基础设施，再通过 QKD、PQC、国密分层融合，构建物理安全、算法安全、兼容安全三重防护，是平衡安全、性能、成本的最优解。

(2) **二是产品化封装、行业化赋能是规模化落地的关键抓手。**将复杂的抗量子安全技术转化为标准化、可复制的产品，针对不同行业场景输出定制化方案，降低客户使用门槛，快速扩大应用覆盖面，是基础设施型企业推动技术普及的有效模式。

(3) **三是轻量化适配、生态协同是移动与边缘场景的破局关键。**面对海量存量终端、低功耗设备与碎片化生态，必须聚焦轻量化算法优化、终端芯片适配、生态伙伴协同，联合设备厂商、终端厂商、行业客户共同推进，才能破解终端兼容难题，实现普惠化量子安全覆盖。

(4) **四是统筹技术演进与成本平衡是长期可持续的基础。**量子技术仍处于发展阶段，物理传输限制、设备成本、算法性能等问题需持续优化；需坚持技术创新与成本控制并重，优先在高价值场景投入，逐步迭代升级，避免过度投入导致资源浪费，保障量子安全建设的长期可持续性。

3.3 能源行业：工控高可用、开采-储运一体化关键设施防护实践

能源行业是国家关键信息基础设施的核心组成，覆盖上游能源开采（油气、煤炭、风光场站）、中游储运（电网、油气管道）、下游调度工控、数据存储等多环节全链条，支撑国民经济命脉运行。数字化转型推动能源系统由封闭专网转向开放互联、跨域协同、海量边缘终端接入，量子威胁沿开采—储运—调度—终端全链路传导，呈现攻击面广、后果致命、影响周期长、设备老旧异构、弱网环境多的行业特征。抗量子安全迁移需兼顾极端环境适配、工控实时性、长周期服役、弱网通信、合规保密等多重约束。

3.3.1 行业迁移约束：极端环境、工控实时、长周期服役、弱网异构与合规保密

能源行业抗量子安全迁移受全链条刚性约束，核心矛盾集中在安全升级与生产连续性、老旧设备适配、弱网兼容、极端环境适配之间的平衡，与金融高并发、运营商广域带宽约束存在显著差异。

（一）极端环境约束

油气井场、海上平台、煤炭工作面、偏远风光场站等多处于荒漠、海上、山区、高寒/高温、高粉尘、强电磁干扰等无人值守场景。设备需满足工业级宽温、防尘抗震、抗电磁干扰、低功耗、长期免维护等要求；抗量子安全改造需采用轻量化、嵌入式、工业级高可靠方案，无法依赖机房级精密设备。

（二）工控实时性约束

电网调度、油气管道阀门控制、开采设备自动化、储能调节等环节，依赖毫秒级确定性时延、指令零抖动、全程无中断运行。抗量子安全改造引入的算法运算开销、报文长度膨胀、密钥交互时延等弊端，直接影响控制指令下发与执行，极端情况下可引发设备误动、介质泄漏、电网振荡、大面积停电等严重生产安全事故。

（三）长周期服役约束

能源开采装备、输变电设备、工控终端等服役周期普遍达 10–30 年，存量设备多为专用工控硬件、嵌入式系统，存在算力有限、存储空间小、无通用扩展接口等短板。设备整体替换成本极高、更新周期极长，抗量子安全改造必须以软件适配、轻量算法移植、旁路部署、存量系统兼容为核心原则，严禁大规模硬件更换。

（四）弱网异构网络约束

开采现场、偏远场站、海上平台普遍采用卫星链路、窄带无线通信，具有带宽受限、时延抖动大、丢包率高、链路稳定性差等特征；同时能源网络存在 Modbus、DNP3、IEC 60870、工业物联网协议、专网/公网混合等异构协议栈，抗量子安全改造需简化密钥交互流程、降低传输开销、兼容多协议、适配弱网容错机制，避免通信中断或协议解析异常。

（五）合规保密约束

能源行业属国家关键信息基础设施的核心，需严格遵循《密码法》、网络安全等级保护 2.0、《电力监控系统安全防护规定》等行业合规要求；开采地质数据、调度指令、生产参数、用户用电数据涉密等级高、保密周期长达数十年，长期面临“先存储、后破解”的量子潜伏威胁，需同时满足国密合规、后量子密码安全、数据长期保密、控制指令完整性等多重刚性要求。

表：能源行业抗量子安全迁移约束对照

约束维度	核心特征	安全影响
极端环境约束	户外无人值守、宽温防尘、强电磁干扰、低功耗免维护	精密量子设备无法部署，常规加密易失效，终端安全防护难度陡增
工控实时性约束	毫秒级响应、确定性时延、指令零抖动、全程无中断	量子加密引入时延/抖动，易诱发设备误动、泄漏、电网事故
长周期服役约束	设备服役 10–30 年、算力弱、存储小、无扩展接口	硬件替换成本高昂，新算法原生适配难，存量兼容复杂度高
弱网异构约束	窄带/卫星、高时延高丢包、多协议异构、链路不稳	密钥交互易中断，报文膨胀加剧丢包，易引发通信失效
合规保密约束	关键基础设施、高涉密、长期保密、强监管	量子破解可致核心数据泄露、合规失效、重大安全事件

3.3.2 核心业务场景解构：开采、储运、调度、通信骨干网、数据中心

能源行业抗量子安全防护覆盖上游开采、中游储运、下游调度、数据存储等全链条多环节，抗量子安全迁移应优先聚焦安全等级最高、威胁传导最直接、后果最严重的核心场景。

（一）能源开采现场通信与控制

- **场景特征：**上游源头核心场景，涵盖油气井场、海上钻井平台、煤炭综采工作面、风电/光伏场站；设备分布分散、长期无人值守、环境极端、依赖远程运维，工业私有协议占比高。
- **安全影响：**量子攻击可窃取地质储量、勘探测绘等核心数据，篡改开采工艺参数，劫持设备启停、调速等控制指令，直接导致生产中断、资源泄露、设备损毁、安全事故。
- **安全诉求：**保障开采勘探数据机密完整、远程运维链路可信、设备控制指令精准可控、适配弱网低功耗、极端环境下稳定可靠运行。

（二）油气/煤炭储运管道工控

- **场景特征**：中游输送关键环节，覆盖油气长输管道、煤炭集运管线、泵站/阀门控制节点；采用专用工业专网、有线无线融合组网，时延低、可靠性高，协议标准化程度高。
- **安全影响：**量子攻击篡改阀门开关、压力调节等指令，劫持控制链路，易引发油气泄漏、爆炸事故、环境污染、能源供应中断等灾难性后果。
- **安全诉求：**保障管道控制指令完整机密、传输链路抗劫持、阀门/压力调节精准可控、毫秒级响应、全程可控可追溯。

（三）电力调度专网

- **场景特征：**能源系统“神经中枢”，涵盖国家/省级调度中心、区域变电站、换流站；专用光纤组网、时延低、可靠性高，为封闭专网，采用 IEC 60870-5-104 标准协议。
- **安全影响：**量子攻击篡改调度指令、劫持控制信号，易诱发电网振荡、大面积停电、跨区域能源供应瘫痪，直接影响国计民生与社会稳定。
- **安全诉求：**保障调度指令完整机密、传输链路抗篡改、继电保护动作可靠、毫秒级响应、全网协同可控。

（四）电力骨干通信网络

- **场景特征：**跨区域能源传输骨干，覆盖特高压交直流线路、省级电力通信网、风光外送通道；光纤专网组网、带宽大、距离长，跨域互联特征明显，逐步向开放网络演进。
- **安全影响：**量子窃听或长期破解可泄露电网运行、新能源出力、负荷预测、灾备策略等关键数据，诱发战略级信息泄露、跨域网络攻击渗透风险。
- **安全诉求：**保障生产运维数据机密完整、跨域传输抗窃听、核心数据长期保密、适配大带宽传输、灾备同步可靠。

（五）能源数据中心与灾备中心

- **场景特征：**全链条数据存储核心，涵盖油气地质数据中心、电网生产数据中心、省级灾备节点；本地高速网络、跨域专线备份，存储容量大、吞吐率高，封闭与开放网络混合组网。
- **安全影响：**量子长期破解可泄露数十年地质、生产、用户、算法模型等核心数据，直接导致历史数据失效、合规追责、核心资产流失。
- **安全诉求**：保障静态数据加密防护、密钥体系量子安全、灾备同步机密完整、核心数据长期保密、数据防篡改可追溯。

表：能源行业核心业务场景特征与安全影响对照

场景名称	场景特征	安全诉求	安全影响	迁移优先级
能源开采现场	极端环境、无人值守、弱网、工业私有协议	数据机密完整、运维可信、指令可控、弱网适配	数据泄露、参数篡改、设备失控、生产事故	★★★★
油气 /煤炭储运工控	工业专网、低时延、高可靠、标准化协议	指令完整机密、抗劫持、精准控制、毫秒响应	泄漏爆炸、环境污染、供应中断	★★★★★
电力调度专网	封闭光纤、低时延、高可靠、调度核心	指令完整机密、抗篡改、继电保护可靠	电网振荡、大面积停电、能源瘫痪	★★★★★
电力骨干通信	光纤骨干、大带宽、跨域互联、逐步开放	数据机密完整、抗窃听、长期保密、灾备可靠	运行数据泄露、跨域渗透、战略信息泄露	★★★★
能源数据中心	高速存储、灾备备份、混合组网、长期存储	静态加密、密钥安全、灾备机密、长期保密	历史数据泄露、合规失效、核心资产流失	★★★★

3.3.3 能源行业典型案例复盘

能源行业覆盖广泛，结合本研究调研发现，油气化工、水电调控等关键领域已率先开展量子科技与抗量子安全技术的落地应用。本节选取齐鲁石化应用量子技术保障全链路数据安全实践、华电四川水电监控量子和后量子密码实践两大权威公开案例，从背景、实施、成效、挑战、方向等维度复盘，提炼行业落地经验。

（一）齐鲁石化：炼化企业量子加密信创一体机实践

- **背景与定位：**齐鲁石化作为国内大型炼化骨干企业，其生产经营涉及生产装置实时监控数据、炼化工艺核心参数、供应链战略情报等高敏感信息，面临量子计算带来的数据泄露、篡改风险。面对石化行业因产业链条长、业务场景复杂、数据敏感性高所带来的数据安全管理挑战，企业将量子技术纳入安全建设重点，依托国产软硬件，打造“量子加密+信创适配一体化”防护方案，保障炼化生产数据安全。
- **问题与需求**：随着行业生产和管理的数字化程度不断提高，能源行业的高价值数据资源呈现出指数级增长的态势。敏感数据一旦发生泄露、被篡改或滥用，不仅可能导致企业失去产品竞争优势，而且可能造成危

害经济运行秩序、威胁国家安全的严重后果。

- **方案实施路径：**
  - ✧ 部署中国移动密玄量子加密信创一体机，其量子加密、量子通信功能为高敏感业务数据构建了更高级的安全屏障，实现了端到端的全链路防窃听、防篡改、防泄露保护。
  - ✧ 密玄量子加密信创一体机的数据加密，是基于中国移动的量子加密核心技术，采用的是“后量子密码算法（PQC）+国密混合算法”，用于信息加解密、身份签名与验证，构建了双重防护机制。
  - ✧ 密玄量子加密信创一体机内嵌的芯片，可基于量子不确定性原理生成不可预测的高熵随机数，用于支撑匹配后量子密码算法依（PQC），能够从根源上规避传统伪随机数风险，杜绝密钥破解风险，抵御量子算力的冲击。
  - ✧ 除此之外，树脂部的安全管理系统、电子作业系统、ERP（企业资源规划）系统、人员定位系统等 83 套核心系统也全部实现了国产软硬件环境下的适配，为能源安全奠定了坚实的“信息底座”。
  - ✧ 在通信安全方面，密玄量子加密信创一体机依托中国移动的 5G 量子专网，构建安全的数据共享通道。同时，量子信道抗电磁干扰强，适配石化复杂工业环境，通信时延较传统 VPN 降低 90%以上，保障了实时数据传输不中断。
  - ✧ 此外配套的量子密盘、量子密邮、加密消息等功能，可实现数据加密、阅后即焚、防截屏录屏、权限分级管理。
- **核心成效：**
  - ✧ 量子随机数从根源规避伪随机数风险，后量子密码算法抵御量子算力攻击，国密算法防护传统网络威胁，形成双重防护。
  - ✧ 5G 量子专网时延较传统 VPN 降低 90%以上，实时数据传输稳定，系统响应流畅、视频无卡顿，解决原有操作迟缓问题。
  - ✧ 工艺、生产、供应链等高敏感数据实现防窃听、防篡改、防泄露，保障炼化核心信息安全。
- **现存挑战：**
  - ✧ 炼化厂区高温、高粉尘、强电磁极端环境，对量子设备稳定性、防护等级要求高。
  - ✧ 存量工控、生产系统老旧，与量子加密模块适配存在一定难度。
- **未来方向：**深化量子技术与智能制造融合，拓展智能仓储、绿色低碳场景应用；推进量子设备工业级适配，向炼化上下游推广。

（二）华电四川：水电站量子通信与监测安全实践

- **背景与定位：**水电作为关键能源设施，集中监控系统远程指令传输、大坝监测存在安全隐患。华电四川牵头，联合多方，在四川凉山博瓦水电站开展“量子通信+量子测量+密码加固”试点，保障水电调控与设施安全。
- **实施路径：**

- ✧ 构建“量子密码+后量子密码+商用国密”三重密码融合体系，形成纵深防御，覆盖控制指令、监测数据、身份认证。
- ✧ 搭建量子加密传输通道，实现成都集控中心至凉山博瓦水电站机组启停、负荷调节、水闸控制指令加密传输。
- ✧ 引入量子测量技术，对大坝、边坡开展全天候高精度形变监测，提前预警风险。

- **核心成效：**
  - ✧ 三重加密有效防范指令劫持、篡改风险，跨数百公里指令传输稳定。
  - ✧ 量子测量大幅提升大坝、边坡监测精度，强化水电设施安全预警能力。
  - ✧ 项目进入试运行，为国内水电行业量子安全应用提供首个样板。
- **现存挑战**
  - ✧ 偏远山区水电站弱网环境下量子密钥分发稳定性需持续优化。
  - ✧ 量子测量技术在水利场景应用尚处初期，规模化成本偏高。
- **未来方向：**以水洛河项目为样板，向四川全域水电站推广；深化量子通信与量子测量融合，拓展流域调度、生态监测场景。

参考资料

新型电力系统未来将面临着超大规模计算量、超多测量应用场景、超高通信安全和超精密时间等新要求，有望率先实现量子技术的产业化应用。近期电力量子技术的应用主要有如下十大场景：

➢ 场景一：电力通信骨干网络量子加密

量子保密通信可用于保护政企专网基础设施及其服务的安全性，已在合肥、济南、武汉、海口、贵阳等政府部门率先实现应用。目前，各省级电力公司部分调度、通信线路已成功试验线路级加密，未来新型电力系统的骨干通信网络，也可采用较为成熟的解决方案，进一步实现网络级加密。

➢ 场景二：电力数据传输终端量子加密

目前终端加密已在电力开关、断路器、监测设备上进行了多种试点试验，未来可能面向调度、营销等核心数据传输的电力移动终端设备，针对数据交互的“最后一公里”问题使用量子加密技术以增强安全性。目前，针对终端的量子加密技术已在人民银行、工商银行、建设银行等金融机构 ATM、POS 机上率先应用。

➢ 场景三：云端、数据中心及灾备中心量子加密

在不同的电力数据中心之间进行数据备份及业务连续性等业务时，量子保密通信可以用于保障数据传输的安全性。目前，该项技术已在阿里云数据中心率先应用。公司灾备中心、数据中心进一步强化数据贯通，可以考虑使用量子加密技术保障稳定同步。

➢ 场景四：重要活动及区域电力通信量子加密

面向奥运保电、重点核心区域保电等典型场景，可以在电话、网络及电力通信中采用量子加密技术以增强通信安全性。2021 年，国网公司在杭州亚运保电中，使用了世界首台配网量子加密智能开关，有效保护了亚运电网安全。

➢ 场景五：电力设备局部放电量子传感检测

利用量子检测技术可以为电力设备局部放电等微弱信号进行精准识别与传感。目前，国网公司在利用光量子进行开关柜及组合电器局部放电、南网公司在利用金刚石色心量子进行变压器局部放电方面均有较多的工程试验。

➢ 场景六：超特高压交直流输变电工程电流电压测量

面向超/特高压环境电流测量设备精度不足、稳定性不够、技术难以自主掌控的难题，基于金刚石色心量子传感器，能够实现各电压等级交直流输变电工程电流、电压测量。2025 年 1 月，南方电网联合中国电气装备，已成功研制全球首套±800 千伏量子电流传感器，满足 1 毫安至 10 千安范围内、万分之六的宽量程、高精度电流测量。

➢ 场景七：振动、气流、气体等量子监测

高压电缆在风力作用下易产生高频低幅振动，变电设备维护与故障诊断需要对气流及气体吸收系数进行精准量测，基于量子传感器能够有效精细感知电力设备及其周边气流气体的变化。2024 年 11 月，国网合肥候店变电站已成功应用多项量子监测技术及相关设备；南网也形成了基于非正交量子测量的气体检测方法及装置。

➢ 场景八：储能电池全生命周期健康水平监测

储能电池涉及 10~30 年的超长服役周期，传统检测手段存在精度不足、破坏性检测等痛点，当前主要以高冗余来应对电池性能退化引发的安全隐患。因此，实时准确地监测电池状态参数，有利于保障电池安全运行、延长电池寿命、优化储能系统性能、推动电池智能管理。目前，日本已实现金刚石量子传感器高精度监测电动汽车电池，可以有效精确监测电池工作状态。

➢ 场景九：精确统一电力系统时间频率标准量值

电力计量、信通、调度、继保和自动化的授时授频服务需求和实验室现场或远程时频装置检测，对时间频率标准量值有高精细化需求。量子时钟及其同步技术能够有效提升当前电力时间频率量值传递体系，进一步提升电力系统控制水平。目前，中国电科院已建立“三氢三铯”钟组，处于国际电力时间频率标准领先水平，但相较国际领先的铝离子量子逻辑光钟还有精度上的量级差距。

➢ 场景十：电网潮流量子计算

新型电力系统中，分布式新能源主体和多元负荷的大量接入，导致电网潮流计算难度剧增。量子计算能在特定环境下，开发专用算法对电网点、负荷点、枢纽点、平衡点的功率、电压、相位角等进行高速计算，进一步提升电力系统整体的控制水平。目前，国网公司已建成合肥候店量子应用示范变电站示范工程，开发了基于量子计算的专用电网潮流算法并在超导量子计算机上对示范站区域真实电网进行示范验证，但应用条件较为苛刻，普适性和推广性仍有较大提升空间。

3.3.4 能源行业实践特征及启示

综合齐鲁石化炼化全链路防护、华电四川水电监控加固两大行业实践，结合能源行业开采—储运—调度—工控全链条特性，本节梳理出能源行业在量子安全建设中的共性特征、差异化路径及核心启示，为能源关键基础设施量子安全规模化落地提供可借鉴的实践规律。

表：能源行业抗量子安全实践共性与差异化特征对比

对比维度	共性特征	差异化特征
技术路线	国密+后量子密码叠加，适配工业环境，信创融合	炼化：后量子+国密+量子随机数+5G 量子专网； 水电：量子通信+后量子+国密+量子测量
推进模式	工业适配优先、工控场景优先、生产连续性兜底	炼化：一体化设备、全系统覆盖、信创深度融合； 水电：试点先行、局部加固、技术融合验证
场景优先级	优先工控指令、实时数据、核心工艺/调控数据	炼化：生产监控、工艺参数、供应链数据； 水电：控制指令、机组调节、大坝边坡监测
核心挑战	工业环境严苛、存量设备老旧、专业人才不足	炼化：极端环境设备稳定性、老旧工控适配； 水电：弱网密钥稳定性、量子测量成本偏高

（一）行业实践共性特征

(1) **一是坚持工业适配、信创融合、密码叠加的安全架构设计。**能源行业普遍以国密算法为基础、后量子密码增强、量子密钥/量子随机数赋能，形成多重防护；同时深度适配工业环境，强调耐高温、防尘抗震、强电磁兼容、低功耗，并与信创生态深度融合，实现软硬件全栈自主可靠，契合关键基础设施安全底线要求。

(2) **二是采用场景聚焦、工控优先、生产兜底的落地策略。**优先覆盖炼化生产监控、水电集中控制、工业指令传输、核心工艺数据存储等高敏感、高影响场景；坚持不影响生产连续性、不中断工控运行、不降低系统稳定性，改造以旁路部署、轻量化嵌入、不改动核心控制逻辑为原则，保障能源生产安全稳定。

(3) **三是突出端到端全链路、数据分级防护、实时优先的安全导向。**覆盖现场终端—传输链路—集控中心—数据存储全链条，针对工艺参数、控制指令、供应链情报、大坝监测数据实施分级加密；优先保障毫秒级控制指令、实时监测数据、调度信令的传输安全，兼顾数据长期保密与业务实时性平衡。

(4) **四是面临工业环境严苛、存量设备老旧、专业人才不足三大共性工程挑战。**炼化、水电现场极端环境对量子设备稳定性、防护等级要求高；存量工控、生产系统服役周期长、异构复杂、算力有限，适配改造难度大；能源行业量子技术专业运维人才储备不足，长期运维体系不完善，制约规模化推广。

（二）行业实践差异化特征

(1) **一是技术路线侧重不同。**炼化行业（齐鲁石化）侧重后量子密码+国密混合、量子随机数赋能、5G 量子专网通信，聚焦工业数据加密、信创适配、复杂工业环境通信稳定；水电行业（华电四川）侧重量子通信+后量子密码+国密三重融合、量子测量技术协同，兼顾控制指令传输安全与大坝边坡物理安全监测，形成“信息安全+物理安全”双重防护。

(2) **二是场景覆盖优先级不同。**炼化行业优先覆盖生产装置实时监控、工艺核心参数、ERP 系统、供应链数据、人员定位等生产经营全链路场景，强调数据防泄露、防篡改、防窃取；水电行业优先覆盖远程集中控制指令、机组启停/负荷调节、水闸控制、大坝边坡监测等调控与设施安全场景，强调指令防劫持、防篡改、风险预警。

(3) **三是改造模式与成本平衡不同。**炼化行业采用一体化设备集中部署、全系统覆盖、信创深度融合模式，侧重一次性全栈升级、安全与效率双提升；水电行业采用试点先行、局部加固、技术融合验证模式，侧重低成本快速落地、小范围验证后推广、技术可行性优先。

（三）行业实践核心启示

(1) **一是工业适配是能源量子安全落地的前提。**能源场景极端环境、工业协议异构、存量设备老旧是刚性约束，量子安全方案必须轻量化、嵌入式、高可靠、强防护，优先采用旁路部署、不改动核心工控逻辑，兼顾安全升级与生产连续性，这是能源行业区别于金融、运营商的核心前提。

(2) **二是密码叠加+信创融合是关键基础设施的最优解。**能源行业需同时满足量子安全、国密合规、自主可靠三重要求，“国密打底、后量子增强、量子密钥/随机数赋能、信创适配”的混合架构，既能抵御量子威胁，又能兼容存量系统、保障国产化替代，契合关键基础设施安全战略需求。

(3) **三是场景分层、工控优先是高效迁移的核心逻辑。**能源场景差异显著，需优先保障工控指令、实时监控、核心工艺数据安全，再逐步扩展至管理、供应链、存储场景；避免一刀切式改造，平衡安全优先级、性能约束与改造成本，实现精准防护、稳步推进。

(4) **四是生态协同与人才储备是规模化推广的基础。**能源行业需联合量子技术厂商、工业设备商、信创企业、

科研机构协同攻关，解决工业级量子设备适配、算法轻量化优化、跨厂商互操作问题；同时加强量子安全+工业控制复合型人才培养，完善运维体系，为抗量子安全技术规模化赋能能源产业奠定基础。

3.4 政务领域：集约化政务云与跨域数据共享实践

政务领域是国家治理体系与治理能力现代化的核心载体，承载政务服务、民生保障、社会治理、应急指挥等关键职能，属于国家关键信息基础设施。随着“数字政府”建设深入推进，政务系统由分散独立、部门壁垒转向集约化云化、跨域共享、开放协同，数据流动更频繁、交互链路更复杂、安全边界更模糊。量子威胁直接冲击政务数据长期保密、跨域互信、身份可信、服务连续性，叠加分级分类管控、等保密评刚性、跨部门互认、公众高可用等约束，形成政务领域独有的抗量子安全迁移路径。

3.4.1 行业迁移约束：分级管控、跨域互认、合规刚性与公众高可用

政务领域抗量子安全迁移受合规、数据、跨域、服务、生态多重刚性约束，核心矛盾集中在安全分级与统一标准、跨部门互信与数据共享、合规刚性与敏捷升级、公众服务连续性之间的平衡，与金融、运营商、能源行业约束特征存在显著差异。

（一）分级分类管控约束

政务数据按涉密等级、敏感程度、公开范围严格分级，涵盖绝密、机密、秘密、内部、公开五级，不同级别数据安全策略、加密强度、访问权限、存储周期要求差异极大。抗量子安全改造需分级适配、精准防护、策略隔离，严禁低级别防护覆盖高级别数据，也不允许过度防护造成资源浪费。

（二）跨域互认与共享约束

政务系统部门林立、层级复杂、地域分散，横向涉及政府各委办局，纵向贯通国家—省—市—县—乡五级，跨部门、跨层级、跨地域数据共享频繁。抗量子安全改造需统一密码标准、统一身份认证、统一密钥体系、跨

域互信互通，打破部门壁垒，同时防范跨域数据泄露、篡改、劫持风险。

（三）合规刚性约束

政务领域需严格遵循《密码法》、网络安全等级保护 2.0、《数据安全法》《个人信息保护法》《政务数据共享开放条例》等法律法规，等保三级及以上系统、涉密系统、个人敏感信息、核心政务数据必须采用国密算法，抗量子安全改造需国密合规为底线、后量子安全为增强、量子密钥为补充，多重合规、多重保障。

（四）公众服务高可用约束

政务服务面向全社会公众、企业、特殊群体，需满足 7×24 小时在线、高并发访问、低时延响应、跨终端适配、无障碍服务要求。抗量子安全改造引入的算法开销、报文膨胀、密钥交互时延，必须控制在公众无感知范围内，严禁出现服务卡顿、中断、响应迟缓等问题，保障政务服务普惠、高效、稳定。

（五）存量生态异构约束

政务存量系统建设周期长、技术路线杂、厂商众多、版本不一，涵盖传统物理机、虚拟化、私有云、混合云等多种架构，操作系统、数据库、中间件、安全设备异构严重。抗量子安全改造需兼容多架构、多系统、多协议、多厂商，避免大规模替换存量设备，降低改造成本与实施难度。

表：政务领域抗量子安全迁移约束对照

约束维度	核心特征	安全影响
分级分类管控约束	数据五级分级、防护策略差异化、权限严格隔离	防护强度不匹配致高密数据泄露、低密资源浪费
跨域互认与共享约束	五级架构、部门壁垒、跨域高频共享、互信要求高	跨域数据劫持篡改、部门间信任断裂、共享失效
合规刚性约束	多重法规强监管、国密强制、数据全生命周期管控	不合规面临追责、数据泄露引发公共安全事件
公众服务高可用约束	7×24 小时在线、高并发、低时延、普惠适配	改造致服务卡顿中断、公众体验下降、公信力受损
存量生态异构约束	架构杂、厂商多、版本不一、异构设备占比高	兼容性差致系统崩溃、改造周期长、运维难度陡增

3.4.2 核心业务场景解构：政务云、跨域数据共享、电子证照、民生服务

政务领域抗量子安全防护聚焦数据存储、跨域共享、身份认证、公众服务四大核心域，覆盖政务云、跨域数据共享、电子证照、民生服务、应急指挥、涉密办公等关键场景。

（一）集约化政务云

- **场景特征：**政务系统核心底座，整合各级政府部门服务器、存储、网络资源，采用私有云/混合云架构，承载政务办公、业务系统、数据存储、灾备备份等核心功能，数据集中存储、多部门共享、访问量大。

- **安全影响：**量子攻击窃取/篡改云内核心政务数据、越权访问敏感信息、破坏灾备备份，可导致政务决策失误、民生信息泄露、公共服务瘫痪、国家治理风险。
- **安全诉求：**保障政务数据机密完整、分级加密、权限可控、长期保密、灾备可靠、云内隔离，适配云环境多租户、动态调度、弹性扩展特性。

（二）跨域数据共享交换平台

- **场景特征：**跨部门、跨层级、跨地域数据流转核心枢纽，对接公安、民政、人社、税务、市场监管等数十个部门，支撑政务协同、联合审批、数据开放、跨域协同办公，数据流动频繁、链路复杂、跨域互信要求高。
- **安全影响：**量子攻击劫持跨域数据、篡改共享内容、伪造身份越权获取数据，可导致部门间信任崩塌、协同失效、敏感数据跨域泄露、公共治理失效。
- **安全诉求：**保障跨域数据传输机密完整、抗劫持篡改、身份可信、全程可追溯、跨域互认、最小权限访问，防范跨域数据泄露与滥用。

（三）电子证照与可信身份认证

- **场景特征：**政务服务“一网通办”核心载体，涵盖身份证、营业执照、结婚证、不动产权证、电子印章、电子签名等，支撑线上办事、材料提交、身份核验、电子签章、文件签署，面向公众高频使用、身份真实性要求极高。
- **安全影响：**量子攻击伪造电子证照、篡改证照信息、破解签名验签、冒用身份办事，可导致政务欺诈、身份盗用、虚假审批、公众权益受损、政务公信力崩塌。
- **安全诉求：**保障电子证照真实可信、不可伪造、防篡改、防冒用、长期有效、跨域互认、签名验签可靠，确保身份认证全程可信。

（四）民生政务服务平台

- **场景特征：**面向公众的普惠服务入口，涵盖社保医保、公积金、教育、医疗、出行、住房、政务咨询等高频服务，用户基数大、并发量高、跨终端适配、数据敏感（个人身份证、手机号、银行卡、健康信息）、服务连续性要求高。
- **安全影响：**量子攻击窃取个人敏感信息、篡改民生数据、劫持服务会话、拒绝服务攻击，可导致大规模个人信息泄露、民生服务中断、公众隐私暴露、社会信任危机。
- **安全诉求：**保障个人敏感信息机密完整、防泄露、防篡改、隐私保护、访问可控、高可用、跨终端适配，兼顾安全与普惠便捷。

（五）应急指挥与涉密办公

- **场景特征：**安全等级最高的核心场景，涵盖应急指挥调度、防灾减灾、公共安全、涉密文件处理、机要通

信、核心决策等，数据涉密等级高、保密周期长、影响范围广、容错率极低。

- **安全影响：**量子攻击破解涉密数据、窃取决策信息、篡改指挥指令、泄露核心机密，可导致国家安全风险、应急处置失误、公共安全事件、核心机密泄露。
- **安全诉求：**保障涉密数据绝对机密、防窃听、防破解、防泄露、防篡改、指令完整、长期保密、物理隔离，满足涉密信息系统最高安全标准。

表：政务领域核心业务场景特征与安全影响对照

场景名称	场景特征	安全诉求	安全影响	迁移优先级
集约化政务云	集中存储、多租户、混合云、数据密集、共享度高	数据机密完整、分级加密、权限可控、长期保密	数据泄露篡改、决策失误、服务瘫痪	★★★★★
跨域数据共享交换	跨部门跨层级、高频流转、链路复杂、互信要求高	传输机密完整、抗劫持、身份可信、全程追溯	跨域泄露、协同失效、治理风险	★★★★
电子证照与可信认证	高频使用、跨域互认、身份敏感、防伪造、防冒用	真实可信、防篡改、防伪造、签名验签可靠	证照伪造、身份盗用、政务欺诈	★★★★
民生政务服务平台	公众普惠、高并发、个人敏感数据、跨终端、高可用	隐私保护、防泄露、防篡改、高可用、便捷适配	信息泄露、服务中断、隐私暴露	★★★
应急指挥与涉密办公	最高密级、长期保密、容错率低、物理隔离、核心决策	绝对机密、防破解、防泄露、指令完整、物理隔离	机密泄露、指挥失误、国家安全风险	★★★★★

3.4.3 政务领域典型案例复盘

政务领域围绕集约化网络、跨域协同办公、敏感信息传输等核心场景，积极推进抗量子安全技术落地应用。本节选取绵阳游仙区政务外网抗量子安全升级、河北量子密讯落地政务司法规模化应用两大权威公开案例，从背景动因、方案设计、实施路径、核心成效、现存挑战与未来方向等维度复盘，提炼政务领域抗量子安全迁移的标杆范式。

（一）绵阳游仙区：集约化政务外网抗量子安全升级实践

- **背景动因：**数字政府建设背景下，游仙区已建成“五统一”集约化电子政务外网，支撑区、镇、村三级政务办公、视频会议、数据共享等业务。随着政务数据跨层级、跨部门流转频次提升，传统加密体系难以抵御量子计算带来的长期破解威胁，骨干链路安全防护短板凸显，亟需通过抗量子技术实现安全能力跃升，筑牢基层政务网络安全底座。
- **方案设计：**
  - ✧ 依托绵阳市西南首个城市级量子城域网基础设施，采用量子网关加密专线技术，实现政务网络的平滑升级；

- ✧ 在不改变现有网络架构、不中断业务运行的前提下，为政务外网骨干链路加载“后量子密码（PQC）+国密算法”融合加密能力；
- ✧ 升级后的政务网络、全区政务数据在传输过程中实现了“端到端”的全方位量子安全防护，能够有效抵御未来量子计算机等新型算力对传统加密体系可能带来的潜在威胁，形成“高安全、低投入、易推广”的集约化升级方案。

- **实施路径：**
  - ✧ 延续“五统一”集约化建设思路，避免重复布线与大规模设备更换；
  - ✧ 仅在网络关键节点注入量子安全能力，实现区、镇、村三级网络全覆盖的安全升级。
  - ✧ 升级过程全程无感知，不影响日常办公、视频会议等核心业务，同步完成量子加密参数调试与全网适配验证。
- **核心成效：**成功推动政务网络从“高速互联”迈入“高安全互联”阶段，骨干链路实现端到端量子防护，有效抵御量子算力带来的安全威胁；相较传统改造模式，资金投入大幅降低，节省超 60%改造成本；形成可复制、可推广的基层政务抗量子安全“游仙模式”，为全国同类地区提供实践范本。
- **现存挑战：**基层政务网络节点分散，边缘侧量子安全适配需持续优化；量子城域网覆盖范围有限，偏远乡镇链路量子加密延伸难度较大；基层政务运维团队量子技术专业能力有待提升。
- **未来方向：**持续拓展量子技术应用边界，向政务云、跨部门数据交换、基层治理等领域延伸；依托绵阳量子产业生态，完善基层抗量子安全运维体系；推广“游仙模式”，助力区域政务网络安全整体升级。

参考资料

游仙区在政务网络量子安全升级方面的成功实践，离不开绵阳市对量子科技产业的前瞻性战略布局和持续不断的坚实投入。作为中国唯一的科技城，绵阳高瞻远瞩地将量子信息产业列为着力培育的八大未来产业之一，明确提出打造全国量子科技产业西部核心增长极的宏伟目标。

城市级量子城域网的建成运营，为绵阳的量子产业发展搭建了一座坚实的桥梁，为包括政务在内的各类量子安全应用提供了关键的基础设施支撑。目前，绵阳的量子技术应用正呈现出蓬勃发展的态势，从政务领域迅速向金融、能源等关乎国计民生的关键行业拓展。在银行同城数据备份、电网调度通信等关键场景中，量子技术已成功落地赋能，为这些行业的数据安全提供了强有力的保障。

与此同时，绵阳还积极投身于“星地一体”量子互联网等国家级前沿项目的技术攻关与试验，与国内顶尖科研机构和企业携手合作，共同推动量子产业生态不断完善。从游仙区的政务网络升级这一局部突破，到全市“以建促用、以用带产”的产业生态构建，绵阳正一步一个脚印，稳步推进量子技术从实验室走向规模化应用。

（二）河北政务司法：量子密讯规模化落地实践

- **背景动因：**政务、公安、司法领域存在大量案件卷宗、审批公文、指挥指令、会议纪要等高敏感信息，传统通信方式易遭监听、拦截、篡改，敏感信息泄露风险突出。数字化协同办公普及后，跨区域会商、远程提讯、应急指挥等场景对“不可破解、全程可控、便捷高效”的安全通信需求迫切，量子密讯成为破解安全痛点的关键方案。
- **方案设计：**
  - ✧ 借助量子不可分割、不可克隆的物理特性，搭配“一次一密”加密机制，让每一次通信都生成全新的

量子密钥，构建端到端加密安全，打造适配政务司法场景的量子密讯产品矩阵。

- ✧ 覆盖加密消息、加密音视频通话、加密文件传输、阅后即焚、防截屏溯源等功能，支持 APP 与 PC 客户端双端部署，兼顾安全性与易用性。

- **实施路径：**
  - ✧ 适配政务内网、司法专网等不同网络环境，无需更换手机号、无需重构现有办公网络，用户仅需安装专用 APP 并搭配量子安全模块即可快速启用；
  - ✧ 支持本地化部署，实现数据物理隔离，既不影响日常办公习惯，又能保障数据安全；
  - ✧ 已分批次在政府、公检法司、企事业单位等 14 家单位规模化落地，完成多场景适配与协同验证。
- **核心成效：**构建起政务司法领域“不可破解”的安全通信防线，敏感信息传输全程加密、防拦截、防泄露；阅后即焚、防截屏、水印溯源等功能，从源头杜绝信息外泄；跨区域协同效率显著提升，加密传输即时可达，无需线下专人送达，大幅缩短案件流转与审批周期，兼顾安全与效率。
- **现存挑战：**政务司法终端类型多样，部分老旧设备适配量子密讯存在兼容性问题；跨部门、跨层级量子密钥统一管理与互认机制需进一步完善；量子密讯功能模块较多，基层人员操作熟练度有待提升。
- **未来方向：**持续扩大政务司法领域覆盖范围，延伸至更多部门与基层单位；深化量子密讯与政务云、电子证照、应急指挥平台融合；优化轻量化适配能力，拓展移动端、嵌入式终端应用场景，助力政务安全协同生态构建。

参考资料

➢ 政务数据具有三大特征，使其成为 HNDL（先存后破）攻击的首选目标：

1）保密期极长。政务重要数据的保密期往往长达数十年。攻击者只需今天截获加密数据，等待量子计算机成熟后即可解密，届时这些关乎国家安全与社会稳定的机密信息将完全暴露。

2）信任链根基深厚。政务 PKI/CA 体系是身份可信的根基，一旦根证书的签名算法被量子计算机攻破，整个信任链将从根部崩塌，所有依赖该体系的身份认证、电子签章、数据加密都将失效。

3）协同证据需长期有效。跨部门协同形成的电子凭证、审批记录、签名文档需要长期可追溯、可验证。如果签名算法失效，这些历史凭证的法律效力将受到根本性质疑。

4）Mosca 定律告诉我们：当数据保密年限加上迁移耗时超过量子计算机可用时间时，数据已经不安全了。对于党政领域而言，这一警钟已经敲响。

➢ 党政领域密码合规：等保、密评、信创三重要求

1）等级保护 2.0 要求政务信息系统达到三级及以上安全防护标准，密码应用方案是测评核心内容。

2）密码测评已成为政务系统上线运行的必要条件，《商用密码应用安全性评估管理办法》对密码算法、密钥管理、证书体系等提出了明确要求。

3）信创适配要求政务系统全面采用国产软硬件，密码产品须在国产 CPU、国产操作系统上稳定运行。

4）后量子密码能力将是下一轮合规升级的核心方向。提前布局的党政客户，将在未来标准更新时占据先发优势。

3.4.4 政务行业实践特征及启示

结合绵阳游仙区集约化政务外网抗量子安全升级、河北政务司法量子密讯规模化落地两大实践，以及政务行业分级管控、跨域协同、公众服务优先的核心特性，本研究系统梳理出政务行业在量子安全建设中的共性特

征、差异化路径与核心启示，为全国数字政府背景下量子安全体系建设提供行业化参考范式。

（一）行业实践共性特征

(1) **一是坚持集约化统筹、轻量化部署、无感知升级的实施原则。**政务行业普遍依托现有集约化电子政务外网、政务云底座推进改造，避免重复建设与大规模硬件替换；优先采用网关植入、客户端适配、旁路集成等轻量化方式，全程不中断区、镇、村三级办公与民生服务，兼顾安全升级与业务连续性。

(2) **二是采用国密合规打底、PQC 增强、量子能力赋能的分层防护架构。**以国密算法满足等保、密评刚性要求，叠加后量子密码抵御量子算力破解风险，结合量子密钥分发或量子随机数技术强化传输与通信安全，形成“合规+抗量子+强保密”的复合防护体系，适配政务数据分级管控需求。

(3) **三是聚焦场景优先、实用导向、普惠适配的落地规律。**优先覆盖政务外网骨干传输、跨部门敏感公文流转、司法案件会商、应急指挥调度等高敏感、高影响场景；兼顾基层运维能力与用户体验，方案强调易部署、易运维、易操作，适配老旧终端、异构网络与基层技术条件。

(4) **四是面临基层运维能力不足、跨域互认机制不完善、边缘节点覆盖难三大共性工程挑战。**基层政务单位量子技术专业人才稀缺，运维体系薄弱；跨部门、跨层级量子密钥互认与统一管理机制尚未健全；偏远乡镇、村社等边缘节点网络条件有限，量子安全能力延伸难度较大。

（二）行业实践差异化特征

(1) **一是技术路线侧重不同。**基层政务网络（游仙区）侧重“量子城域网+PQC+国密融合专线”，聚焦骨干链路传输安全，依托城市级量子基础设施实现低成本、规模化覆盖；政务司法场景（河北）侧重“量子密钥+一次一密”的端到端加密通信，聚焦移动办公、跨域协同、敏感信息传输，以轻量化客户端实现便捷化、普惠化应用。

(2) **二是改造模式与成本策略不同。**基层政务采用集约化整体改造、节点注入、低成本复用模式，依托现有网络架构与量子城域网资源，大幅降低改造成本，突出规模化复制价值；政务司法采用分批次试点、单位化部署、功能化适配模式，优先保障核心敏感场景安全，兼顾不同部门差异化需求，强调快速落地与灵活适配。

(3) **三是安全防护重点不同。**基层政务网络重点强化数据传输机密性、链路抗劫持、全网覆盖防护，保障三级政务网络数据流转安全；政务司法重点强化信息防泄露、防篡改、防冒用、全程可追溯，突出敏感文件、指令、会议内容的闭环防护，适配司法办案、政务审批的高保密要求。

（三）行业实践核心启示

(1) **一是集约化复用是基层政务量子安全落地的核心路径。**基层政务资源有限、网络分散，依托现有集约化政务外网与城市级量子基础设施，采用节点注入、轻量化部署模式，既能大幅降低成本、避免重复建设，又能实现全网无感知升级，是平衡安全、成本与效率的最优选择。

(2) **二是“轻量化适配+场景化方案”是政务行业普惠化推广的关键。**政务行业终端异构、基层能力薄弱、场景差异大，量子安全方案需摒弃复杂架构，聚焦轻量化客户端、旁路集成、功能化适配，针对传输、通信、

办公等不同场景定制方案，才能快速覆盖基层、司法、公安等多领域，实现普惠化安全升级。

(3) **三是合规与安全双重融合是政务行业的刚性底线。**政务行业受多重法规强监管，必须以国密合规为基础，叠加 PQC 与量子技术增强抗量子能力，兼顾分级管控、数据保密与跨域互认，形成符合监管要求、抵御量子威胁、适配政务特性的安全体系。

(4) **四是生态协同与能力下沉是规模化推广的重要支撑。**需依托地方量子产业生态，推进城市级量子基础设施建设，为基层政务提供低成本能力支撑；同时加强基层运维人才培养、完善跨部门密钥互认机制、优化边缘节点适配方案，推动量子安全能力从核心节点向基层末梢延伸，构建全域一体化量子安全防护体系。

表：政务行业抗量子安全实践共性与差异化特征对比

对比维度	共性特征	差异化特征
技术路线	国密+PQC 融合，量子能力赋能，分层防护	基层政务：量子城域网+融合专线； 政务司法：量子密钥+端到端加密通信
推进模式	集约化统筹、轻量化部署、无感知升级	基层政务：整体改造、节点注入、低成本复用； 政务司法：试点分批、单位部署、功能适配
防护重点	数据安全、业务连续、合规适配、基层普惠	基层政务：链路传输、全网覆盖、抗劫持； 政务司法：信息防泄露、防篡改、全程追溯
核心挑战	基层运维弱、跨域互认难、边缘覆盖难	基层政务：边缘节点延伸、运维体系薄弱； 政务司法：终端兼容、密钥互认、操作适配

3.5 跨行业实践收敛：共性规律与差异化启示

综合金融、运营商、能源、政务四大重点行业的抗量子安全迁移实践，本研究系统梳理并提炼出全行业适用的共性规律，同时清晰区分不同行业在技术路线、实施策略、落地优先级上的差异化特征，为国家层面统筹抗量子安全产业布局、行业精准施策、企业科学规划提供系统性参考。

3.5.1 跨行业实践共性

（一）行业推进节奏共性：先行试点、稳步扩容、分层落地

四大行业均遵循高价值场景先行、核心系统试点、边缘末梢延后的统一推进节奏，呈现清晰的阶段性特征。

- 金融行业率先启动、节奏最快，聚焦交易清算、跨境结算、核心账务等高敏感高频场景，已进入规模化试点与双栈并行迁移阶段；
- 运营商紧随其后、覆盖最广，依托量子城域网与 5G 底座，优先覆盖政企专线、骨干传输、移动加密通信，推进规模化基础设施建设；
- 能源行业稳中求进、聚焦工控安全，优先覆盖调度指令、炼化工艺、水电监控等工控核心场景，坚持生产连续性优先、试点先行、局部加固；
- 政务行业普惠适配、基层先行，依托集约化政务网与轻量化加密应用，优先覆盖骨干传输、司法办公、民生服务，强调低成本、无感知、易推广。

（二）技术路线共性：国密打底、PQC 增强、量子赋能、混合架构

四大行业均摒弃单一技术路线，形成国密合规为底线、PQC 抗量子为核心、量子能力（QKD/量子随机数）为补充、分层防护为架构的共性技术范式，是当前过渡期平衡安全、性能、成本、合规的最优解。

国密算法保障存量兼容与合规刚性，PQC 抵御量子算力长期破解威胁，量子密钥分发或量子随机数强化物理层/熵源安全，三者叠加构建“算法安全+物理安全+兼容安全”三位一体防护，适配不同行业异构存量、复杂场景、性能约束的共性需求。

（三）工程难点共性：报文膨胀、算力开销、终端碎片化、存量兼容难

四大行业均面临算法性能损耗、终端生态割裂、存量设备异构、跨域互认不足四大共性工程挑战，是制约量子安全规模化落地的核心瓶颈。

- PQC 算法普遍存在密钥/证书体积膨胀、运算时延增加、CPU/带宽开销上升问题，对金融高频交易、运营商高并发转发、能源工控实时控制、政务普惠服务均造成性能压力；
- 终端生态碎片化严重，存量设备算力弱、无扩展接口、不支持新算法，跨厂商、跨代际互操作性差；
- 存量系统架构复杂、协议异构、更新周期长，大规模硬件替换成本高、周期长、风险大；
- 跨部门、跨层级、跨行业密钥互认与统一管理机制尚未健全，制约跨域数据安全共享。

3.5.2 行业差异化经验：场景驱动、约束适配、路径分野

（一）金融行业：高并发交易驱动，优先性能平衡与敏捷迁移

金融行业核心约束为交易 SLA 极致严苛、毫秒级响应、零中断、高并发，差异化经验聚焦轻量化 PQC 优化、密码敏捷能力、双栈并行灰度回退。

落地方面优先选用低时延、高吞吐的 PQC 算法（如 ML-KEM），构建密码服务抽象层实现算法可插拔，通

过双栈并行、灰度推送、熔断回退机制保障业务无感知迁移，平衡安全与性能。

（二）运营商：广域承载驱动，优先基础设施先行与规模化覆盖

运营商核心约束为网络规模庞大、跨域互联、带宽承载、7×24 小时稳定，差异化经验聚焦量子城域网先行、分层部署、产品化封装。

落地层面优先建设城市级量子基础设施，骨干网叠加 QKD+PQC 融合专线，边缘侧轻量化适配，将量子安全能力封装为标准化产品（量子专线、量子密讯），实现低成本规模化赋能千行百业。

（三）能源行业：工控高可用驱动，优先生产连续性与工业适配

能源行业核心约束为工控实时性、设备长周期服役、极端工业环境、弱网异构，差异化经验聚焦旁路部署、工控优先、工业级防护。

落地层面严禁改动核心控制逻辑，采用轻量化嵌入、旁路部署模式，优先保障调度指令、工艺参数、监控数据安全，设备需耐高温、防尘抗震、强电磁兼容，适配炼化、水电等极端工业场景。

（四）政务行业：合规普惠驱动，优先分级管控与轻量化适配

政务行业核心约束为分级分类管控、跨域互认、合规刚性、公众高可用、基层资源有限，差异化经验聚焦集约化复用、轻量化客户端、无感知升级。

落地层面依托现有政务云、政务网集约化资源，避免重复建设，优先采用客户端适配、网关植入、旁路集成等轻量化方式，适配老旧终端、异构网络与基层运维能力，兼顾合规、安全、普惠与低成本。

3.5.3 跨行业核心启示：分层分级、混合架构、敏捷能力、生态协同、信任迁移

（一）分层分级是高效迁移的前提

- 需按安全等级、性能约束、影响范围、改造难度对场景分层分级，高安全长周期场景（金融清算、能源调度、政务涉密）采用“QKD+PQC+国密”三重防护；
- 高频并发场景（金融交易、运营商 5G、民生服务）采用轻量化 PQC+国密；
- 边缘末梢场景（能源开采、基层政务、移动终端）采用极简算法组合，避免一刀切改造，平衡安全、性能与成本。

（二）混合架构是过渡期最优解

国密、PQC、QKD 不存在单一最优路线，混合架构是当前唯一可行路径。国密保障合规兼容，PQC 抵御量子威胁，QKD 强化高安全链路，三者灵活组合适配不同行业、不同场景，兼顾安全强度、性能需求、改造成本与迁移风险。

（三）密码敏捷能力是存量系统迁移关键

面对海量异构存量系统，必须构建密码服务抽象层、算法可插拔、双栈并行、灰度回退、密钥统一管理的敏捷能力，实现算法策略化切换、协议兼容适配、业务无感知升级，降低改造风险、缩短迁移周期，是大型存量系统平滑过渡的核心支撑。

（四）生态协同是规模化落地基础

抗量子安全规模化落地需密码设备厂商、终端厂商、CA 机构、行业主管部门、科研机构协同攻关，突破算法轻量化优化、工业级量子设备适配、跨厂商互操作、标准统一、人才培养等共性瓶颈，构建全链路、全生态量子安全支撑体系，才能推动量子安全从试点走向普及，赋能数字经济高质量发展。

表：四大行业抗量子安全实践差异对比

对比维度	金融行业	运营商行业	能源行业	政务行业
行业属性与安全定位	资金密集、交易高频、安全等级最高，关系国家金融稳定与公众财产安全	国家通信基础设施、网络覆盖最广、承载业务最复杂，支撑全社会数字通信运转	关键能源设施、工控闭环、生产不可中断，直接影响国计民生与能源安全	国家治理中枢、分级管控、跨域协同、普惠服务，保障政务运行与民生权益
核心约束条件	毫秒级交易时延、零业务中断、高并发承载、数据长期保密、监管合规刚性	网络规模庞大、跨域互联、带宽承载极限、7×24 小时稳定、异构设备复杂	工控实时性、设备长周期服役、极端工业环境、弱网异构、生产连续性优先	分级数据管控、跨部门互认、合规刚性、公众高可用、基层资源有限
核心技术路线	轻量化 PQC+国密双栈、密码敏捷架构、算法可插拔、灰度回退	QKD+PQC +国密、量子城域网先行、分层部署、量子能力产品化	国密打底、轻量化 PQC、工业级适配、旁路部署、不改动核心控制逻辑	国密合规、轻量化 PQC、量子密钥赋能、集约化复用、客户端轻量化适配
重点落地场景	核心交易清算、跨境结算、账务系统、客户敏感数据、电子签章	量子城域网、政企专线、5G 安全底座、量子密讯、边缘节点加密	电网调度、炼化工艺、水电监控、工业控制指令、生产数据传输	政务外网骨干、跨域数据共享、司法加密通信、民生服务平台、涉密办公
典型改造模式	双栈并行、试点先行、灰度推送、熔断回退、业务无感知升级	基础设施先行、节点注入、分层加固、产品化输出、规模化赋能	旁路集成、轻量化嵌入、核心系统不动、工控优先、工业级防护	集约化复用、网关植入、客户端适配、无感知升级、低成本推广
核心工程挑战	PQC 性能损耗、高频交易时延敏感、交易链路无感知迁移、跨机构互认难	量子信号传输衰减、带宽开销大、终端碎片化、跨厂商互操作复杂	极端工业环境适配、存量工控老旧、弱网密钥分发不稳定、运维能力弱	基层运维能力不足、跨域密钥互认难、边缘节点覆盖难、老旧终端兼容差
行业实践特征	安全优先、性能极致、敏捷迁移、合规先行、风险可控	规模优先、覆盖优先、基础设施先行、生态开放、普惠赋能	生产优先、稳定优先、工业适配、保守审慎、试点先行	合规优先、普惠优先、低成本、易推广、基层适配、服务优先

（五）信任体系迁移是核心

抗量子安全迁移不应局限于通信加密通道。大量行业系统真正复杂的迁移对象是信任体系，包括数字签名、

CA 证书链、电子签章、金融报文签名、软件/固件代码签名、设备身份、日志签名、可信时间戳、区块链/存证系统和 API 调用签名等。传统 RSA、ECDSA、EdDSA、SM2 等签名机制在具备大规模密码相关量子计算机的条件下均面临结构性风险，因此应将签名类资产纳入第一批密码资产盘点和 CBOM 范围。

(1) 各行业信任体系迁移侧重：

- 金融行业应重点关注交易签名、清算报文签名、电子回单、银企直连证书、支付接口签名和移动银行客户端签名；
- 政务领域应重点关注电子证照、电子印章、跨部门数据共享签名、政务服务身份认证和电子档案长期验真；
- 能源行业应重点关注工控指令签名、固件升级签名、边缘网关身份、远程运维授权和调度日志完整性；
- 运营商应重点关注网络设备证书、网元身份、MEC/边缘节点认证、政企专线接入认证、SIM/eSIM 相关信任链和海量 IoT 设备身份。

(2) 签名类迁移应遵循“先发现、再并行、后替换”的原则：

- 先识别所有签名资产和验证依赖，再采用传统签名+PQC 签名、国密签名+PQC 签名等混合证书或双签机制进行灰度验证，最后结合标准成熟度、监管要求和生态兼容性分批替换。
- 任何代码签名、固件签名和证书链迁移均必须具备回滚能力、吊销能力、离线验签能力和长期验证策略，避免因签名体系切换造成设备不可用、软件不可升级或历史证据无法验证。

综上，本章围绕金融、运营商、能源、政务四大重点行业，系统剖析了抗量子安全迁移的约束条件、核心场景、典型实践与行业规律。各行业因业务属性、安全底线、性能要求差异，形成了截然不同但又高度趋同的迁移路径：均以国密合规为基础、PQC 为核心、量子技术为补充，采用分层防护、混合架构推进落地。金融行业聚焦高并发交易，强调性能平衡与敏捷迁移；运营商依托广域网络，优先基础设施建设与规模化覆盖；能源行业严守工控安全底线，突出生产连续性与工业适配；政务行业立足分级管控，强调普惠适配与低成本落地。跨行业对比可见，行业共性集中在报文膨胀、算力开销、终端碎片化、存量兼容难等工程瓶颈，而差异化主要源于业务驱动、约束强度、安全等级。

整体而言，四大行业已形成场景分层、混合架构、敏捷迁移、生态协同的实践共识，为国家关键信息基础设施量子安全体系建设提供了可复制、可推广、可验证的行业范式。

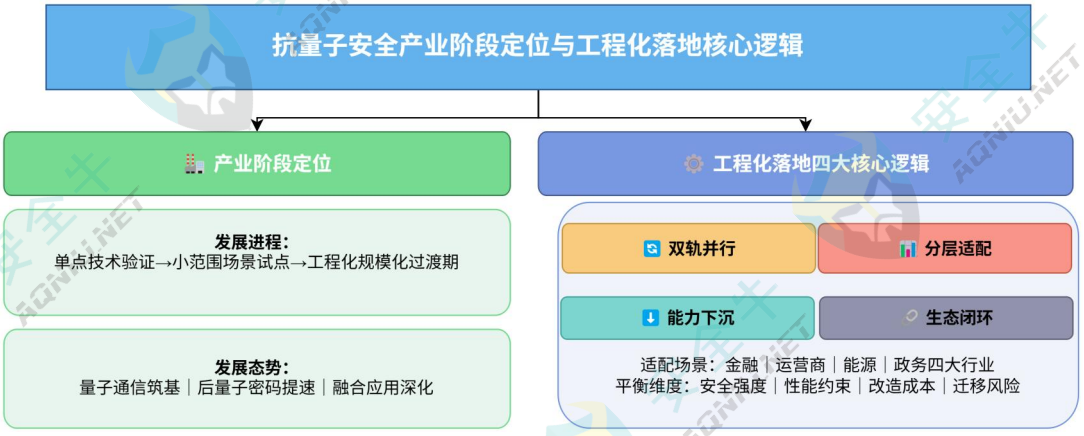
第四章 抗量子安全工程化落地产业侧能力全景与路径突破

当前，抗量子安全已从概念探索、单点试点迈入工程化落地、规模化推广的关键阶段。前三章已经围绕产业重构逻辑、迁移改造框架、行业实践差异完成了系统论证，揭示了“国密+PQC+量子赋能”混合架构的普适性、行业约束驱动的差异化路径，以及工程化过程中的共性瓶颈。在此背景下，产业侧的技术供给、产品成熟度、产业链协同能力，就成为决定抗量子安全能否从试点走向普及、从行业标杆走向全域覆盖的核心变量。

本章立足产业全局，聚焦量子通信与后量子密码双生态圈，系统梳理从底层硬核技术、核心芯片设备、网络基础设施，到网络安全、密码安全方案以及行业应用集成的完整能力链条。重点剖析工程化落地面临的技术性能、产品生态、成本效益、运维人才四大核心挑战，明确轻量化适配、标准化互操作、国产化替代、生态协同等关键突破口；同时结合标杆厂商亮点能力，验证产业化可行性与成熟度；最后总结当前产业短板，提出未来技术攻坚、产品完善、生态共建、规模推广的能力建设方向，旨在从产业供给端回答“能落地什么、难在哪、如何突破”，为抗量子安全规模化工程化落地提供全景判断与路径参考。

4.1 产业阶段定位与工程化落地核心逻辑

抗量子安全工程化落地的推进节奏，很大程度上取决于产业所处的发展阶段，因此首先需要明确当前产业侧技术与产品供给能力的边界和成熟度，各行业才能在此基础上结合实际情况推进适配落地工作。本节将聚焦抗量子安全产业发展阶段划分与工程化落地逻辑两大核心，围绕双轨并行、分层适配、能力下沉、生态闭环等产业核心命题，厘清量子通信、后量子密码、量子随机数三大技术领域的能力边界与成熟度差异。



4.1.1 产业阶段定位：从技术试点迈向工程化规模化过渡期

基于前三章对抗量子安全产业重构、迁移改造框架逻辑、行业实践共性与差异的系统性分析，本研究认为

当前我国抗量子安全产业已完成单点技术验证、小范围场景试点的起步阶段，正加速进入混合架构普及、工程化适配攻坚、产业链协同推进的关键过渡发展期，呈现出“量子通信筑基、后量子密码提速、融合应用深化”的发展态势。

- **量子通信保密（基于物理 QKD）领域：**依托头部运营商城市级量子城域网建设，骨干链路加密能力已实现重点城市覆盖、跨域互联试点，处于基础设施规模化部署初期，核心价值聚焦高安全等级场景物理层防护。
- **后量子密码（PQC）领域：**NIST 标准算法定型后，算法优化、硬件适配、产品迭代全面提速，国密与 PQC 融合方案逐步成熟，处于全面替代前夜、工程化适配攻坚期，核心目标是兼容存量体系、降低迁移门槛。
- **量子随机数（QRNG）领域：**芯片技术成熟、成本持续下探，已在加密设备、终端安全产品中规模化集成，处于普惠化应用普及期，为全链路加密提供高熵真随机熵源支撑。

表：抗量子安全产业阶段定位与特征对比

技术领域	当前发展阶段	核心特征	典型应用场景
量子通信保密（QKD 技术支撑）	基础设施规模化部署初期	骨干网覆盖、跨域互联试点、物理层高安全、成本偏高	金融骨干专线、能源调度网、政务涉密链路
后量子密码（PQC）	全面替代前夜、工程化适配攻坚期	标准定型、国密融合、算法优化、硬件加速适配	数据中心加密、跨域数据共享、工控旁路加固
量子随机数（QRNG）	普惠化应用普及期	芯片成熟、成本下探、高熵真随机、终端规模化集成	加密设备熵源、量子密讯、身份认证、终端加密

4.1.2 工程化落地核心逻辑：双轨并行、分层适配、能力下沉、生态闭环

结合金融、运营商、能源、政务四大行业差异化迁移实践，抗量子安全工程化落地需遵循双轨并行、分层适配、能力下沉、生态闭环四大核心逻辑，平衡安全强度、性能约束、改造成本与迁移风险，适配全行业异构存量、复杂场景的共性需求。

- **双轨并行：**是以 QKD 技术体系为支撑的量子通信保密提供物理层绝对安全、以 PQC 技术体系为支撑的后量子密码选型提供算法层抗量子安全，落地实践中还需叠加国密算法保障合规兼容，以此形成“物理安全+算法安全+兼容安全”三位一体混合架构，是当前过渡期唯一可行、最优的实施路径。
- **分层适配：**按网络层级与场景特性差异化配置安全能力，骨干层采用“QKD+PQC 融合加密”保障跨域高安全传输，接入层部署“轻量化 PQC 网关”适配广域异构网络，终端层集成“量子随机数+极简加密模块”适配移动、工控、边缘等末梢场景，实现安全强度与性能约束的精准匹配。
- **能力下沉：**依托运营商骨干量子基础设施、厂商轻量化产品方案，推动抗量子安全能力从核心骨干网、大型数据中心，向工业控制终端、移动办公设备、偏远边缘节点延伸，破解末梢安全短板，构建端到端全链路防护体系。

- **生态闭环：**构建“量子技术提供商/算法提供者→量子安全设备制造商/芯片制造商→网安/密安厂商/运营商→行业用户→运维服务商”全链路协同生态，打通技术与算法的创新研发、设备与芯片及产品制造、方案集成、场景落地、运维保障各环节，形成技术与算法-芯片与产品-方案与应用-实施与运维的正向循环，支撑规模化、可持续落地。

表：抗量子安全工程化落地核心逻辑框架

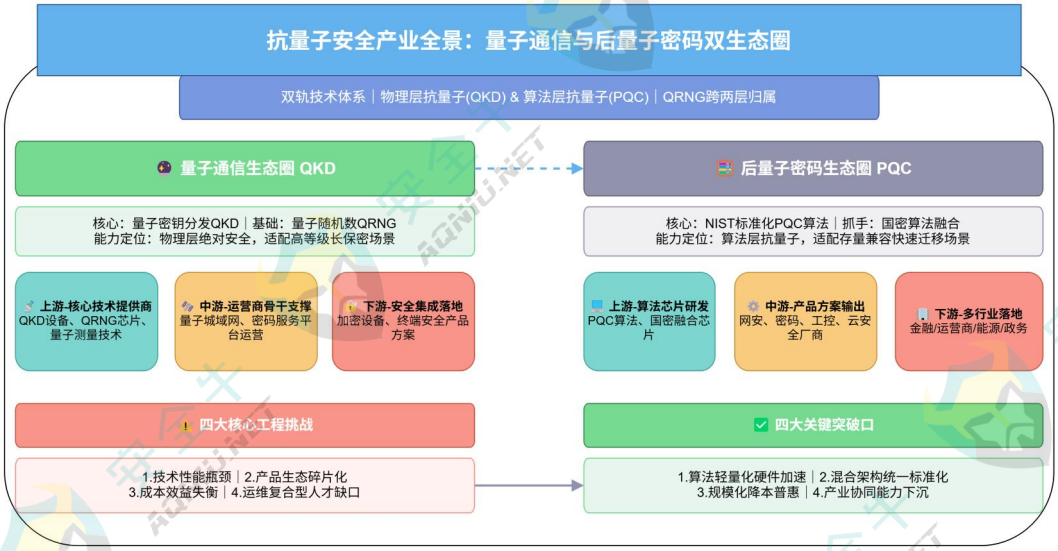
核心逻辑	核心内涵	关键作用
双轨并行	量子通信保密（物理安全）+ 后量子密码（算法安全）+ 国密（合规兼容）	构建三位一体混合架构，平衡安全、合规与兼容
分层适配	骨干层融合加密、接入层轻量化 PQC、终端层极简加密	匹配不同层级性能约束，实现安全-性能最优解
能力下沉	量子安全从骨干网、数据中心向工控/移动/边缘终端延伸	补齐末梢安全短板，构建端到端全链路防护
生态闭环	技术/算法-芯片/产品-方案/应用-实施/运维全链路协同	打通产业环节，支撑规模化、可持续落地

4.2 抗量子安全产业全景：量子通信与后量子密码双生态圈

伴随 QKD 和 PQC 双轨并行技术体系的发展，国内抗量子安全产业逐步形成量子通信和后量子密码两大并行互补的生态圈，分别对应“物理层抗量子”与“算法层抗量子”两条技术主线（量子随机数从源头供给维度常被划归在物理层抗量子的 QKD 生态圈，但从落地应用维度又常被划归在算法层抗量子的 PQC 生态圈）。

两大生态圈相互渗透、协同演进，构建起从上游核心技术提供（如 PQC 算法、量子技术、芯片技术）、中游设备制造（如支持 PQC 算法的网络安全设备、支持 PQC 算法的密码产品、支持 QKD 的网络传输设备、支持 QRNG 的装置器），到下游行业应用（如运营商 QKD 骨干网、金融 PQC 数据加密、政务 QRNG 密钥）的完整产业链条。

本节将分别解构两大生态圈的层级结构、核心主体与能力定位，厘清上下游分工与价值传递路径，为后续分析产业挑战、标杆能力与短板方向提供全景框架。



4.2.1 量子通信生态圈：硬核技术、骨干支撑与终端赋能

量子通信生态圈以量子密钥分发（QKD） 为核心、量子随机数（QRNG）为基础，形成“上游核心器件—中游网络运营—下游安全集成”的垂直产业链条，侧重提供物理层抗量子绝对安全能力，支撑高等级、长保密周期场景。

（一）上游：量子通信核心技术提供商

上游聚焦量子信号生成、传输、处理的硬核技术，是整个生态圈的能力源头。

- QKD 设备商：提供量子发射/接收终端、量子密钥管理系统（QKMS）、量子密钥分发网络设备，核心能力是产生、分发、管理无条件安全的量子密钥，支撑骨干链路加密。
- 量子随机数（QRNG）芯片商：提供基于量子物理特性的高熵随机数芯片/模块，作为加密设备、身份认证、密钥生成的底层熵源，支撑终端与边缘节点安全。
- 量子测量技术商：提供量子传感、高精度监测设备，延伸至能源、水利、交通等关键设施的物理安全监测场景。

（二）中游：运营商骨干链路硬核支撑

中游以头部运营商为核心，承担量子基础设施建设、运营与开放服务职能，是量子安全能力规模化扩散的关键枢纽。

- 量子城域网建设运营：电信、移动等运营商布局城市级量子城域网，构建骨干量子密钥分发网络，为金融、能源、政务等行业提供量子加密专线、5G 量子专网等规模化服务。
- 量子密码服务平台：整合量子密钥、国密算法、轻量 PQC 能力，向行业客户输出轻量化、可定制的量子安全服务，降低接入门槛。

（三）下游：网安与密安厂商量子能力安全集成

下游面向行业场景，由网络安全、密码安全厂商完成量子能力与现有安全体系的融合集成，输出可落地的产品与方案。

- 加密设备厂商：推出量子加密认证网关、量子加密一体机、国密-量子融合加密机，适配政企骨干网、数据中心、跨域传输场景。
- 终端安全厂商：研发量子密讯、量子超级 SIM、量子加密终端、量子安全模块，覆盖移动办公、应急指挥、现场作业等末梢场景。

表：量子通信生态圈产业链层级与核心能力

产业链层级	核心主体	核心产品/服务	核心能力	典型应用
上游（核心技术）	QKD 设备商、QRNG 芯片商、量子测量商	QKD 终端、密钥管理系统、QRNG 芯片、量子传感器	量子密钥生成分发、高熵随机熵源、高精度物理监测	骨干链路加密、终端熵源、设施监测
中游（网络运营）	电信、移动等头部运营商	量子城域网、量子加密专线、5G 量子专网、量子密码服务	量子基础设施建设、密钥服务开放、规模化接入支撑	金融专线、能源调度网、政务涉密网
下游（安全集成）	网安/密安厂商、终端安全厂商	量子加密网关、一体机、量子密讯、量子超级 SIM	量子能力融合、场景化方案输出、终端安全赋能	数据中心、移动办公、应急指挥

4.2.2 后量子密码（PQC）生态圈：芯片驱动、方案输出与行业落地

后量子密码生态圈以 NIST 标准化 PQC 算法为核心、国密融合为抓手，形成“上游算法芯片—中游安全方案—下游行业落地”的产业链条，侧重提供算法层抗量子安全能力，适配全场景、存量兼容、快速迁移需求。

（一）上游：高性能密码芯片与算法提供商

上游聚焦 PQC 算法研发、硬件化实现与国密融合，是 PQC 规模化落地的性能基础。

- PQC 算法研发商：深耕 ML-KEM、CRYSTALS-Kyber 等 NIST 标准算法，开展轻量化优化、效率提升、侧信道防护研究，适配不同算力终端。
- 国密+PQC 融合芯片商：研发支持国密、PQC 双栈的安全芯片、密码卡、硬件安全模块（HSM），实现算法硬件加速、密钥安全存储，兼容存量国密体系。

（二）中游：网安与密安厂商产品方案输出

中游以专业密码、网安厂商为主体，将 PQC 算法与硬件能力封装为标准化、场景化产品方案，适配不同行业。

- 密码基础设施及网络安全厂商：推出 PQC 安全网关、加密机、VPN、身份认证系统、密钥管理平台，支撑数据中心、跨域共享、云加密场景。

- 工控安全厂商：提供轻量化 PQC 加密模块、旁路加密设备、协议适配插件，适配能源、工业控制的实时性、弱网、老旧设备场景。
- 云安全厂商：构建 PQC 云加密服务、云密钥管理、数据脱敏方案，支撑政务云、金融云、行业云的数据安全防护。

（三）下游：行业应用集成与落地

下游由金融、运营商、能源、政务等行业用户主导，完成 PQC 方案与业务系统的集成适配，实现场景化落地。

- 金融行业：核心交易清算、跨境结算、客户数据、电子签章系统 PQC 改造。
- 能源行业：电网调度指令、炼化工艺参数、水电监控数据、工控网络 PQC 加固。
- 政务行业：政务云、跨域数据共享、电子证照、涉密办公系统 PQC 升级。
- 运营商行业：骨干传输网、政企专线、5G 基站、边缘节点 PQC 适配。

表：后量子密码（PQC）生态圈产业链层级与核心能力

产业链层级	核心主体	核心产品/服务	核心能力	典型应用
上游（算法芯片）	PQC 算法商、国密+PQC 芯片商	标准 PQC 算法、轻量化算法库、双栈安全芯片、HSM	算法优化、硬件加速、国密兼容、密钥安全	加密设备、终端芯片、工控模块
中游（方案输出）	密码/网安厂商、工控安全厂商、云安全厂商	PQC 加密认证网关、加密机、VPN、轻量化模块、云加密服务	场景化适配、协议兼容、旁路部署、存量集成	数据中心、工控网络、政务云、跨域共享
下游（行业落地）	金融、能源、政务、运营商行业客户	业务系统 PQC 改造、数据加密、身份认证升级	业务适配、安全集成、运行维护、风险管控	交易清算、调度指令、电子证照、骨干传输

4.3 工程化落地核心挑战与突破口

从产业全景看，量子通信与后量子密码双生态圈已初步成型，但从试点走向规模化工程化落地，仍面临技术性能、产品生态、成本效益、运维能力四大系统性挑战。这些挑战相互交织、层层传导，直接制约抗量子安全在关键行业的普及速度与覆盖广度。本节将从技术、产品、成本、运维四个维度提炼核心挑战，并对应提出可落地、可验证、可推广的关键突破口，为产业规模化推进提供精准路径指引。

4.3.1 四大核心工程挑战

（一）技术性能瓶颈：算法开销高、量子能力受限

- 后量子密码（PQC）算法复杂度显著高于传统密码，存在密钥尺寸大、报文膨胀、运算时延增加、CPU/内存开销上升等问题，对金融高频交易、能源工控毫秒级控制、运营商高并发转发、政务普惠服务造成直接

性能压力。

- 量子通信（QKD）受物理原理限制，传输距离、成码率、环境适应性存在天然上限，极端工业环境、弱网场景下稳定性不足；
- 量子随机数（QRNG）高端芯片成本高、功耗大，难以大规模下沉至边缘终端。

（二）产品生态碎片化：标准不统一、互操作难、适配滞后

当前抗量子安全产品体系处于多标准并行、多厂商异构、多协议混杂阶段，NIST PQC 算法与国密融合标准尚未完全统一，跨厂商、跨代际设备密钥互认、协议兼容、算法协同能力不足。

- 存量系统架构复杂、协议异构、更新周期长，大规模硬件替换不可行、轻量化适配方案不完善；
- 终端生态碎片化严重，工控终端、移动终端、边缘设备算力差异大，PQC 与量子能力适配参差不齐，端到端全链路产品覆盖不足。

（三）成本与效益失衡：投入门槛高、普惠场景性价比低

量子通信设备、高端 QRNG 芯片、PQC 硬件加速模块研发与制造成本偏高，导致量子加密专线、一体化加密设备部署成本居高不下，中小机构、普惠场景投入意愿低。

- 高安全等级场景（金融清算、能源调度、政务涉密）价值凸显，但占比低、规模有限，难以摊薄产业研发与量产成本；
- 边缘末梢、海量终端场景安全需求迫切，但成本敏感、预算有限，形成“高安全场景用得起、普惠场景用不起”的失衡格局，制约规模化推广。

（四）运维与人才缺口：复合型人才稀缺、运维体系不完善

抗量子安全融合量子物理、密码学、网络安全、工业控制、云平台、行业场景等多领域知识，既懂量子技术、又通行业业务、还熟安全运维的复合型人才极度稀缺，成为产业落地的关键短板。

- 现有运维体系基于传统密码与网络安全构建，缺乏量子密钥管理、PQC 算法运维、混合架构故障排查的标准化流程；
- 行业客户安全意识不足，对量子威胁认知薄弱，重部署、轻运维、弱管理现象普遍，导致设备利用率低、安全效能打折扣。

4.3.2 四大关键突破口

（一）算法轻量化与硬件加速：平衡安全与性能

- **聚焦 PQC 算法轻量化优化：**
  - ✧ 优先选用 ML-KEM 等低时延、高吞吐算法，压缩密钥尺寸、简化运算流程，适配低算力终端；
  - ✧ 研发专用 ASIC/FPGA 加速芯片，实现 PQC 算法硬件化，大幅降低 CPU 开销、缩短运算时延。
- 推进量子设备小型化、低功耗、宽温适配，优化 QKD 成码率、传输稳定性，提升极端环境适应性；

- 量产低成本 QRNG 芯片，推动量子随机数能力下沉至边缘、移动终端，夯实底层熵源安全。

（二）混合架构标准化与互操作：打通产业壁垒

- 加快制定“国密+PQC+量子融合”落地的标准指引，明确算法选型、密钥格式、协议接口、互认规则，消除标准碎片化。
- 建立跨厂商联合测试验证平台，统一密钥互认、协议兼容、算法协同规范，推动量子城域网、PQC 设备、加密网关互联互通。
- 推行分层分级适配标准，骨干层、接入层、终端层差异化配置安全能力，形成“骨干强安全、接入中安全、终端轻安全”的标准化方案，降低存量系统适配难度。

（三）成本下降与规模化普惠：释放规模效应

- 推动量子设备、PQC 芯片国产化替代与规模化量产，突破核心器件技术瓶颈，降低研发与制造成本；依托运营商量子基础设施共建共享模式，开放量子城域网、密码服务平台能力，降低行业客户接入门槛。
- 实施场景化分级定价，高安全场景保障收益、普惠场景薄利多销，平衡成本与效益；优先在金融、能源、政务等高价值场景规模化部署，形成标杆效应后逐步向普惠场景延伸，摊薄产业成本、提升性价比。

（四）生态协同与能力下沉：夯实落地基础

- 构建产业链联合攻关机制，联合技术厂商、芯片企业、网安厂商、行业客户，聚焦轻量化适配、硬件加速、互操作等共性瓶颈协同研发；共建行业级测试验证与培训平台，提供方案验证、人员培训、运维指导服务，补齐人才短板。
- 推进安全能力下沉，依托运营商、头部厂商输出轻量化、低门槛、易运维的标准化方案，适配基层政务、中小金融机构、边缘工业场景；完善混合架构运维体系，制定量子密钥管理、PQC 算法运维、故障排查的标准化流程，提升运维效率、保障安全效能。

表：工程化落地核心挑战与突破口对照

核心挑战	关键成因	核心突破口	预期成效
技术性能瓶颈	PQC 算法开销大、量子设备物理限制、QRNG 成本高	算法轻量化、硬件加速、量子设备小型化、低成本 QRNG 量产	性能损耗可控、极端环境适配、终端熵源普惠
产品生态碎片化	标准不统一、跨厂商互操作难、存量适配滞后	混合架构标准化、联合测试验证、分层分级适配	设备互联互通、存量兼容提升、端到端覆盖完善
成本效益失衡	量子/PQC 设备成本高、普惠场景预算有限、规模效应不足	国产化量产、基础设施共享、分级定价、高价值场景先行	成本持续下探、性价比提升、规模化推广加速
运维人才缺口	复合型人才稀缺、运维体系不完善、客户意识薄弱	产业链协同攻关、培训平台建设、运维流程标准化	人才供给充足、运维效率提升、安全效能最大化

4.4 产业亮点能力与特色厂商佐证

随着抗量子安全产业进入工程化落地关键期，产业链各环节涌现出一批具备核心技术、成熟产品与规模化落地能力的标杆厂商。它们在量子通信基础设施、QKD+PQC 融合体系、后量子密码芯片与网关、量子随机数应用等领域形成亮点能力，既验证了技术可行性，也为行业提供了规模化商业应用的落地范式。本节选取量子通信、后量子密码、跨界芯片三大领域的代表性厂商，从核心能力、标杆产品、典型案例三个维度进行佐证，展现产业供给侧的成熟度与创新力。

4.4.1 量子通信生态圈特色厂商（基础设施+融合能力）

（一）中国电信：全国量子安全基础设施与“量子+”全场景赋能能力

- **核心能力：**打造“一网、一池、一平台”量子安全基础设施底座；构建融合 QKD 和 PQC 的分布式密码体系，实现密钥生成、分发、供给全链路抗量子攻击；采用量子网络层、密码服务层、应用接入层、运营监管层四层架构；具备集中式密钥中继、动态密钥调度、高并发高可靠密钥服务能力。
- **标杆产品：**天翼量子密信、量子密话、量子云印章、量子加密对讲、OTN 量子加密专线、抗量子密改系列产品。
- **建设进展：**2024 年启动建设；2025 年 5 月在北京、上海、合肥节点验证发布；已在 40 个重点城市规模化建设，覆盖 31 个省；申请核心专利 30 余项，主导/参与 10 余项行业标准，密码产品获 CNAS 认证并完成信创适配。
- **典型案例：**服务湖南“湘办通”政务平台、福建漳州智慧城市、河北“量子安全和美乡村”、中车量子轨道网络、辽宁地震局防灾工程、民航空管量子专线；支撑奥运会、全运会等重大活动通信保密保障，用户规模突破 680 万

（二）中国移动：量子通信国家队主力军、通量一体与 PQC 融合能力

- **核心能力：**自 2019 年前瞻布局量子科技，践行筑基、融合、赋能三大使命，聚焦融入国家大局、科研攻关、设施建设、打造产品、引领生态五大主线；突破量子密钥“随用充注”、通量一体核心技术；构建 QKD 与

PQC 融合后量子密码体系，提出自主可靠+弹性兼容抗量子安全韧性网络架构。

- **标杆产品：**量子密话、量子密讯、量子对讲、小型化后量子密码芯片、量子超级 SIM 卡；投产量子密码服务平台；发布通量一体板卡及设备。
- **建设进展：**启动“点亮百城”量子试验网，推进超 10 个省量子基础设施建设；成立量子生态联盟，联合十余家核心企业覆盖全产业链；与国科量子合资成立信通数智量子科技有限公司；发布《通量一体技术白皮书》《抗量子密码敏捷技术白皮书》《抗量子密码迁移白皮书》。
- **典型案例：**量子产品赋能政务、司法、公安等超 10 个领域，服务用户规模超百万；在安徽完成国内通量一体现网试验。

（三）国盾量子：QKD 核心设备龙头、量子保密通信基础设施主力

- **核心定位：**全球领先的量子通信设备制造商与量子安全解决方案供应商，专注 QKD 设备自主研制与迭代，支撑“天地一体、自主可靠”量子保密通信网络建设。
- **核心产品（QKD 系列）：**基于诱骗态 BB84 协议，具备信息论安全性，可抵御量子计算攻击；产品 1U 机架尺寸、支持百公里级密钥分发，核心指标国际领先。
  - ✧ 安全性高：基于物理原理抗截获、窃听、破译，提供信息论安全；
  - ✧ 技术领先：核心指标国际领先，量子通信同族专利全球第一；
  - ✧ 权威认证：2021 年小型化 QKD 产品首个获国密局商用密码检测报告，全系列设备合规；
  - ✧ 自主可靠：突破单激光器量子态调制等关键技术，核心器件全国产化；
  - ✧ 广泛部署：服务政务、金融、电力、电信等行业，覆盖京沪干线、国家广域骨干网，部署超 15000 公里量子保密通信网络，支撑国内超 90%量子通信网络建设。
  - ✧ 关键技术突破（量子-经典共纤传输）：联合中国电信研究院首创空芯光纤量子-经典联合优化方案。
- **技术与应用布局：**覆盖点对点 QKD、QKD+PQC 融合、经典-量子共纤传输、基于纠缠城域量子网络；产品成码率、功耗等核心指标国际领先，适配城域/城际/特殊信道场景。

4.4.2 后量子密码生态圈标杆厂商（密码+网安）

（一）密码类——三未信安：后量子密码领域基础设施级核心供应商

- **核心定位：**以自研芯片为根基，打造全栈式后量子密码产品体系，定位为行业密码体系平滑过渡至抗量子时代的总建筑师与核心供应商，致力于成为后量子密码领域基础设施级服务商。
- **整体布局：**搭建从底层密码芯片到上层密码系统的全产业链产品架构，产品全面兼容国密全系列算法与 NIST 国际标准后量子密码算法；2024 年率先发布《抗量子密码技术与应用白皮书》，输出行业实践经验；获批组建后量子密码技术与应用北京市重点实验室，依托科研平台开展核心技术攻关与人才培育。
- **主力产品与方案：**拥有后量子密码芯片、SDK、UKEY、密码板卡、密码机、安全网关、密钥管理系统等全品类软硬件产品；全面支持 KYBER、DILITHIUM、FALCON、SPHINCS+四类 NIST 标准算法；自研抗量子

TLS 协议，兼顾通信安全防护与现有网络协议兼容适配；推出抗量子高性能密码芯片，搭载可重构密码引擎，实现高吞吐多算法并行运算。

- **核心业务能力：**具备抗量子密钥全生命周期管理能力，配备标准化密码接口，可无缝对接各类存量业务系统；依托实验室平台，聚焦算法轻量化优化、可重构密码芯片研发等关键技术突破，深度参与各级标准编制，推进产学研协同创新；推动技术成果在金融、能源、通信等重点行业落地转化，助力各领域完成密码体系安全升级。

（二）密码类——格尔软件：场景化后量子密码服务商与平滑迁移方案提供商

- **核心技术：**掌握 PQC 核心算法技术，采用“商密+后量子密码”平滑迁移路径，实现业务无感知升级，抵御“先存后解”量子威胁；支持接入 QKD 系统，构建“PQC+QKD”立体防御架构，并支持引入量子随机数源提升密钥通信安全性。
- **产品体系：**搭建密码机、PKI/CA、密钥管理、安全网关等全栈量子安全产品矩阵，覆盖网络、数据、数字信任全场景，其后量子密码解决方案获评行业年度优秀解决方案。
- **灵活部署模式：**支持传统商密、混合加密、纯抗量子三种运行模式，可按需切换，无需重构存量业务，实现分步式安全升级。
- **全链路加固：**完成通信协议适配、存储密钥增强、身份认证双算法证书部署，实现全链路抗量子防护。
- **实测性能：**经国泰海通证券真实场景验证，ML-KEM-768 封装超 80 万次/秒、解封装超 62 万次/秒，适配金融高频低时延业务。
- **生态落地：**联合海光信息、国泰海通证券打造“芯-端-用”全栈迁移方案，形成可复用的关基行业落地范式，深度参与后量子密码标准制定，具备双重工程验证能力。

（三）网络安全类——电科网安：“量铠”构建层次化抗量子安全体系

- **核心理念：**提出敏捷层次化后量子密码迁移体系思路，围绕威胁识别、指标搭建、方案设计、试点验证形成完整落地思路，积极应对量子回溯攻击风险。
- **主力产品：**打造量铠后量子密码全系列产品，覆盖算法、协议、芯片、模块、设备及系统，自研后量子密码算法并融合国密技术实现混合加密；搭载芯片可重构、软硬件协同架构，可灵活调配算法与安全强度，部署适配性强。
- **融合应用：**实现 PQC 与 QKD 技术融合落地，助力相关行业后量子密码敏捷技术白皮书编制，产品已落地政务、电力、通信、医疗等多个行业。
- **配套安全方案：**推出“衡”系列一体化安全解决方案，包含界衡、流衡、钥衡三大组件，分别负责网络安全运营、数据安全管控、云上统一密码服务，三道防线协同形成全域体系化安全防护能力。
- **终端与协同产品：**推出量子安全手机、量子 VoLTE 密话、橙讯抗量子即时通讯协作平台，补齐终端侧量子安全应用场景。
- **发展方向：**持续攻坚抗量子核心技术，迭代完善全谱系抗量子产品，搭建一体化量子安全支撑体系，护航

网络空间与数字经济安全发展。

（四）网络安全类——山石网科：网络安全设备领域抗量子安全能力落地先行者

- **布局初衷：**针对政务、金融、能源等行业十年以上长周期数据保密需求，提前布局后量子密码能力，防范数据留存后遭量子算力回溯破解风险。
- **产品落地：**率先在下一代防火墙产品中完成 FIPS 203、204、205 首批 NIST 后量子密码国际标准工程化适配，覆盖密钥交换、数字签名核心能力，应用于安全通信隧道、设备密钥协商、管控平面安全加固。
- **产品策略：**采取国际标准先行、国内标准紧跟思路，依托共通工程能力，待国内后量子密码标准发布后快速完成无感适配升级，无需更换硬件、重构现有网络。
- **技术优化：**通过算法与系统架构优化，平衡抗量子改造后的安全性、运行性能与业务兼容性，控制时延与算力损耗；自研 ASIC 芯片已规划下一代集成后量子算法，以此进一步提升运行效能。
- **长期规划：**在产品架构预留算法可插拔扩展空间，长远推动 PQC 与 QKD 两条技术路线融合应用，依托国产化设计优势，打造适配国内外双标准的长效网络安全防护方案。

4.4.3 跨界与创新生态圈标杆厂商（芯片+创新企业）

（一）芯片类——海光信息：芯片级内生抗量子安全底座服务商

- **联合成果：**携手格尔软件、国泰海通证券发布全球首个后量子密码平滑迁移解决方案，打造行业可复制落地范本。
- **架构模式：**采用“国密+后量子密码”双模并行混合架构，支持传统国密、混合加密、纯抗量子三种模式一键切换，保障核心业务平稳运行，实现无感升级过渡。
- **全链路加固：**将 ML-KEM768 算法嵌入通信握手、数据库存储流程，完成接入网关、数据加密、数字证书三大环节升级，实现传输、存储、身份认证全维度抗量子防护。
- **实测性能：**ML-KEM768 密钥封装 80 万次/秒、解封装超 62 万次/秒，可稳定承载 10000-30000TPS 高并发，业务平均时延 48-61ms，适配证券高频交易严苛场景。
- **硬件底层能力：**依托自主“CPU+DCU”双芯架构，融合密码、机密计算、可信计算等技术，从芯片指令集层面适配后量子密码算法，避免大规模硬件替换。
- **分阶段演进规划：**2025-2026 年完成主流 NIST 后量子密码算法生态适配落地；2027-2028 年推出抗量子 CCP 硬件与专用指令集，通过硬件加速释放芯片级抗量子算力。

（二）创新类——杭州量安科技：浙大系孵化 PQC 产业化科创标杆企业

- **企业背景：**由浙江大学、之江实验室联合孵化，核心团队集聚院士及国家级科研人才，深耕 AI 赋能抗量子安全领域，先后获评杭州准独角兽、浙江未来独角兽，2026 年入选中国未来独角兽榜单，为抗量子安全赛道唯一上榜企业。

- **科研实力**：牵头主持 1 项国家重点研发计划，参与多项国家级、省级重大科研项目；手握授权发明专利 17 项、受理发明专利 42 项、软件著作权 40 项，拥有高新技术企业、专精特新中小企业等多项资质，产品通过国密商用密码认证与信通院评测。
- **技术理念**：依托行业前沿趋势研判，明确后量子密码迁移已成为关基行业战略必需，主张 QKD 与 PQC 技术协同互补，共建全域抗量子安全防护体系。
- **核心业务**：主营后量子密码研发、高性能国密改造、智能安全三大业务，搭建自主可靠抗量子安全平台，相关技术方案已在金融、政务、工业、电力、军工、医疗等多行业完成落地验证。
- **行业影响力**：斩获日内瓦国际发明展金奖、科技创新一等奖等多项重磅行业奖项，立足浙江科创产业生态，持续加速技术成果产业化，助力打造区域抗量子安全产业高地。

（三）创新类——量安智联：原生融合架构抗量子创新型企业

- **战略定位**：布局北京国家级技术研发总部，聚焦攻坚抗量子安全领域关键核心技术，卡位万亿级抗量子安全市场，面向关基行业筑牢长效数字安全屏障。
- **核心技术架构**：首创“国密+抗量子”双引擎原生单栈架构，区别于传统叠加改造模式，支持算法热升级，无需更换硬件、不中断业务即可适配未来密码标准，大幅削减行业重复建设成本。
- **主力产品与性能**：推出国内首款原生双算法一体化安全网关，具备 2000Mbps 加密吞吐、5000 路并发用户承载能力，适配政务、金融、能源、工控等主流场景。
- **航天领域布局**：研发轻量化星载抗量子安全载荷，搭建星上加密、星地传输、地面解密端到端防护体系，防范低轨卫星通信数据截获后远期破译风险，赋能商业航天星座项目安全建设。
- **产业与资本发展**：立足长三角科创走廊夯实产业根基，积极对接科创板资本市场政策与融资渠道，借力资本加速技术迭代与场景落地；依托军创企业优势，搭建人才培育体系，拓展基层数字安全应用新模式。

表：抗量子安全产业链供给侧层级定位、核心能力、产品布局与应用场景对照

产业生态圈层	企业名称	圈层核心定位	核心技术能力	主力产品/解决方案	核心技术路线	典型落地场景	差异化核心优势
量子通信生态圈（基础设施层）	中国电信	国家级量子安全底座建设运营方	搭建“一网、一池、一平台”基础设施；四层架构体系；融合 QKD+PQC 分布式密码体系；动态密钥调度	天翼量子密信、量子密话、OTN 量子加密专线、量子云印章、抗量子密改方案	QKD 为主、PQC 为辅	数字政务、智慧城市、乡村治理、轨道交通、空管通信、重大活动安保	全国广域网络覆盖能力强，具备运营商级规建维优营完整体系，服务用户规模庞大
	中国移动	量子通信国家队主力军	突破通量一体、密钥随用充注技术；提出抗量子安全韧性网络架构；发布多项行业迁移白皮书	量子密讯、量子超级 SIM 卡、通量一体板卡、小型化后量子密码芯片	QKD 组网+轻量化 PQC 并行	政务、司法、公安基层场景	点亮百城试验网布局完善，生态联盟资源整合能力突出，侧重终端侧轻量化普及
	国盾	QKD 核心设	掌握诱骗态 BB84 协议	全系列商用 QKD	纯 QKD 物	国家广域骨干	QKD 设备市占率

产业生态圈层	企业名称	圈层核心定位	核心技术能力	主力产品/解决方案	核心技术路线	典型落地场景	差异化核心优势
	量子	备龙头制造商	核心技术；实现量子-经典共纤传输；核心器件全国产化	设备、量子密钥管理设备	理安全路线	网、京沪干线、各地量子城域网	领先，通过国密权威检测，远距离组网工程经验成熟
后量子密码生态圈-密码类（密码核心层）	三未信安	全栈后量子密码基础设施供应商	自研密码芯片技术；全品类 NIST 标准算法适配；牵头组建市级重点实验室	后量子密码芯片、密码板卡、安全网关、密钥管理系统、抗量子 TLS 协议	全场景 PQC 全算法覆盖	金融、能源、通信关键领域	从芯片到系统全产业链布局完备，率先发布行业技术应用白皮书
	格尔软件	密码平滑迁移方案领军者	精通 PQC 算法落地；商密 + 抗量子混合架构；完成高并发场景性能实测	后量子密码整体解决方案、双算法安全网关、统一身份认证体系	PQC 为主，可兼容接入 QKD	证券金融核心交易、大型政企涉密业务	三种加密模式灵活切换，联合芯片厂商实现芯端用全栈落地，实测性能数据完备
后量子密码生态圈-网安类（网络安全集成层）	电科网安	体系化量子安全综合服务商	提出敏捷层次化抗量子迁移思路；国密混合加密架构设计	量铠系列抗量子产品、量子安全终端、橙讯通讯平台、界衡/流衡/钥衡全域安全方案	PQC 融合传统安全运营体系	政务、电力、通信、医疗行业	兼具抗量子能力与全域网络数据安全运营能力，一体化防护体系完善
	山石网科	网络边界设备抗量子适配先行者	完成 NIST 国际标准工程化落地；预留算法可扩展架构	集成抗量子能力下一代防火墙、入侵防御设备	设备端嵌入 PQC 算法	政企数据中心、跨域网络边界防护	率先实现网安主流硬件产品标准化适配，兼顾性能与兼容性优化
跨界生态圈-芯片类（底层硬件支撑层）	海光信息	芯片级内生抗量子安全底座	CPU 底层指令集适配后量子密码算法；双芯内生安全架构；分阶段硬件加速规划	抗量子适配服务器 CPU、硬件协处理器、全栈平滑迁移方案	硬件底层赋能 PQC 算法	证券高频交易、大型算力中心	从硬件层面降低后量子密码算法性能损耗，为全行业迁移提供算力支撑
新锐创新生态圈-创新企业类（前沿突破层）	量安智联	原生架构抗量子创新企业	首创国密+抗量子单栈双引擎原生架构；实现算法热升级	原生融合一体化安全网关、轻量化星载安全载荷	原生双算法融合架构	工控、政务、商业航天星地传输	无需更换硬件完成迭代升级，大幅降低行业重复建设成本
	杭州量安科技	高校孵化 PQC 产业化科创企业	AI 赋能抗量子安全；多领域原创密码技术研发	自主可靠后量子密码平台、行业定制安全服务	PQC 产业化落地为主	电力、军工、医疗、政务多行业场景	科研底蕴雄厚，知识产权储备充足，多项权威奖项与官方资质加持

4.5 抗量子安全产业供给侧能力特征、成熟度研判与未来发展方向

历经多年技术攻关、产品迭代与场景试点落地，国内抗量子安全产业已形成量子通信、后量子密码、跨界芯片、新锐科创等多类型梯队，依托头部运营商、老牌密码厂商、主流网安企业、自研芯片厂商及高校孵化科创企业形成多元供给格局。

4.5.1 产业供给侧整体能力特征

（一）供给主体分层清晰，全产业链布局基本成型

当前国内抗量子安全产业供给侧已形成明确层级划分，分工清晰、协同互补。

- **第一层级为基础设施建设主体：**以中国电信、中国移动、国盾量子为代表，主攻全国性量子保密通信网络搭建、量子试验网布局、QKD 核心设备研发部署，主导天地一体量子通信底层网络底座建设，掌控量子密钥资源池、密码服务平台等核心公共基础设施，具备大规模组网与跨域密钥调度服务能力。
- **第二层级为商用密码核心供给主体：**以三未信安、格尔软件等密码企业为主，聚焦后量子密码全栈产品研发，覆盖底层密码芯片、密码板卡、密码机、密钥管理系统、PKI 基础设施等核心商用密码软硬件，主打传统密码体系向后量子密码平滑迁移方案，深耕金融、政务等高密级场景。
- **第三层级为网络安全集成应用主体：**以电科网安、山石网科等网络安全企业为代表，依托原有网络边界安全、数据安全、安全运营产品优势，将后量子密码能力融入防火墙、安全网关、即时通讯、全域安全运营体系，侧重现有网络架构无感适配，面向政企通用安全市场快速落地。
- **第四层级为底层算力硬件支撑主体：**以海光信息为代表，从 CPU 芯片底层切入，搭建内生安全硬件底座，通过指令集优化、协处理器硬件加速，解决后量子密码算法部署带来的性能损耗问题，为全行业密码升级提供硬件算力支撑。
- **第五层级为新锐科创创新主体：**以杭州量安科技、量安智联为代表，依托高校科研资源、原创架构技术实现差异化突破，聚焦原生融合架构、轻量化星载安全载荷、AI 赋能抗量子安全等创新方向，填补细分赛道技术空白。

表：国内抗量子安全产业供给主体层级分工对照

产业层级	核心定位	特色企业	核心能力	核心发展侧重
基础设施层	国家级量子网络底座搭建运营	中国电信、中国移动、国盾量子	建设广域量子通信网络、密钥资源池、运营监管平台	QKD 组网、天地一体网络布局、公共密钥服务输出
密码核心层	抗量子密码软硬件研发供给	三未信安、格尔软件	自研密码芯片、算法适配、全栈密码产品输出	PQC 算法落地、商密与抗量子融合、平滑迁移方案
网安集成层	现有安全体系抗量子赋能	电科网安、山石网科	边界安全、数据安全、安全运营产品升级	网络设备嵌入 PQC 能力、全域安全体系融合
硬件支撑层	芯片级底层安全算力赋能	海光信息	CPU 架构优化、指令集改造、硬件密码加速	从硬件层面降低抗量子算法性能损耗
新锐创新层	前沿架构与细分赛道突破	量安智联、杭州量安科技	原创架构研发、细分行业场景攻坚	原生融合架构、AI 赋能量子安全、航天场景落地

（二）技术路线双线并行，融合部署成为主流趋势

产业供给侧已全面形成“QKD 物理安全+PQC 算法安全”双线并行的技术供给格局，单一技术路线产品逐步向混合融合方案演进。

- 在量子通信路线上，头部企业已实现 QKD 设备小型化、国产化、共纤传输技术突破，可完成远距离稳定密钥分发，能够为政务、国防、重大活动等高安全场景提供物理层级绝对安全防护；
- 在后量子密码路线上，主流厂商产品已全面兼容 NIST 国际标准后量子密码算法，同时同步推进国产自主后量子密码算法适配，支持商密与后量子密码混合部署。
- 现阶段供给端不再局限单一技术输出，多数头部厂商均可提供“PQC+QKD”一体化融合解决方案，既满足日常业务轻量化抗量子防护需求，又可适配顶级涉密场景物理级安全需求，技术供给灵活性大幅提升。

表：产业主流抗量子安全技术路线应用特征对照

技术路线	核心安全原理	适用场景	主流应用企业	落地优势	现存局限
QKD 量子密钥分发	物理层防窃听、信息论安全	政务涉密、国防、空管、骨干专网	中国电信、中国移动、国盾量子	安全等级极高，抵御一切算力破解	部署成本高，依赖专用光纤，泛用性偏弱
PQC 后量子密码	数学难题抗量子破解	金融交易、政企内网、通用业务	三未信安、山石网科、海光信息	部署灵活、兼容现有网络、改造成本低	仅抵御算法破解，无物理传输防护
PQC+QKD 融合路线	物理安全 + 数学安全双重防护	高等级关基行业、大型集团全域防护	格尔软件、中国电信、电科网安	兼顾灵活部署与顶级安全，适配分层防护	方案架构复杂，统筹运维难度提升

（三）产品体系日趋完备，场景适配能力持续增强

经过持续迭代，国内抗量子安全产品已实现全品类覆盖，从底层硬件到上层应用形成完整产品矩阵。

- 硬件端涵盖后量子密码芯片、QKD 组网设备、安全网关、终端加密模块、量子超级 SIM 卡等；
- 软件端覆盖抗量子密钥管理平台、抗量子 TLS 协议、统一身份认证系统、安全运营平台等；
- 应用端形成量子密话、量子云印章、抗量子即时通讯、行业专用迁移方案等标准化落地产品。
- 同时产品场景化定制能力显著提升，可针对性适配金融高频交易、电力工控、轨道交通、空管通信、商业航天星地传输、基层政务治理等差异化场景，兼顾高并发、低时延、广覆盖、高涉密等不同业务运行要求，多款产品已完成真实业务环境压力实测，实战适配性得到验证。

（四）平滑迁移成为核心供给逻辑，兼容优先理念深入人心

当前供给侧企业均摒弃全面替换、推倒重建的激进升级思路，统一以存量兼容、无感升级、分步迭代作为产品研发与方案设计核心逻辑。主流方案普遍采用国密算法与后量子密码算法双模并行架构，支持多加密模式自由切换，在保障现有业务连续稳定运行的前提下，逐步完成安全能力升级。

多数厂商产品已预留算法可插拔、可扩展接口，既能快速适配现行国际标准，也可等待国内自主后量子密码标准正式落地后快速完成迭代适配，最大限度降低行业升级改造成本，避免重复建设。

（五）自主可靠水平稳步提升，国产化替代进程提速

供给侧核心技术自主化成效显著，国盾量子实现 QKD 核心器件全国产化；三未信安、海光信息等企业实现后量子密码芯片自主研发；格尔软件、杭州量安科技等深度参与国家后量子密码标准制定，掌握核心算法研发能力。

同时全系列产品陆续完成信创适配、国密局商用密码检测、信通院权威评测，国产自主可靠的抗量子安全产品已提前为具备同类进口产品能力做出前置充分准备，可全方位满足关键信息基础设施领域国产化安全建设要求。

4.5.2 当前产业整体成熟度研判

从技术成熟度、产品成熟度、落地成熟度三大维度综合来看，国内抗量子安全产业整体处于从试点示范迈向规模化商用的过渡成熟期。

（一）**技术层面：**核心底层技术已完成原理验证与工程化攻关，远距离 QKD 组网、后量子密码算法高性能适配、芯片级硬件加速、量子-经典共纤传输等关键技术均实现突破，主流技术路线稳定可靠，仅在轻量化极致功耗、超大规模并发调度、星地一体组网协同等细分领域仍存在优化空间。

（二）**产品层面：**标准化通用产品已趋于成熟，主流厂商标准化网关、密码卡、密钥管理平台等产品性能稳定、参数达标，且经过多行业项目落地验证；仅细分行业专用定制化产品、轻量化终端嵌入式产品仍处于持续优化阶段。

（三）**落地应用层面：**高安全价值场景落地成熟度最高，金融核心交易、国家级政务平台、能源骨干网络、

重大活动通信保密等场景已实现常态化部署；政企通用场景处于小规模试点推广阶段；面向海量民用终端、基层普惠场景的轻量化低成本解决方案尚未全面普及，整体呈现高端场景成熟、大众场景滞后的差异化成熟度格局。

整体而言，产业供给侧已经具备全面承接各行业抗量子安全升级需求的基础能力，能够支撑国家层面前瞻布局量子时代网络安全防线的整体战略部署。

表：抗量子安全产业各维度成熟度分级对照

研判维度	成熟等级	具体表现	企业实证依据
核心技术成熟度	较高成熟	远距离组网、共纤传输、硬件加速、高并发算法适配全部实现工程化落地	国盾量子共纤传输、海光芯片加速、格尔金融场景实测
标准化产品成熟度	基本成熟	通用安全网关、密码板卡、密钥管理平台可批量商用	三未信安、电科网安标准化产品完成多行业落地
行业应用成熟度	梯度分化成熟	高端关基场景成熟普及，通用场景试点，民用场景滞后	金融、政务落地成熟；中小微、物联网终端普及缓慢

4.5.3 产业现存核心发展挑战

（一）行业统一标准体系尚未完全落地，产品互通性不足

目前国内自主后量子密码正式标准仍处于编制推进阶段，行业内暂时以 NIST 国际标准作为主要落地依据，不同厂商算法适配规格、密钥格式、通信接口、加密协议存在细微差异，跨品牌、跨品类抗量子安全设备互联互通难度较大，极易形成产业技术孤岛，不利于全网统一抗量子安全体系搭建。

（二）高性能与低成本难以兼顾，下沉市场推广受限

高端抗量子组网设备、硬件加速密码芯片研发与量产成本偏高，面向大型政企、涉密机构的高价值场景接受度较高，但下沉至中小机构、基层治理、海量物联网终端等普惠场景时，部署成本偏高、投入产出比偏低，导致产业规模效应难以快速释放，整体市场下沉速度缓慢。同时后量子密码算法天然存在运算开销偏大问题，部分低端终端设备难以承载加密运算需求，性能与成本平衡难题依旧突出。

（三）行业认知参差不齐，主动升级意愿存在明显差距

现阶段仅金融、政务、国防、能源等关键领域充分认识到“先收集、后解密”量子回溯攻击风险，具备主动提前部署抗量子安全能力的意识；多数普通行业、中小企业对量子计算安全威胁认知不足，尚未将抗量子安全升级纳入网络安全建设规划，市场主动需求培育不足，多以政策驱动被动改造为主。

（四）复合型专业人才供给缺口较大

抗量子安全产业融合量子通信、商用密码、网络安全、芯片硬件、行业业务架构等多领域知识，既懂底层

量子技术、又精通商用密码应用、同时熟悉各行业业务流程的复合型技术人才、运维人才、方案设计人才数量严重不足，一定程度制约方案落地调试、后期运维与技术持续迭代效率。

（五）天地一体协同应用体系仍不完善

地面量子保密通信网络布局速度较快，但量子卫星、星地协同组网、星载轻量化抗量子安全载荷等空天领域配套产品与应用方案仍处于研发试点阶段，天地一体全域覆盖的抗量子安全网络尚未完全成型，远距离跨境、跨区域全域安全防护能力仍有待完善。

表：抗量子安全产业现存核心挑战对照

挑战分类	具体问题表现	成因来源（对应 4.4 企业现状）
标准体系挑战	国内自主标准未落地，厂商接口、协议不统一	目前全行以 NIST 标准过渡，各家算法适配规格存在差异
成本性能挑战	高端硬件造价高，算法算力开销大，下沉市场难普及	芯片、QKD 组网设备量产成本偏高，轻量化优化尚未普及
市场需求挑战	行业认知不均，仅高安全领域主动布局，其余依赖政策推动	多数企业未重视 “先存后解” 量子回溯攻击风险
人才资源挑战	跨领域复合型研发、实施、运维人才缺口大	产业高速扩张，量子、密码、网安、硬件交叉人才培育滞后
全域组网挑战	地面网络完善，星地一体协同应用体系尚不健全	地面量子网络布局快，星载轻量化安全产品仍处试点阶段

4.5.4 产业供给侧未来核心能力发展方向

（一）加速统一标准制定，构建全域互通产业生态

全力推进国内自主后量子密码算法、应用接口、密钥管理、安全检测等全维度行业标准落地，统一产品技术规范与互联互通协议；搭建国家级抗量子安全产品联合测试认证平台，打通不同厂商产品适配壁垒，实现量子网络、后量子密码设备、底层算力芯片之间无缝协同，构建统一开放、互联互通的全国抗量子安全产业生态。

（二）双向优化技术路径，平衡性能、功耗与部署成本

一方面持续推进后量子密码算法轻量化精简优化，降低算法运算时延与资源占用；另一方面扩大国产抗量子芯片、QKD 通用设备量产规模，依托规模化生产压缩硬件制造成本。同时大力推广原生融合架构、算法热升级等创新技术，减少行业改造重复投入，推出分层分级轻量化解决方案，兼顾高端涉密场景高安全需求与普惠场景低成本普及需求。

（三）深化多场景融合创新，拓宽产业应用边界

持续深化“量子通信+后量子密码+算力硬件”三者深度融合应用，重点发力商业航天星地安全传输、工业互联网工控加密、车联网通信安全、医疗数据隐私防护等新兴场景；依托运营商公共量子基础设施，开放轻量

化密钥服务能力，降低中小客户接入门槛，推动抗量子安全能力从核心关基行业向全行业数字化场景全面渗透。

（四）完善人才培育体系，夯实产业发展人才底座

推动高校增设后量子密码、抗量子安全相关专业课程，依托企业研发中心、重点实验室、科创平台搭建产学研联合培养机制；面向行业推出系统化抗量子安全运维、方案设计、项目实施培训课程，快速补齐产业复合型人才缺口，同步完善行业从业能力评价体系。

（五）统筹天地一体布局，完善全域安全防护架构

持续扩大全国地面量子保密通信网络覆盖范围，同步加快量子卫星组网、星载抗量子安全载荷研发落地，完善星地密钥协同分发、远距离跨域加密传输技术体系，早日建成天地一体、自主可靠、全域覆盖的国家级抗量子安全防护基础设施，全面筑牢数字经济时代长效网络安全屏障。

（六）强化生态协同联动，完善全链条供给服务体系

进一步强化运营商、密码厂商、网安企业、芯片企业、科创团队之间产业链协同分工，明确上下游权责与技术对接标准；依托行业联盟、科创平台整合产业资源，联合打造行业通用落地范本与迁移实施指南，形成从底层硬件、中层密码服务/安全产品集成/算力芯片支撑、再到上层行业应用的全链条一体化供给服务能力，推动国内抗量子安全产业实现高质量规模化发展。

表：抗量子安全产业未来发展方向与落地依托对照

未来发展方向	核心建设内容	可依托企业现有能力基础
统一标准生态建设	推进国产密码标准落地，打通设备互通壁垒	格尔、三未信安、杭州量安深度参与标准研制经验
性能与成本双向优化	算法轻量化+硬件规模化降本，推出分层级方案	量安智联热升级架构、海光硬件加速技术
全场景生态拓展	向商业航天、工控、车联网、医疗等场景延伸	量安智联星载载荷、电科网安多行业落地经验
复合型人才体系搭建	产学研协同育人，完善行业培训体系	杭州量安浙大孵化科研平台、企业重点实验室资源
天地一体全域布局	统筹地面量子网 + 空间量子星座协同建设	中国电信天地一体规划、国盾量子星地通信技术
全产业链协同升级	理顺上下游分工，输出行业通用迁移范本	运营商+密码+网安+芯片企业现有协同合作模式

综上，本章围绕抗量子安全工程化落地的产业供给侧能力进行了详尽阐述：首先明确当前国内抗量子安全正处于从技术试点向工程化规模化应用过渡的关键发展阶段，形成了“双轨并行、分层适配、能力下沉、生态闭环”的核心落地特色；其次清晰划分了量子通信、后量子密码以及跨界与创新三大产业生态圈；同时对各生态圈特色企业的技术积累、产品布局、实测性能与行业落地案例等情况，完成了全维度产业能力验证，直观展现了当前各类市场主体的差异化竞争优势与产业化成效；最后系统研判了供给侧整体能力格局与产业成熟梯度，梳理出行业长期发展现存的挑战，锚定了后续产业能力迭代与整体升级的清晰方向。

通过本章的系统性分析，最终得出明确结论：国内抗量子安全产业已建成完备的多赛道产业生态，各类市

场主体技术储备充足、产品体系日趋完善，已基本具备大范围工程化部署的基础条件；但现阶段仍存在标准不统一、成本适配性不足、场景渗透不均等现实短板，整体应用呈现出“高端场景成熟、普惠场景滞后”的分化格局。后续需要依托既定落地准则，联动全产业链协同发力，补齐体系与应用层面的短板，持续优化技术架构与部署模式，才能稳步推动抗量子安全能力从试点示范走向全域规模化落地，为各类关键信息基础设施领域平稳完成密码体系迭代筑牢坚实的产业根基。

第五章 总结与趋势判断

经过前四章逐层递进的系统分析，本研究已依次完成四大核心板块研究：抗量子安全的发展背景梳理与技术边界界定、多元混合落地架构体系设计、四大重点行业落地实践复盘、产业供给侧整体能力全景研判，以此围绕量子威胁演变规律、技术协同实施框架、行业落地差异、产业生态现状，梳理出当前抗量子安全产业及工程化落地的基本发展脉络。本章将整合前述核心研判成果，凝练多维度核心结论，预判 2026 至 2030 年各应用领域密码迁移推进时序，剖析技术、产业、应用层面的长期演变走向，并结合现存短板提出分层落地行动建议，为抗量子安全工程化落地的整体推进提供重要指引。

5.1 抗量子安全产业及工程化落地的四维关键结论

（一）风险维度：量子威胁走向现实风险，布局抗量子安全具备极强战略与现实价值

(1) 量子算力突破催生实质性风险

随着量子计算技术迭代提速、实用化进程加快，传统密码算法赖以生存的数学安全壁垒已被打破，传统公钥密码体系正式进入高危风险窗口期。一方面，业务运行中数据存储、网络传输、身份认证等全链路环节产生的加密数据，普遍存在未来被量子算力批量破解的潜在隐患；另一方面，行业高度关注的“先存储、后破解”回溯攻击风险，已彻底脱离理论假想范畴，形成可落地、可预见的实质性安全威胁。

(2) 前置防护成为刚性建设要求

对于金融交易、涉密政务、能源管控等承载国家关键基础设施与高价值数据的核心领域而言，各类业务核心数据、涉密信息、生产管控信息的保密周期普遍长达十余年。相较于短期算力风险，长周期数据留存带来的远期破译风险更为致命。若行业未能提前完成抗量子防护体系升级，存量加密数据将长期暴露在量子攻击风险之下，极易引发核心数据泄露、业务数据篡改、关键业务中断等重大安全事件，直接动摇关键信息基础设施的稳定运行根基。在此背景下，主动前置布局抗量子安全防护，已经从行业前瞻性技术储备，转变为关键行业必须落地的刚性安全建设任务。

(3) 2026 年产业拐点到来

基于本研究研判，2025 年为量子密码产业化元年，在此之后，2026 年将成为抗量子安全产业重塑的元年，也是产业发展的核心拐点。该拐点不仅标志着产业发展阶段的迭代升级，更从应用实践和产业链生态维度实现了抗量子安全认知与建设体系的全面重构：行业认知已从过去“单点算法加固、局部技术防御”，正式升级为全业务、全周期、体系化、规模化统筹部署的抗量子风险治理工程。产业发展也彻底告别了零散试点、碎片化技术探索的初级阶段，正式迈入技术体系重构、标准推进落地与产业链生态融合的全新发展周期。

(4) 应对风险需要一系列系统迁移改造工程

同时全文研究进一步验证，抗量子安全改造绝非单一密码算法替换的简单技术迭代，而是覆盖业务资产、数据链路、密钥体系、运维机制的全局性系统工程。行业落地必须依托密码资产盘点、脆弱性评估基础，结合数据保密等级、业务运行特征与场景容错能力统筹规划，建立数据全生命周期量子风险管理机制，依据业务价值敏感度与风险等级分层排序，精准划定各领域、各场景抗量子迁移的建设优先级。

表：风险维度核心结论对照

风险维度要点	核心结论	核心启示
量子算力突破催生实质性风险	量子计算实用化提速，传统公钥密码安全壁垒失效，全业务加密链路存在远期批量破解风险，“先存储、后破解” 回溯攻击由理论变为现实威胁	全域存量加密数据均存在潜在风险，需树立全域风险防范思维
前置防护成为刚性建设要求	高价值关基行业数据保密周期长达十余年，远期破译危害远超短期风险，可直接威胁基础设施运行根基	抗量子防护由可选技术储备，转变为关键行业强制性安全建设任务
2026 年产业重塑拐点到来	2025 年为产业化元年，2026 年开启产业重塑拐点，行业认知从单点防御升级为体系化治理，产业告别零散试点进入规模化重构阶段	行业建设逻辑、生态模式、落地范式迎来全方位体系重塑
风险应对为系统性迁移工程	抗量子升级非简单算法替换，是覆盖资产、链路、密钥、运维的全链条系统工程，需基于风险评估分层划定改造优先级	必须依托资产盘点与脆弱性评估，分层、分周期、分优先级统筹落地

（二）顶层设计维度：抗量子安全技术架构与落地范式成型

(1) “PQC+量子赋能（QKD 和 QRNG）”多技术路线发展明确

国内抗量子安全体系已明确形成 QKD、PQC、QRNG 三类核心技术路线的研发与应用，其中 QKD 和 QRNG 都属于量子物理赋能的物理层安全技术，PQC 则属于算法层安全技术，但 PQC 的标准算法还尚未出台。三类技术依托自身技术原理、安全机制与演进路径，形成了清晰的差异化能力边界、技术特色与阶段成熟度。三类技术各司其职、各有优劣，形成了层次清晰、边界明确、成熟度分层的完整技术顶层体系。其中：

- QKD 量子密钥分发依托物理层安全机制，具备无条件安全优势，高安全等级属性突出，经过多年基建落地，技术体系最为成熟，主打核心涉密、关键基础设施等高可靠场景；
- PQC 后量子密码基于新型数学抗量子算法，部署灵活、适配性强，现阶段迭代速度最快，主打通用业务、

高并发、广域普及场景，是规模化迁移的核心主力；

- QRNG 量子随机数聚焦密码熵源补强，技术轻量化、适配性高，作为全域补位技术，为各类加密链路、终端设备提供真随机数支撑。。

(2) 确立分层选型适配逻辑，多技术组合架构形成标准化应用范式

基于三类技术路线的差异化特征，本研究明确了场景驱动、按需组合、分层适配的顶层技术选型逻辑，解决了单一技术无法适配全场景安全改造的核心难题。行业不再采用单一技术一刀切的改造模式，而是根据业务安全等级、并发压力、网络条件、终端形态、保密周期等多维要素，灵活搭配 QKD、PQC、QRNG 技术组合。该套顶层技术路线选型逻辑适配国内政企、关基、民用全场景生态，最终形成了国密打底、多技术协同、分层组合的中国特色抗量子安全混合落地方案。

- 高密级核心场景优先采用 QKD 物理安全兜底、PQC 算法应急补强的组合模式；
- 通用高并发场景以 PQC 算法替换为主体、QRNG 熵源增强为辅；
- 边缘物联网、轻量化终端场景采用“轻量 PQC 适配+QRNG 补位”的极简架构。

(3) 工程化落地框架体系完备，量化评价机制供参考

基于既定的顶层技术路线选型，当前抗量子安全产业界已联合开展抗量子迁移实践的行业用户，共同形成了从资产摸排到落地验收的全流程实施框架，构建出“密码资产盘点—量子脆弱性评估—分层算法适配—统一密钥管控”的现实工程实施体系。

依托顶层设计确立的场景划分标准，本研究提出极高安全、通用高并发、边缘物联网三类差异化落地范式，实现顶层架构与细分场景的精准匹配。同时配套构建了抗量子就绪度（PQR）量化评价体系与阶梯式成熟度模型，从顶层设计维度明确了迁移进度、建设质量、防护成效的判定标准，推动体系化改造从试点摸索转向标准化、可量化、可管控的规范落地模式。

(4) 密码敏捷架构顶层兜底，支撑全行业平滑迁移与长期迭代升级

为适配多技术路线混合架构的长期共存、分步迭代特征，顶层设计确立了密码敏捷性架构作为整体迁移底座。通过标准化算法接口、动态密钥调度、策略自适应调整的顶层机制设计，有效解决新旧体系兼容、多算法并行、业务不间断运行的核心难题，大幅缓解报文膨胀、算力开销、协议适配等工程化痛点。该顶层设计既保障了现阶段混合架构的平稳落地，也为未来技术迭代、标准升级、体系全域统一预留演进空间，是抗量子安全体系分层落地、有序迭代的核心顶层保障。

表：顶层设计维度核心结论对照

顶层设计维度要点	核心结论	核心启示
“PQC+量子赋能（QKD 和 QRNG）”多技术路线发展明确	国内抗量子安全顶层技术体系成型，形成 PQC 算法层技术、QKD&QRNG 量子物理层技术互补格局，三类技术差异化能力边界、特色与成熟度分层清晰。QKD 技术成熟度最高，适配高密级核心场景；PQC 迭代速度快、部署灵活，是规模化迁移主力；QRNG 轻量化适配性强，承担全域熵源补位作用，整体构建出层次完备的顶层技术体系。	摒弃单一技术路线思维，需基于各类技术的成熟度与能力边界，差异化匹配不同安全场景，构建多技术互补的顶层技术布局。
分层选型适配逻辑与混合应用范式成型	确立场景驱动、按需组合、分层适配的顶层选型逻辑，打破单一技术一刀切的改造模式。依据业务安全等级、并发压力、终端形态等多维要素，针对高密核心、通用高并发、边缘轻量化三类场景，形成专属多技术组合方案，最终落地为国密打底、多技术协同的中国特色混合架构范式。	全行业改造需坚持场景化按需适配原则，依托标准化技术组合模式，兼顾安全合规与业务适配性，适配国内全场景落地生态。
工程化落地框架与量化评价机制完备	行业形成“密码资产盘点—量子脆弱性评估—分层算法适配—统一密钥管控”全流程标准化工程实施体系，匹配三类差异化场景落地范式。同步构建 PQR 抗量子就绪度量化评价体系与成熟度模型，实现迁移进度、建设质量、防护成效的可量化、可管控、可验收。	抗量子迁移落地可依托标准化工程框架推进，通过量化评价体系规范建设标准，摆脱试点摸索的零散化建设状态。
密码敏捷架构支撑长期平滑迭代	以密码敏捷架构作为混合架构落地的核心顶层底座，通过标准化接口、动态密钥调度、自适应策略调整机制，有效解决新旧体系兼容、多算法并行、业务不间断运行难题，缓解各类工程化痛点，同时为后续技术迭代、标准升级、体系统一预留演进空间。	行业迁移为长期分步迭代工程，需依托敏捷架构兜底，保障现阶段平稳落地与未来体系可持续升级。

（三）行业实践维度：多行业落地共性与差异并存，分层适配、梯度推进验证成立

(1) 各领域落地节奏拉开差距，整体呈现梯队化推进格局

结合四大重点行业落地实践复盘内容，国内抗量子安全改造并未同步铺开，而是依托各行业自身安全诉求与建设基础形成明显推进梯队。

金融行业受强监管约束与高价值交易数据防护需求驱动，风险响应主动、项目投入充足，成为落地实践最早、改造成熟度最高、经验积累最丰富的标杆领域。运营商、能源、政务领域紧随其后，参照金融行业实践经验，结合自身业务属性逐步启动试点改造与存量优化工作，整体形成头部引领、多行业依次跟进的梯度发展态势。

(2) 各行业改造存在普遍共性，工程实践面临一致现实瓶颈

从实际落地反馈来看，不同行业在建设思路与实操难点上具备诸多共通特征。各领域均认可混合技术架构的防护价值，普遍采用国密算法结合抗量子技术的组合模式搭建防护体系。同时行业普遍遭遇共性工程难题，数据加密后报文体积膨胀、设备算力资源消耗上涨、老旧存量系统兼容难度偏大、终端设备品类碎片化等问题，成为制约改造效率的共同阻碍，也是各行业开展技术调优、方案优化的统一发力点。

(3) 业务约束催生路径分化，场景诉求决定技术选型差异

受行业运行规则、承载规模、现场环境等约束条件限制，各领域落地路径呈现显著差异化特征。金融聚焦高并发交易清算场景，侧重算法性能与交易连续性平衡；运营商立足广域承载网络，重点保障跨域组网安全与专线业务可信交互；能源行业兼顾工控实时性与极端环境适配，优先保障生产调度链路稳定；政务围绕跨域数据共享，着力满足分级管控与公众服务高可用要求。差异化的业务诉求，直接推动各行业在技术路线搭配、改造实施节奏、核心防护重心上形成清晰分野。

(4) 实践经验形成统一共识，分层协同模式适配规模化落地

经过多领域真实项目检验，各行业逐步沉淀出具备普适性的落地准则。分层分级匹配防护能力、灵活运用混合技术架构、保持密码策略动态可调、联动产业链各方协同作业，成为经受实战验证的核心推进思路。兼顾行业共性规律与自身差异化特征开展建设，既能规避重复试错成本，也可贴合业务实际运行要求，充分证明分层适配、梯度推进的落地模式，能够有效支撑全行业规模化改造工作有序开展。

表：行业实践维度核心结论对照

行业实践要点	核心结论	核心启示
各领域落地节奏拉开差距，整体呈现梯队化推进格局	国内重点行业抗量子安全改造非同步推进，形成清晰梯队化发展格局。金融行业依托强监管要求与高价值数据防护需求，落地最早、成熟度最高、实践经验最丰富，成为行业标杆；运营商、能源、政务行业紧随跟进，参照标杆经验结合自身业务稳步开展试点与存量优化，整体呈现头部引领、梯度推进的发展态势。	行业改造无需全域同步推进，可遵循标杆先行、分批跟进的节奏，依托成熟行业经验降低试错成本。
各行业改造存在普遍共性，工程实践面临一致现实瓶颈	各大行业落地建设具备高度共性，均普遍采用国密结合抗量子技术的混合防护架构，统一适配量子风险防护需求。同时全行业面临共性工程难题，加密报文膨胀、设备算力开销增加、老旧存量系统兼容难度高、终端设备碎片化突出，成为制约各行业改造落地的普遍瓶颈与优化重点。	需针对行业共性工程痛点开展通用技术调优与方案迭代，形成普适性改造规范，提升整体落地效率。
业务约束催生路径分化，场景诉求决定技术选型差异	受行业业务规则、运行场景、运维约束差异影响，各领域落地路径与防护重心形成明显分化。金融侧重高并发交易稳定性与连续性；运营商聚焦广域组网与跨域通信安全；能源兼顾工控实时性与极端环境适配；政务注重分级管控与跨域数据共享安全，场景差异化诉求直接决定各行业技术选型与改造节奏的差异化布局。	行业改造不可一刀切，需立足自身业务属性、场景诉求与运行约束，定制适配专属改造方案与防护重心。
实践经验形成统一共识，分层协同模式适配规模化落地	经过多行业真实项目实战验证，分层分级配置防护能力、灵活运用混合架构、动态调整密码策略、全产业链协同推进，成为行业普适性落地准则。兼顾行业共性规律与个性化差异开展建设，可有效适配各类场景需求，充分验证了分层适配、梯度推进模式可支撑全行业规模化改造落地。	全行业规模化迁移需坚持共性范式+个性适配相结合，依托实战验证的分层协同模式稳步推进全域改造。

（四）产业供给维度：量子通信和后量子密码两大生态圈为主，供给能力基本配齐

(1) 双生态圈格局成型，市场主体实现多元集聚

国内抗量子安全产业经过多年培育发展，已形成以量子通信、后量子密码两大核心生态圈为主，跨界芯片企业与创新型企业跟进参与的产业格局。两大生态圈汇聚了网络基建运营、密码技术研发、安全集成服务、芯片硬件制造以及前沿科创企业等各类市场主体，不同企业依托自身技术积淀与赛道优势，打造出定位各异的产品体系与行业解决方案，当前产业整体的市场主体结构已初具雏形，正处于蓬勃发展阶段。

(2) 产品服务体系基本完备，可全方位适配各层级落地需求

从产品与服务供给层面来看，当前行业整体供给体量初具规模，能够覆盖不同安全等级、不同规模体量的改造需求。量子通信生态圈可提供骨干密钥组网、高安全专线部署、全域密钥调度等基础设施类产品与配套服务；后量子密码生态圈可输出适配算法、加密芯片、终端安全模块、传输和认证安全网关以及全流程迁移方案，创新型企业也持续补齐边缘场景、轻量化应用的产品缺口，整体处于基本完备的产业链状态，不存在明显的供给断层与资源短缺问题。

(3) 产业处于规模化过渡阶段，现有工程落地能力基本成熟

对照产业所处发展阶段判断，目前行业正处在技术试点向规模化工程应用过渡的区间。现有技术储备、产品成熟度与项目实操经验，可以满足现阶段各行业中小规模落地建设的需求。但产业发展依旧存在客观短板，行业统一标准尚未完全落地，产品互通性有待提升，面向普惠场景的低成本方案供给偏少，兼具跨领域能力的专业人才储备不足，同时天地一体组网体系仍有优化空间，这些因素也在一定程度上约束着产业全域规模化普及的速度。

(4) 供给侧可匹配现阶段需求，后续迭代空间充足

结合市场应用反馈来看，产业供给端可以较好响应各行业现阶段的改造诉求，能够匹配试点探索、体系升级等不同建设阶段的使用场景。后续随着行业需求逐步释放，依托各生态圈的技术迭代与产品优化，产业供给实力还将持续提升，进一步适配更大范围的抗量子安全改造建设工作。

表：产业供给维度核心结论对照

产业链及产业供给要点	核心结论	核心启示
双生态圈格局成型，市场主体实现多元集聚	国内抗量子安全产业经过长期培育，已形成量子通信、后量子密码双核心生态圈主导，各类跨界企业、科创企业协同参与的成熟产业格局。产业集聚基建运营、密码研发、硬件制造、安全集成等多类型市场主体，各企业依托自身赛道优势与技术积淀，打造差异化产品体系与行业解决方案，整体市场主体架构成型，产业发展活力充足。	双生态协同发展格局已基本稳固，可依托多元化市场主体资源，支撑各类型行业项目落地建设。

产业链及产业供给要点	核心结论	核心启示
产品服务体系基本完备，可全方位适配各层级落地需求	当前产业产品与服务供给体系初具规模、覆盖全面，无明显供给断层与资源短缺问题。量子通信生态圈主打高安全基础设施与组网密钥服务，适配核心高密级场景；后量子密码生态圈输出算法、芯片、安全网关及全流程迁移方案，适配通用规模化场景；创新企业补齐轻量化、边缘场景产品短板，全方位覆盖不同安全等级、不同体量的行业改造需求。	现阶段产业供给能力充足，可精准匹配各行业试点改造、存量优化、体系升级的全层级落地需求。
产业处于规模化过渡阶段，现存部分发展短板约束全域普及	目前产业整体处于技术试点向规模化工程应用过渡的关键阶段，现有技术储备、产品成熟度与工程实操经验，可充分支撑中小规模项目落地。同时产业仍存在诸多短板，统一行业标准未完全落地、产品互通性不足、普惠型低成本方案稀缺、复合型专业人才缺口较大、天地一体组网体系不完善，诸多问题制约产业全域规模化普及进程。	产业规模化落地具备基础条件，但需针对性补齐标准、成本、人才、体系短板，破除全域推广约束。
供给侧适配现阶段需求，长期具备充足迭代升级空间	从市场反馈来看，当前产业供给能力可精准适配各行业现阶段试点探索、体系优化等阶段性建设诉求。伴随后续行业改造需求持续释放，依托双生态圈技术迭代、产品升级与方案优化，产业整体供给实力、适配能力、场景覆盖能力将持续提升，可逐步适配更大范围、更高标准的全域抗量子改造建设。	现阶段可依托现有供给体系稳步推进改造，长期可通过产业迭代持续完善供给能力，适配规模化、全域化行业发展需求。

5.2 中长期整体发展趋势

结合前文对量子安全风险特征、多技术顶层架构、重点行业落地规律、产业供给能力的系统性研究，以及5.1 各维度核心定论，可以预判，国内抗量子安全体系将进入技术持续迭代、产业日趋成熟、应用规范普及的中长期演进阶段。整体将摆脱零散试点、碎片化探索的初级发展形态，逐步走向标准化、规模化、体系化的成熟建设阶段，技术、产业、应用三大层面呈现清晰、稳健的中长期发展趋势。

（一）技术侧迭代趋势：轻量化、高算力加速、天地一体协同组网成演进主线

中长期来看，国内已定型的“PQC+QKD+QRNG”多技术路线协同架构将保持整体框架稳定，技术优化重

点从“路线探索”转向“工程适配与性能升级”。

(1) **一是算法轻量化迭代成为必然趋势。**现阶段抗量子算法普遍存在报文膨胀、算力开销偏大、终端适配性不足等工程短板，难以适配海量边缘终端与轻量化业务场景。后续行业将持续围绕算法精简、协议优化、压缩适配等方向迭代，逐步形成高安全、低开销、易部署的轻量化算法体系，大幅提升存量系统兼容能力与全场景适配能力。

(2) **二是硬件高算力加速体系持续完善。**伴随国产密码芯片、专用加速模组、量子硬件设备的迭代升级，硬件算力瓶颈将逐步突破。通过专用硬件赋能缓解通用设备算力压力，能够有效解决高并发业务时延高、加密运算负载大、终端算力不足等痛点，为规模化、全链路抗量子改造提供底层硬件支撑。

(3) **三是天地一体协同组网逐步成型。**现阶段抗量子防护多以地面专网、局域组网为主，覆盖范围与跨域协同能力有限。中长期将依托地面量子骨干网与卫星量子通信技术融合，逐步构建天地协同、全域覆盖、统一调度的立体组网体系，实现跨区域、跨层级、跨场景的密钥联动与安全协同，完善全域技术防护底座。

（二）产业侧发展趋势：标准互通、成本下行、全链协同推动产业成熟升级

基于当前双生态圈成型、市场主体集聚、供给能力基本配齐的产业现状，中长期产业将从试点过渡阶段全面转向规模化普及阶段，整体呈现标准化、低成本、高协同的发展趋势。

(1) **首先，行业标准将逐步统一互通。**当前国内外标准并行、行业规范不统一、产品互通性差的问题将持续改善。国内自主抗量子密码标准、迁移实施标准、测评认证标准将持续落地细化，同时兼顾国际标准兼容互通，逐步形成自主可控、内外兼容、统一规范的标准体系，解决方案不通用、产品难互联、验收不统一的产业痛点。

(2) **其次，部署成本将持续稳步下行。**随着技术迭代成熟、产品规模化量产、工程方案持续优化，早期试点阶段定制化程度高、设备成本高、改造成本昂贵的问题将逐步缓解。标准化通用方案、轻量化普惠产品持续丰富，产业整体建设门槛持续降低，推动抗量子安全从高等级核心场景，逐步向中小机构、民用终端等普惠场景延伸。

(3) **最后，全产业链将深度协同融合。**量子通信、后量子密码两大生态圈将从独立发展走向互补融合，基建运营、密码研发、硬件芯片、安全集成、测评服务、人才培养等上下游环节逐步形成闭环协同体系。产业链分工更加精细、供需匹配更加精准，逐步补齐人才短板、体系短板、服务短板，整体产业成熟度持续提升。

（三）落地应用趋势：分级常态化防护、无感迁移、全域联防逐步构建成型

结合各行业梯度推进、分层适配的落地实践规律，中长期行业应用将从试点零散改造转向常态化、体系化、全域化防护建设。

(1) **一是分级防护走向常态化、制度化。**行业应用将基于资产价值、数据密级、业务重要性，建立常态化量子风险评估与分层防护机制，将抗量子安全建设纳入常态化安全运维体系，告别阶段性、运动式改造，形成分级管控、动态更新、精准防护的常态化治理模式。

(2) **二是新旧体系实现无感平滑迁移。**依托密码敏捷架构的顶层设计，结合分层适配、梯度推进的成熟范式，后续行业迁移将以渐进式迭代为主，最大程度规避业务中断、系统重构、运行波动等改造风险，实现存量业务无感知升级、增量业务标准化部署，形成低风险、高适配、可持续的平滑迁移格局。

(3) **三是全域安全联防体系逐步落地。**各行业孤立建设、局部防护的现状将逐步打破，依托统一技术标准与协同机制，实现跨行业、跨领域、跨网络的安全态势联动、策略互通、资源共享，最终构建自主可控、全域覆盖、兼容互通的标准化抗量子全域安全防护体系。

5.3 分主体、创新 AI 及时间表落地行动建议

结合前文对抗量子安全多维度的现状以及对技术、产业、应用三大板块中长期演进趋势的剖析。现阶段行业应用侧普遍存在技术选型分散、标准体系碎片化、各领域落地节奏失衡、产品供需适配度不足、工程落地痛点突出等现实问题；长远来看，行业应用将朝着算法精简高效、产业标准统一互通、应用分级联防、体系自主可控的成熟形态演进。本节将分别面向行业用户、产业供给、产业主管三大主体制定落地举措，通过现阶段针对性补短板、强弱项，稳步推动行业形态向预期中长期发展目标过渡靠拢。

（一）行业用户主体

从现状层面来看，各领域改造大多处于零散试点阶段，整体建设缺乏统一规划，资产防护层级划分模糊，行业内部改造规范互不统一，尚未形成可复制推广的迁移模式，不同赛道建设进度差距显著。

(1) 分层分级统筹推进改造工作：

对照中长期分级常态化防护、全域无感平滑迁移、业务稳定运行的发展趋势，现阶段必须扭转无序建设局面，以分层分级思路统筹推进改造工作。

- **统筹规划改造体系，破解碎片化建设问题。**各行业机构摒弃粗放式全覆盖改造思维，针对当前防护边界不清、优先级混乱的问题，全面摸排自身业务架构、资产体量与数据涉密等级，依据资产实际重要程度划分防护层级，分层分类编制分阶段系统升级方案。
- **锚定核心风险点位，优先筑牢当下安全底线。**立足远期回溯破译风险凸显的现实隐患，坚守核心优先原则，集中资源率先完成核心业务链路、高价值涉密数据、关键基础设施的安全加固，快速补齐现阶段高危环节防护漏洞。
- **凝练统一改造规范，铺垫规模化迁移基础。**汇总梳理各类试点落地成效与问题经验，打破行业内各自为政的改造现状，提炼通用性强的迁移实施模板，统一行业改造技术准则与适配标准，化解现阶段重复建设、适配兼容混乱的难题。

(2) 梯度推进工作节奏：

结合当前进度差距与远期建设目标，本研究建议行业用户侧划定 2026-2030 年分领域梯度推进节奏，逐步

缩小行业发展断层：

- **高敏感涉密领域：**当前安全防护诉求最为迫切，现有防护体系难以匹配高等级保密要求。需即刻全面启动全链路改造升级，补齐现阶段传输、存储、认证各环节防护短板，率先完成抗量子安全体系加固，抢先达成高阶安全防护的未来建设标准。
- **金融、运营商领域：**目前已具备一定试点基础，但整体仍以局部迭代为主，尚未形成规模化普及形态。后续依托现有建设根基持续优化架构，大范围落地商用密码与抗量子安全融合防护体系，逐步平衡安全性能与业务并发效率，稳步趋近安全与效能协同发展的中长期趋势。
- **能源、政务领域：**现阶段改造整体进度滞后，存量老旧系统数量多，新旧体系适配难度较大。以试点项目作为突破抓手，积累场景化适配经验，循序渐进完成存量业务无感知调整，逐步改善当下系统兼容不畅、改造推进缓慢的现状。
- **工控、民用终端领域：**当前防护基础薄弱，终端品类繁杂且算力普遍偏低，暂不具备大规模改造条件。现阶段重心放在技术储备、方案验证与生态适配上，逐步下沉轻量化防护能力，提前布局适配未来终端全域防护的发展格局。

（二）产业供给主体

从现状层面来看，抗量子安全产业已形成量子通信、后量子密码为主的多元生态圈格局雏形，但各生态联动性偏弱，技术产品普遍存在报文膨胀、算力损耗偏高、跨设备兼容差等工程缺陷；产品场景覆盖不均衡，普惠型轻量化产品供给偏少，服务模式也多局限于单一供货，一体化落地支撑能力不足。结合中长期全产业链深度协同、产品通用互通、技术性能全面优化、全场景适配供给的发展方向，本研究建议供给端需立足现存短板精准发力，缩小当下供给水平与行业需求、未来发展的差距。

(1) **技术迭代层面：攻坚现存工程痛点，贴合长远技术演进方向。**紧盯各行业差异化改造进度与实际痛点，针对目前技术产品落地弊端，持续优化 PQC、QKD、QRNG 系列软硬件产品性能。重点攻关算法轻量化重构、专用硬件算力加速、天地一体跨域组网等核心方向，以技术迭代破解现阶段工程落地难题。

(2) **生态协同层面：打破技术发展壁垒，提升产品通用适配能力。**改变当前两大生态圈独立发展、技术壁垒偏高的现状，推动芯片研发、设备制造、安全集成、组网服务等上下游企业协同联动，统一产品接口与交互规范，有效改善不同技术、不同厂商产品互通性不足的问题。

(3) **产品布局层面：补齐场景供给缺口，搭建分层化产品矩阵。**针对现阶段高密核心、商用办公、边缘终端各层级产品供给失衡问题，分层研发定制化设备与安全模块，全面覆盖不同防护等级应用场景，填补轻量化、普惠类产品供应短板。

(4) **服务模式层面：转变单一供货思维，完善全周期落地支撑。**跳出当下单纯产品售卖的经营模式，拓展风险评估、方案设计、现场部署、后期运维的全流程服务体系，匹配行业梯度化改造节奏，逐步构建协同高效、品类齐全、服务完善的成熟产业供给体系。

（三）产业主管层面

从现状层面来看，国内自主抗量子安全相关的后量子密码算法标准尚未完全落地，行业应用规范零散，缺少统一参照依据；产品测评认证体系尚不健全，市场产品质量参差不齐，行业建设秩序有待规整；同时兼具密码技术、量子原理、业务运维的复合型人才存量不足，人才缺口制约产业提速发展。对标中长期标准统一互通、监管体系完备、人才储备充足的产业发展愿景，主管部门需从顶层制度、行业监管、人才培育三方面补齐现阶段发展弱项，引领产业稳步迈向规范化成熟阶段。

(1) **制度规范层面，建议加快自主标准落地，终结建设依据零散乱象。**针对当下标准碎片化、建设无统一依据的现状，加快推进自主后量子密码算法国家标准、行业应用细则落地实施，细化不同场景技术选型规则、系统改造要求与工程验收指标，为未来跨领域兼容互通筑牢制度根基。

(2) **行业监管层面，建议健全测评认证体系，规整市场建设运行秩序。**完善现阶段不够健全的产品检测、资质认证与成效评估机制，明确质量评判门槛与项目建设规范，约束市场经营行为，整治低质建设、无序竞争等问题，推动行业从零散试点向标准化、高质量规模化发展过渡。

(3) **人才培育层面，建议搭建协同培养渠道，补足产业智力支撑短板。**直面当前产业人才供给短缺、专业能力匹配度不足的困境，统筹高校、科研院所、行业企业多方资源，搭建产学研一体化人才培养平台，定向培育复合型专业技术与运维人才，保障中长期技术研发、项目落地、产业扩张的人才需求，全方位夯实产业长效发展保障。

（四）创新摸索：AI 辅助抗量子迁移的行动要求

鉴于当前 AI 技术对各技术领域和各行业应用的赋能与渗透，行业用户可利用 AI 辅助代码库密码调用识别、配置文件解析、证书异常分析、流量特征识别、测试用例生成和迁移影响分析；产业供给侧厂商可在 PQC 兼容性测试、自动化运维、证书异常监测、密钥轮换失败根因分析中引入 AI 能力；监管和标准组织可推动形成 AI 辅助密码资产发现的最小证据要求、脱敏规范和人工复核机制。

但需注意 AI 只能作为辅助工具，不能替代密码专家评审、密评、变更审批和上线验证。任何涉及私钥、生产密钥、核心证书、敏感拓扑和关键配置的信息，均不得输入外部公有模型；确需使用 AI 时，应优先采用本地化、私有化或受控环境，并建立提示词脱敏、日志留存、输出复核和责任追溯机制。

（五）时间表及路线图

围绕抗量子安全迁移的中长期整体发展趋势本节将抗量子安全体系迁移从时间维度划分为“三阶段路线图”。其中：

- **短期准备阶段（2026-2027 年）：**以资产盘点、CBOM、标准跟踪、非生产验证、PQR 基线评估和试点规划为主；
- **中期试点与灰度阶段（2028-2030 年）：**以高价值链路、关键证书、签名类资产、核心应用和重点行业系

统的混合部署、灰度切换、性能优化和合规验收为主；

- **长期规模化替换阶段（2031-2035 年）：**以传统脆弱公钥算法有序退役、密码敏捷平台化、证书与密钥生命周期重构、供应链协同和持续监测运营为主。

需要特别说的是，上述路线图应保留不确定性管理，对应各项变量因素——量子计算真实突破时间、国际标准迭代、国内标准发布、行业监管节奏和供应链成熟度等。因此，相关行业用户不应等待单一“最终标准”后才启动迁移，而应先做可逆、可验证、可回退的准备性工程，逐步建设并具备密码敏捷能力。

综上所述，立足当前抗量子安全产业的发展实际，本研究认为，现阶段产业现存短板体现为技术选型分散、标准体系碎片化、落地节奏失衡、供需适配不足。结合产业发展规律，本研究研判得出，算法轻量化、产业标准统一、全域协同防护是产业中长期演进趋势。围绕现状痛点与未来发展目标的差距，本研究分别从行业用户、产业供给、产业主管三大核心主体层面明确行动建议方向，厘清各主体差异化履职路径，确定行业用户 2026 至 2030 年分领域梯度推进节奏，通过统筹规划改造方案、迭代优化技术产品、完善顶层制度规范等针对性举措补齐当下发展弱项，循序渐进推动行业应用摆脱零散试点的建设形态，稳步朝着自主可控、兼容互通、全域覆盖的标准化抗量子安全防护体系有序演进。

附录 A：抗量子安全核心术语与标准状态表

对象	正式/建议名称	状态口径	落地含义
ML-KEM	FIPS 203，来源于 CRYSTALS-Kyber	NIST 已发布正式标准	主要用于密钥封装/密钥建立，是通用 PQC 迁移主干能力
ML-DSA	FIPS 204，来源于 CRYSTALS-Dilithium	NIST 已发布正式标准	主要用于数字签名，适用于证书、报文、代码和设备身份迁移
SLH-DSA	FIPS 205，来源于 SPHINCS+	NIST 已发布正式标准	哈希签名备选路径，适合关注算法多样性和长期安全冗余的场景
FALCON/FIPS 206	紧凑签名候选方向	仍需以正式发布状态为准	还在候选标准讨论中
QKD	量子密钥分发	工程适配能力与链路条件相关	解决特定链路密钥分发增强，不直接替代认证、访问控制和代码签名
QRNG	量子随机数生成器	可作为熵源增强能力	用于密钥生成和随机数质量提升，不是独立抗量子加密算法

附录 B：密码资产清单与 CBOM 字段模板

字段	说明	来源
系统/业务名称	对应业务系统、应用、网关、设备或服务	CMDB、系统台账、资产管理平台
密码用途	加密、签名、密钥交换、认证、代码签名、日志签名等	代码扫描、配置审计、系统设计文档
算法与参数	RSA/ECC/SM2/AES/SM4/ML-KEM/ML-DSA 等及密钥长度/参数集	流量分析、密码库配置、证书详情
证书与密钥位置	CA、KMS、HSM、终端安全芯片、配置文件等	证书平台、KMS/HSM 台账、终端清单
数据保密期限	数据需要保密的年限及是否存在 HNDL 风险	数据分类分级、业务制度、合规要求
外部暴露面	互联网、专线、内网、跨域、第三方接口等	攻击面管理、网络拓扑、API 清单
迁移批次	首批、第二批、中期、长期运维优化	风险评分和项目计划

附录 C：PQC 兼容性与性能测试基线

测试类别	关键指标	适用场景
协议互操作	TLS/IPSec/SSH/VPN/API 网关/mTLS/国密 SSL 连接成功率、协商失败率	所有生产上线前必测
握手与吞吐	握手时延 p50/p95/p99、TPS、吞吐量、重传率、分片率	金融高并发、运营商大流量、政务公众服务
签名验签	签名生成耗时、验签耗时、证书链大小、签名失败率	电子签章、代码签名、设备身份、清算报文
资源占用	CPU、内存、带宽、硬件加速利用率、终端功耗	云平台、边缘终端、工业设备
业务连续性	灰度成功率、回退成功率、业务中断率、故障恢复时间	核心业务迁移验收
安全与合规	弱算法清除率、密钥轮换成功率、审计日志完整率、密评证据	金融、运营商、能源、政务等关基领域

附录 D：PQR 评分证据与否决项清单

维度	主要证据	典型否决项
资产	自动化扫描、CMDB、证书平台、代码仓库、HSM/KMS 台账	核心系统无密码资产清单或高危资产遗漏
算法	算法清单、兼容性测试、弱算法清除报告	核心系统仍使用禁用算法或 1024 位 RSA 等高危配置
密钥	KMS/HSM 审计日志、密钥轮换记录、权限审批记录	私钥明文存储、密钥导出不可控、无轮换机制
协议	TLS/IPSec/SSH/国密 SSL 测试报告、证书链验证记录	未验证兼容性即生产切换
管控	算法热插拔策略、灰度计划、回退方案、变更审批	无回退方案、无应急吊销和替换流程
合规	密评、等保、关基密码使用管理、行业监管检查材料	高敏感长期数据无迁移计划或不满足监管要求
运维成效	监控指标、事件工单、SLA 报告、用户体验数据	迁移造成不可接受业务中断且无法快速恢复

附录 E：供应商能力评价表

评价维度	评价要点	建议证据
算法能力	ML-KEM、ML-DSA、SLH-DSA、国密/PQC 混合支持情况	产品说明、测试报告、算法清单
协议适配	TLS、IPSec、SSH、国密 SSL、PKI、mTLS、API 网关适配情况	互操作报告、PoC 记录
工程性能	吞吐、时延、硬件加速、终端适配、功耗控制	压力测试、第三方测评
密钥治理	KMS/HSM、密钥生命周期、审计、轮换、备份恢复	运维手册、审计日志样例
密码敏捷	算法热插拔、灰度切换、策略配置、回退能力	演示环境、变更记录
合规与生态	商密、密评、信创、云/数据库/CA/SOC/零信任集成	认证证书、案例材料、集成清单
交付成熟度	行业案例、服务团队、SLA、升级路线图、文档完备性	合同、服务报告、路线图

参考文献

[1] 《中华人民共和国密码法》
[2] 《商用密码管理条例》
[3] 《商用密码应用安全性评估管理办法》
[4] 《关键信息基础设施商用密码使用管理规定》
[5] 《政务信息系统密码应用与安全性评估工作指南》
[6] 《政务领域政务服务平台密码应用与安全性评估实施指南》
[7] 《政务领域政务云密码应用与安全性评估实施指南》
[8] 《金融业商用密码技术应用发展报告（2023—2024）》
[9] 《工业领域数据安全能力提升实施方案（2024-2026 年）》
[10] 《能源行业数据安全管理办法（试行）》
[11] NIST FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM), 2024
[12] NIST FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA), 2024
[13] NIST FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA), 2024
[14] NIST IR 8547 (Initial Public Draft): Transition to Post-Quantum Cryptography Standards, 2024
[15] NIST SP 1800-38A/B/C: Migration to Post-Quantum Cryptography, NCCoE Preliminary Drafts.
[16] IETF TLS WG, ML-KEM Post-Quantum Key Agreement for TLS 1.3, Internet-Draft, 2026; Hybrid Key Exchange in TLS 1.3, Internet-Draft, 2025/2026
[17] 《密码安全产业发展关键动因与竞争格局演变（2026 版）》 2026-05
[18] 四川首次将量子技术运用于水电站项目 2026-05
[19] 从高速到高安全 游仙区政务网迈入量子安全时代 2026-04
[20] 广东移动“5G+量子加密”护航应急指挥安全 2026-04
[21] 交通银行在量子技术领域的应用与探索 2026-03
[22] 齐鲁石化推动科技创新保障能源安全的实践探索 2026-03
[23] 金融业抗量子迁移的全球实践与趋势展望 2026-01
[24] 后量子加密落地，天翼云 PQC 筑牢量子时代安全防线 2026-01
[25] 量子计算突围路线图 2026-01
[26] 全球金融银行业抗量子安全迁移白皮书 2025-12
[27] 量子技术发展及其电力应用趋势展望 2025-12
[28] 从评估、规划到上线运维的一站式抗量子迁移路 2025-12
[29] 中国移动发布《抗量子密码迁移白皮书》 2025-10
[30] 金融业抗量子密码迁移的研究与思考 2025-08
[31] 抗量子密码标准化进展与展望 2025-08
[32] 国泰海通证券抗量子密码迁移 2025-08
[33] 邮储银行抗量子密码敏捷迁移研究探索 2025-08
[34] 中国信通院张萌等：抗量子密码升级迁移关键问题研究 2025-07
[35] 全球首例，我国量子密码技术实现双重抗量子里程碑！ 2025-05
[36] 后量子密码学的工程化实践：从理论到落地的技术挑战与解决方案 2025-05
[37] 量子威胁下的安全革命：后量子密码学技术路线与迁移挑战全解析 2025-05
[38] 《后量子密码安全能力构建（2025 版）》 2025-03
[39] 从《量子准备：向后量子密码的迁移》看美国后量子密码迁移的新进展 2024-10