iCV TA&K
Technology Advisory
& Knowledgebase

光子盒研究院
QUANTUMCHINA

Q-STAR

Quantum Strategic Trends Annual Report



2026 全球量子安全产业发展展望

2026-02

序言

产业成型 格局重塑

2026年，全球量子安全产业正由技术能力构建阶段迈向体系化成型阶段。经过多年标准酝酿、技术验证与示范部署的积累，量子安全逐步嵌入各国数字基础设施升级框架之中，其角色从前瞻性技术储备转向现实安全能力建设。产业发展的核心逻辑正在发生转变，由单点突破驱动转向制度安排、工程实施与产业协同共同推动。

从全球格局看，主要经济体均已将量子安全提升至国家战略与网络安全体系的重要组成部分。美国在完成抗量子密码标准确立后，加快推动联邦系统迁移与产业配套落地；欧洲在统一战略框架下强化标准体系建设，并同步推进量子通信基础设施布局；中国在国家规划引导下，强调量子安全与新型信息基础设施融合发展；加拿大、日本、韩国和印度等国家也围绕关键基础设施安全与前沿通信体系展开部署。总体而言，各国路径虽有差异，但均呈现出政策牵引、标准落地与工程推进协同演进的趋势，全球量子安全产业已进入制度化、体系化推进阶段。

面向未来，随着量子计算能力持续进展与传统公钥体系风险逐步纳入长期评估框架，量子安全将由阶段性布局转向更具规模性的系统部署。抗量子密码的迁移节奏与量子密钥分发的网络化能力建设将形成分层协同格局，混合安全架构有望成为现实路径。产业增长将与各国制度推进节奏、基础设施升级周期及行业迁移需求密切相关，在2030年前后进入加速释放阶段，并在更长周期内重塑全球数字安全体系结构。

本报告立足全球视角，对政策环境、技术演进、产业结构与规模趋势进行系统梳理与综合研判，旨在呈现量子安全产业在关键过渡阶段的整体态势，分析不同区域的发展逻辑与结构特征，为理解未来全球数字安全格局演进方向提供参考。

光子盒研究院 院长

顾成建

声明

01 本报告体现的内容和阐明的观点力求独立、客观，本报告中的信息或所表述的观点均不构成投资建议，请谨慎参考。

02 本报告旨在梳理和呈现2025年度内全球与量子细分技术和产业领域发生的重要事件，涉及数据及信息以公开资料为主，以及对公开数据的整理。并且，结合发布之时的全球经济发展状态，对短期未来可能产生的影响进行预判描述。

03 本报告重点关注2025年度量子安全细分行业发生的相关内容，以当地时间报道为准，以事件初次发布之时为准。对同一内容或高度相似内容的再次报道，若跨年度，不视为2025年发生的重要事件。

04 本报告版权归光子盒研究院所有，其他任何形式的使用或传播，包括但不限于刊物、网站、公众号或个人使用本报告内容的，须注明来源（2026全球量子安全产业发展展望[R].光子盒研究院.2026.02）。本报告最终解释权归光子盒研究院所有。

05 任何个人和机构，在使用本报告内容时，在不得对本报告进行任何有悖原意的引用、删减和篡改。未经书面许可，在任何机构和个人不得以任何形式翻版、复制、发表、印刷等。如征得同意进行引用、转载、刊发的，在需在允许范围内。违规使用本报告者，在承担相应的法律责任。

06 本报告引用数据、事件及观点的目的在于收集和归纳信息，并不代表赞同其全部观点，不对其真实性负责。

07 本报告涉及动态数据，呈现截至统计之时的情况，不代表未来情况，不构成投资建议，请谨慎参考。

研究方法

本研究报告基于系统化、科学化和多元化的研究方法论，通过深度数据挖掘、专家洞见提炼、产业建模分析与多维价值链梳理，全方位评估量子科技的技术前沿、市场潜力及其产业化路径。

01 多源数据收集与验证：本研究采用横跨多维度、多渠道的精细化数据采集策略，涵盖量子科技领域的多元数据源，包括全球量子产业链中的核心企业公开数据、领先科研机构的技术研发成果、政策法规解读、行业市场洞察及学术文献等。为确保数据的广泛代表性与严谨性，我们对采集数据进行了多轮验证与交叉比对，构建高质量的实证数据集，以支持后续分析工作的科学性与精确性。

02 专家网络与深度访谈：通过建立涵盖不同领域的多层次专家网络，本研究与量子科技领域的一线从业人员展开了深度对话。受访专家包括知名量子科技企业的创始团队及技术负责人、行业协会的资深顾问、顶尖高校及科研机构的量子科学家等。访谈以结构化与非结构化相结合的方式进行，围绕技术路径、企业商业模式及未来发展等关键议题展开，从而提炼具有高度前瞻性的洞见。

03 先进建模与数据量化分析：结合全球管理咨询领域的实践经验，研究构建了多层次分析框架与量化模型，以揭示量子科技产业的动态趋势和潜在价值。运用各类统计模型、预测算法及市场模拟技术，对投融资活动、市场规模及产业链分布进行量化分析，力求精准刻画量子科技行业的发展路径及关键驱动因素。

04 产业价值链及场景化洞察：研究采用端到端价值链分析方法，全面梳理量子科技在产业链各环节中的核心要素，从上游关键技术与核心组件研发，到中下游应用场景开发及市场拓展。系统探讨了量子技术在卫星通信、无源导航、金融、化工、材料、能源电力、基础科研、生命科学等多个重点行业的潜在变革性实践，为行业赋能提供战略参考。

05 地区与政策差异化分析：本研究从全球视角出发，开展了区域比较分析，重点评估全球各主要科技国家和地区在量子科技领域的政策扶持、创新生态、人才集聚及技术商业化等能力。基于差异化定位，揭示了区域之间的竞争优势与互补性，为全球量子科技协同发展提供洞见支持。

致谢

本篇报告由量子科技服务平台光子盒下属光子盒研究院撰写和全球前沿科技咨询机构ICV TA&K联合发布。

感谢包括但不限于以下公司给予技术和素材的支持：



目录

1. 2025产业发展概览 8

2. 量子保密通信 22

3. 抗量子密码 52

4. 全球主要国家现状与分析 77

5. 投融资分析 90

6. 供应商评价 100

7.新型应用场景分析 128

8. 产业分析预测 141

9. 产业展望 150

10. 附件 161

研究对象

本研究报告的研究对象是量子安全产业（Quantum-Safe Industry），该产业是为应对量子计算对传统密码体系的威胁而形成的技术密集型产业，聚焦于量子通信技术（如量子密钥分发Quantum Key Distribution，QKD）和抗量子密码技术（Post-Quantum Cryptography,PQC）的研发、应用与商业化。其目标是构建融合物理机制与数学理论的下一代安全体系，保障信息在传输、存储与交互过程中的保密性、完整性、可用性与长期安全性。

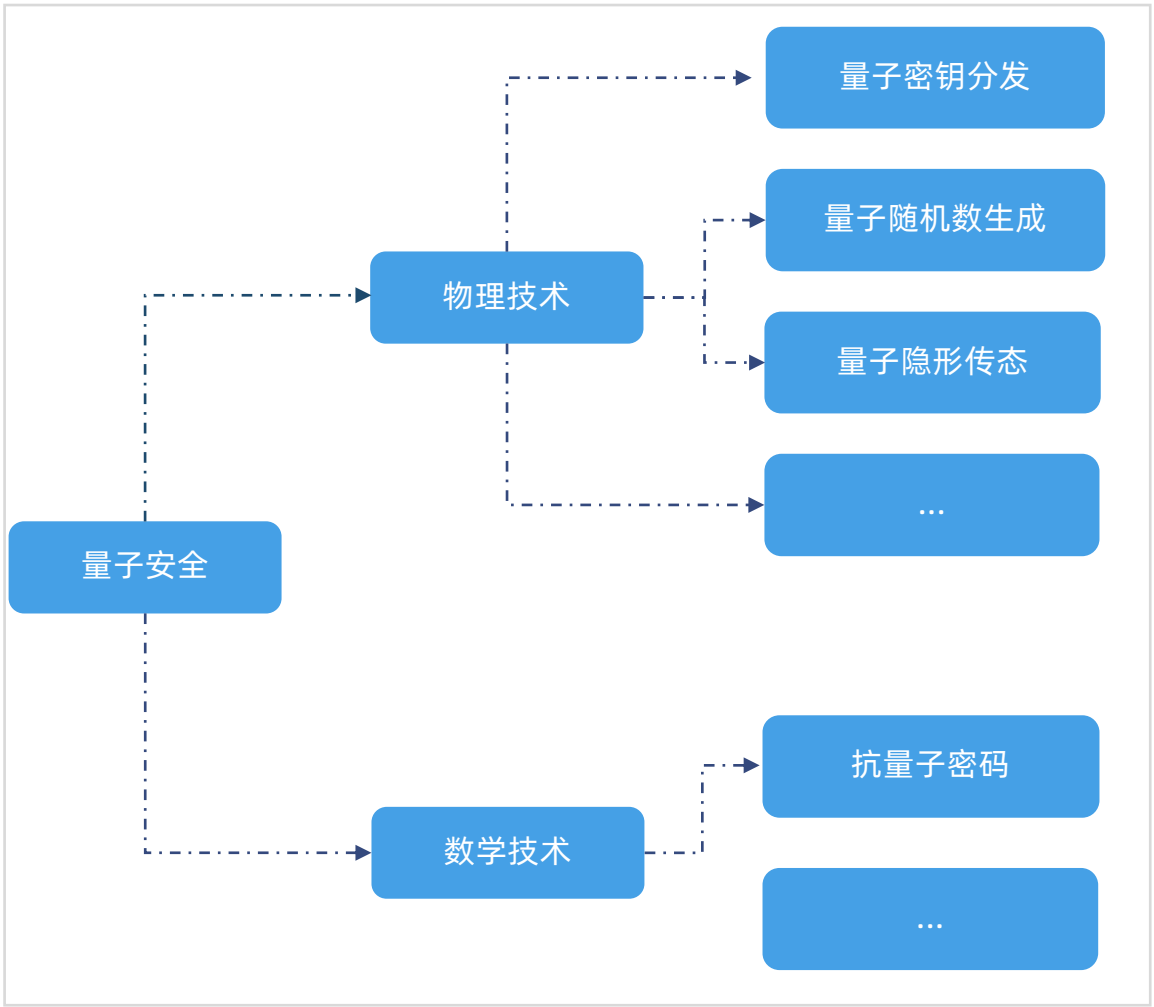
量子安全体系包含两大技术路径：一是物理路径，以量子保密通信为核心，基于量子不可克隆、量子纠缠等原理，通过量子密钥分发、量子随机数生成等技术实现信息传输的本质安全；二是数学路径，以抗量子密码为核心，基于格、哈希、编码等数学难题设计算法，实现向抗量子时代的平滑迁移。两者协同形成“物理层安全+算法层加固”的双重防御体系。

量子保密通信是利用量子态实现安全密钥分发与随机数生成的技术体系，核心产品包括QKD设备、QRNG芯片等，可与现有光网络融合部署，已在政务、金融、能源等领域实现应用。

抗量子密码是一类能抵御量子计算攻击的密码算法，其安全性基于经典与量子计算模型下均难解的数学问题。PQC支持渐进式迁移，涵盖算法标准化、芯片实现、系统集成等环节，是未来信息安全升级的核心方向。

研究对象

图表 量子安全产业研究对象架构



iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2



01

2025产业发展概览

目录

01
2025产业发展概览

01 政策标准协同推进，国家战略牵引产业方向

02 技术体系走向完整，工程化与应用能力同步推进

03 产业链协同加速，量子安全融入现有数字基础设施

04 抗量子密码进入工程部署阶段，应用范围持续扩大

05 投融资趋于理性，资本配置更加集中

06 产业规模持续扩张，发展路径逐渐明确

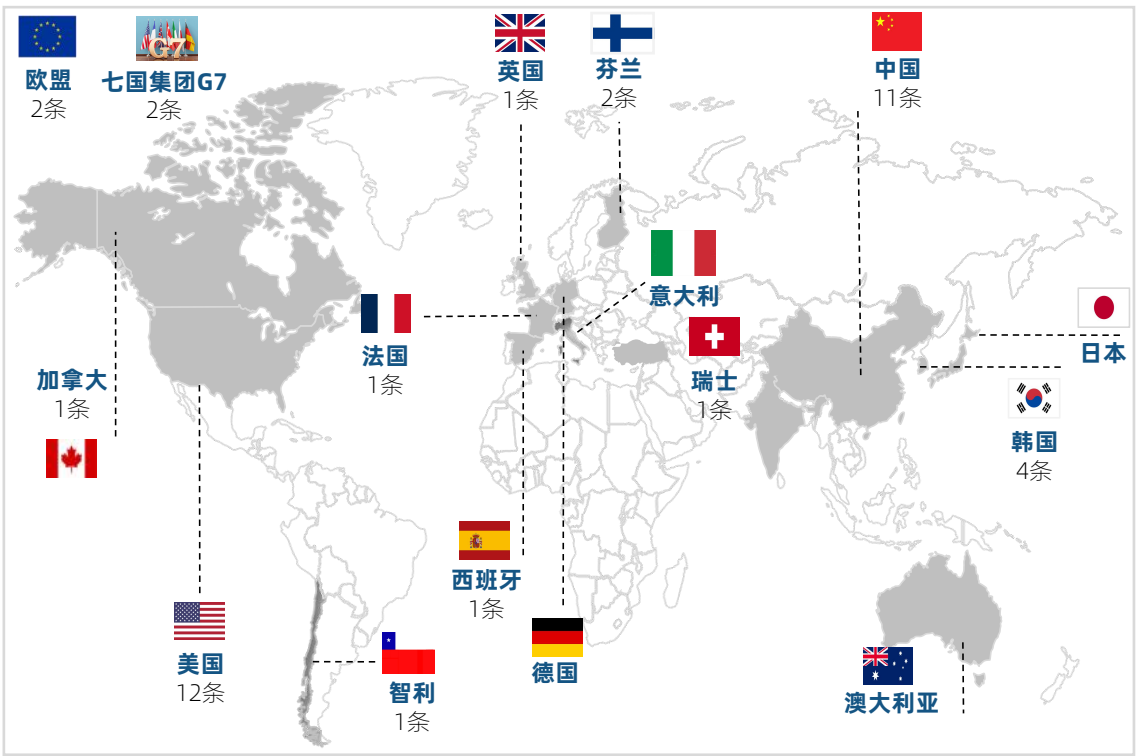
07 量子安全生态结构调整，规则约束不断强化

01 政策标准协同推进，国家战略牵引产业方向

2025年，全球主要经济体将量子安全提升至国家战略与网络安全核心议题的高度，相继出台或更新国家量子科技发展战略、网络安全法案及相关产业政策：

美国推动《国家量子倡议再授权法案》，但相关立法目前仍处于国会审议推进阶段，尚未完成正式通过程序。欧盟发布统一的量子战略/法案《量子技术旗舰计划》等，将量子科技上升至国家战略层面高度，同时设立专项，为量子技术研发提供资金。中国则在“十五五”规划中将量子科技发展放在首位，明确了量子科技作为中国新经济增长点的关键地位。这些政策不仅明确了技术的发展路线、重点领域与支持措施，还引导与市场机制相结合，共同营造有利于技术研发、产业转化和生态建设的宏观环境。

图表 2025年全球量子科技领域发布的国家级政策条数



iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

标准化建设在全球范围内加速推进，并逐步呈现出分阶段演进的格局。在抗量子密码领域，美国已完成以美国国家标准与技术研究院为核心的抗量子密码标准制定工作，当前工作重心转向标准实施、系统迁移与合规应用。欧洲和中国处于持续推进阶段，分别在欧洲电信标准协会及国家密码管理部门主导下，不断完善量子安全与抗量子密码相关标准体系，推动标准与工程实践、行业应用的衔接。

02 技术体系走向完整，工程化与应用能力同步推进

2025年成为量子安全技术由实验验证走向规模化应用的重要节点，核心技术路径在工程化、标准落地与融合应用等多个层面取得系统性进展。

量子密钥分发在网络架构与运行模式上不断成熟，逐步从点对点试验向网络化、服务化形态演进；量子随机数发生器在芯片集成度、生成速率与系统兼容性方面实现产业化突破；部分前沿量子通信与量子信息技术在实验环境中持续刷新性能指标。同时，抗量子密码在完成核心标准制定后，正加速向工程部署与产业迁移阶段推进，量子安全整体技术体系的可实施性明显增强。

图表 2025年量子安全关键技术发展情况



iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

在量子保密通信领域，量子密钥分发技术正围绕网络架构、运行机制和服务模式持续演进，逐步由早期的点对点试验形态，向网络化、平台化和服务化方向推进。量子密钥分发协议在安全性证明、传输距离与密钥生成速率等关键指标上持续优化，多种技术路线在实验和试验网络中验证了百公里级光纤传输及稳定运行能力。与此同时，星地量子密钥分发技术路径逐步清晰，围绕轻量化载荷、高稳定性光学系统与地面接收技术的工程进展不断积累，为构建覆盖地面、空间与跨区域场景的量子通信网络提供了现实基础。

抗量子密码学在2025年已完成从“算法标准制定”向“工程化落地与迁移实践”的阶段性转变。在核心算法体系明确的背景下，产业关注点逐步转向算法实现效率、软硬件适配能力以及在真实系统中的安全性与稳定性表现。围绕算法与现有公钥基础设施（PKI）的兼容部署、证书体系升级、密码敏捷性设计以及硬件加速与侧信道防护等问题，相关工程化研究与产业实践显著增多，标志着PQC正从标准文本走向可运行、可验证的实际系统。

在量子通信与密码技术两条路径同步推进的背景下，量子安全技术整体呈现出由分散能力建设向系统化、可集成安全体系演进的趋势。

量子安全与现有密码基础设施的融合应用成为面向落地的重要方向。学术界与产业界围绕QKD与PQC的协同使用展开探索，通过在网络、身份与密钥管理体系中引入混合安全架构，使不同技术优势在实际系统中形成互补。一方面，PQC为大规模信息系统提供可快速部署的基础安全能力；另一方面，QKD在高安全需求场景中为关键链路提供物理层增强保障。通过分层部署与差异化应用，这类融合架构正在为金融、政务与关键基础设施等领域提供更具工程可行性的量子安全解决方案。

03 产业链协同加速，量子安全融入现有数字基础设施

2025年，量子安全产业链协作水平进一步提升，产业发展更加注重核心器件、系统集成与行业应用之间的协同推进。各环节之间的衔接趋于稳定，为量子安全技术融入现有数字基础设施提供了更成熟的产业支撑。

在上游环节，单光子探测器、量子随机数源以及抗量子密码相关芯片等关键器件在性能稳定性、集成度和供给能力方面持续改进，部分产品开始具备规模化交付条件。这些进展为中游设备和系统厂商提供了更可靠的硬件基础，同时有助于降低系统部署成本，改善量子安全方案的可获得性。

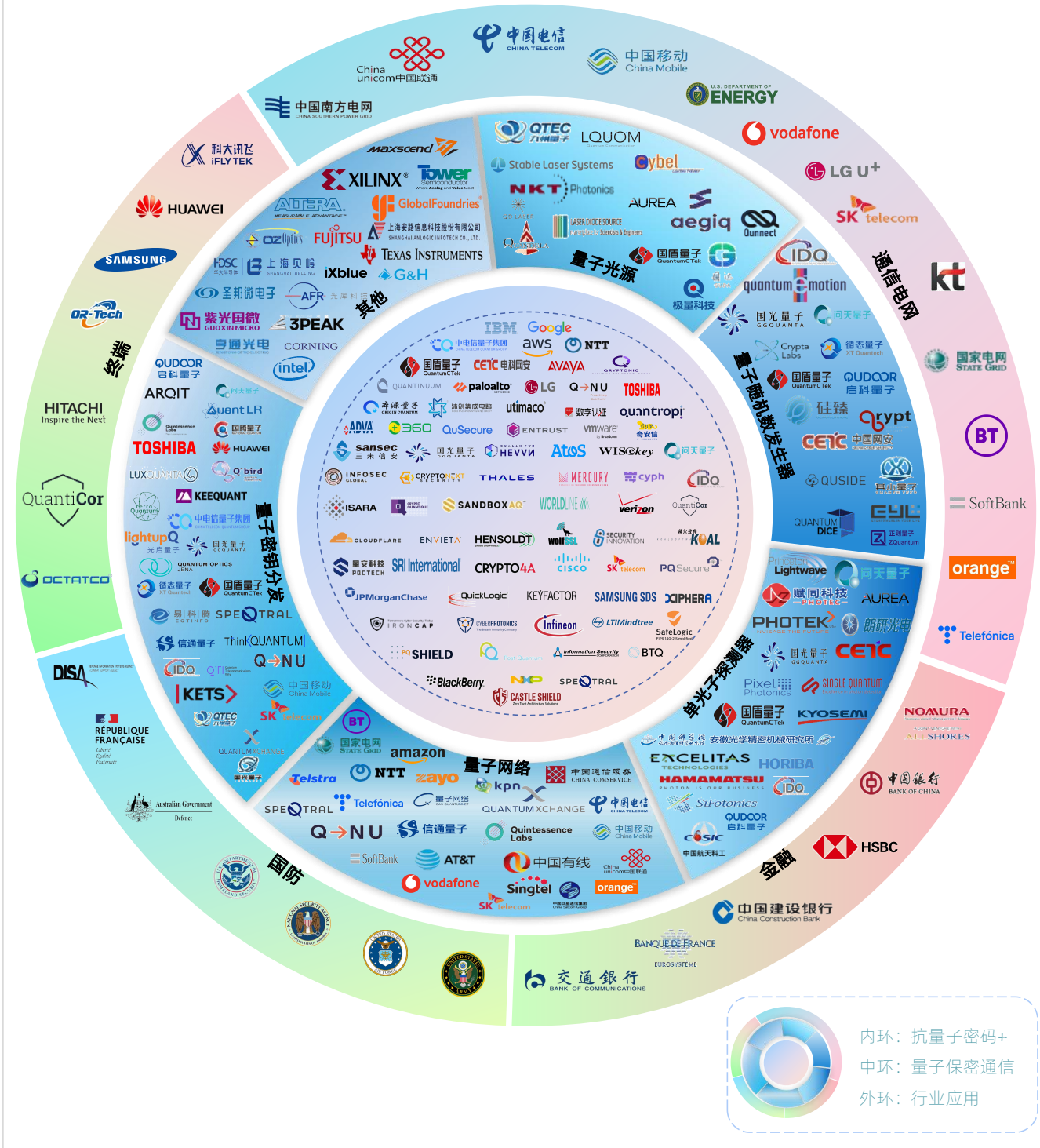
中游环节中，系统集成商和设备厂商更加注重产品的通用性与可配置能力，通过模块化设计和平台化方案，提升量子安全系统在不同网络和业务环境中的适配性。这一变化使量子安全方案从定制化项目，逐步向可复制、可推广的产品形态过渡。

在产业协作方式上，量子安全企业与通信、云计算及行业信息化厂商之间的合作更加常态化。围绕抗量子密码硬件实现、量子安全网络验证以及通信系统安全增强等方向，多方协同推进技术验证和工程测试，推动量子安全能力与现有基础设施的协同部署。

与此同时，量子安全技术开始更系统地融入新一代数字基础设施建设。在6G、车联网、低轨卫星通信等前沿领域，抗量子密码与量子密钥分发被纳入安全架构设计的考虑范围，用于提升长期数据安全与关键链路的防护能力。这类融合更多体现为安全能力的嵌入，而非独立系统建设。

总体来看，随着协作方式和应用边界的变化，量子安全产业中不同类型企业之间的分工逐步调整。量子安全技术正从相对专业的解决方案，转变为可被集成到各类数字系统中的通用安全能力，为数字基础设施的长期安全运行提供支撑。

图表 2025全球量子安全产业生态图谱



04 抗量子密码进入工程部署阶段，应用范围持续扩大

随着量子计算对传统公钥密码体系威胁逐步被量化和验证，抗量子密码正由算法研究和原型验证阶段，进入以标准落地和工程部署为特征的规模化应用阶段。以格基、编码和多变量多项式为代表的算法体系不断成熟，相关的算法选型、性能优化、密钥管理及系统兼容能力持续完善。当前，抗量子密码已在政务、金融、通信、能源等关键领域启动先行部署，并通过与现有密码体系的协同与平滑迁移，成为各国应对量子计算风险的现实技术路径，推动产业发展重心由标准牵引加速转向应用落地。

图表 全球抗量子密码研究企业分布



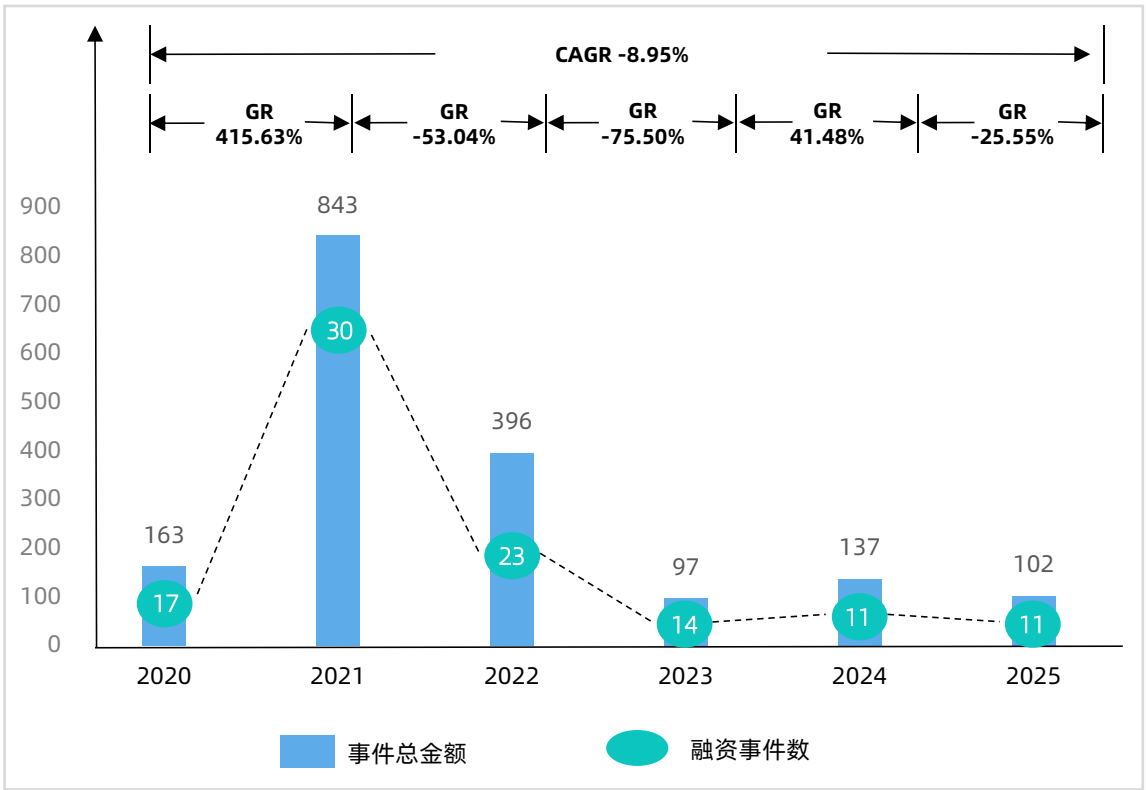
北美在量子安全领域整体保持领先，其中美国依托国家层面的基础设施投入和标准体系建设，加速推进抗量子密码与量子密钥分发技术落地，并在全球规则制定中发挥主导作用；加拿大近年来活跃度明显提升，围绕量子通信与量子安全网络形成了较为集中的创新力量，在北美体系中逐步形成重要补充。欧洲方面，量子安全呈现多国协同推进的格局，欧洲电信标准协会持续推动相关标准建设，德国、法国和英国在量子通信与抗量子密码方向保持较高研发密度，其中英国在量子安全初创和工程化验证方面表现突出。中国则在国家层面持续加大投入，推动量子安全技术与信息基础设施融合，并同步参与国际标准进程，整体发展节奏稳健。与此同时，日本、韩国和印度等国家也在量子安全通信和关键基础设施保护领域加快布局，推动全球量子安全格局呈现多区域并行推进的态势。

总体来看，这张地图突显了国际合作与竞争在量子安全领域日益重要的角色。每个地区都在为全球量子安全的发展贡献力量，美国和欧洲继续在研究与开发方面保持领先地位，而亚洲，特别是中国，正迅速迎头赶上。

05 投融资趋于理性，资本配置更加集中

2025年，全球量子安全领域投融资活动整体保持活跃，但资本配置明显趋于理性。全年量子安全相关融资事件数量保持稳定，抗量子密码与量子密钥分发方向分别完成4起和5起融资，显示资本仍持续关注核心技术路径；与此同时，全年投融资总额约为1.02亿美元，较2024年有所回落，反映出市场由前期广泛布局转向更加注重技术成熟度和商业可行性的阶段。

图表 2020-2025年全球量子安全领域融资总额及融资事件数量（单位：百万美元）



iCV TA&K | 2026.2

从投资取向看，资本更加青睐具备明确技术壁垒、工程化部署能力和实际行业应用案例的企业，投资重点逐步集中于抗量子密码迁移方案、量子安全系统集成以及关键器件的规模化供给等方向。

区域层面，欧美地区依托成熟的信息安全产业基础和标准推进节奏，仍保持在量子安全投融资中的领先地位；同时，亚太地区部分国家在抗量子密码软件、安全服务及应用型解决方案方面的创新活跃度有所提升，使全球投融资格局呈现出更加多元的发展态势。

总体来看，量子安全领域的投融资活动已逐步回归理性，资金配置更强调技术成熟度和落地可行性。资本不再追求广覆盖式布局，而是围绕具备明确应用路径和工程实施能力的方向持续投入。这一变化与量子安全产业从验证阶段迈向工程部署的整体节奏相一致，也为后续市场规模的稳步释放提供了现实支撑。

06 产业规模持续扩张，发展路径逐渐明确

2025年，全球量子安全产业进入以应用落地和规模扩展为特征的发展阶段，产业规模约为27.03亿美元，预计2030年将增长至118.05亿美元，2025-2030年期间年复合增长率约为34%；随着抗量子密码与量子密钥分发协同应用逐步形成稳定部署模式，量子安全产业有望在2030年后加速扩展，预计2035年产业规模将达到约767.95亿美元，2030-2035年期间年复合增长率约为45%-46%，表明量子安全正由补充性安全技术演进为支撑全球数字系统长期安全运行的重要基础能力。

当前产业发展呈现出两大关键特征：一方面，核心企业凭借完善的产业链布局和标准化能力，构建起较高的行业准入门槛，使得单纯依赖技术创新的初创企业面临更大商业化挑战；另一方面，政府主导的顶层设计和政策推动成为产业发展的重要驱动力，各国通过专项规划、合规要求和采购标准等方式，为量子安全技术的规模化应用创造了必要条件。

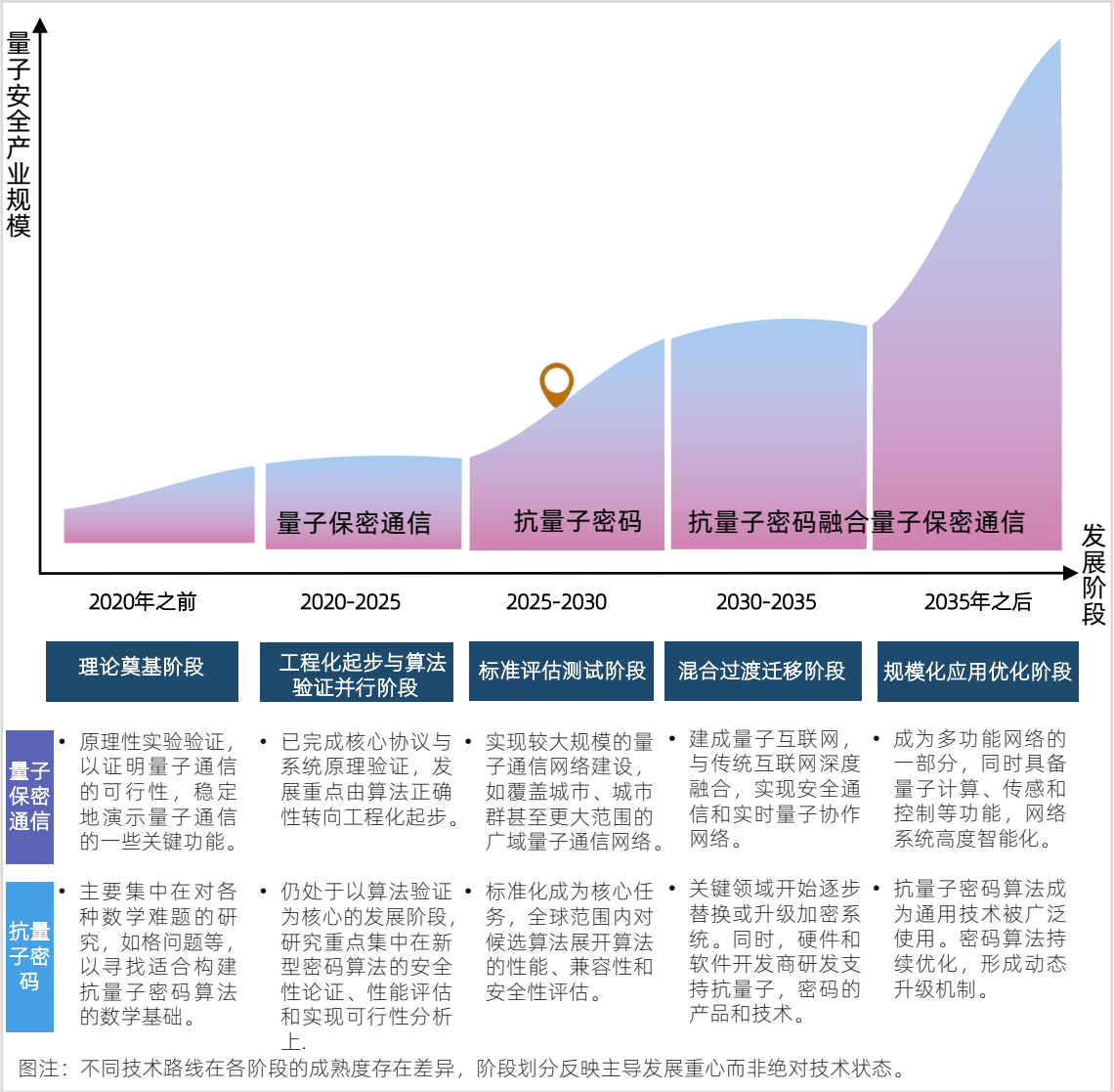
从产业演进的时间维度分析，量子安全技术的应用推广呈现清晰的阶段性特征。在2027年之前，经典密码体系仍能维持基本的安全需求，这为量子安全技术的成熟完善与产业生态构建提供了关键的缓冲期。预计到2035年前后，随着量子计算能力的实质性突破，经典密码体系将面临系统性安全风险，各行业对量子安全解决方案的需求将迎来爆发式增长，推动量子密钥分发、抗量子密码等核心技术进入规模化部署阶段。

总体来看，全球量子安全产业正处于由小规模验证向规模化应用过渡的关键阶段，产业增长节奏与技术成熟度、政策推进和系统迁移需求高度相关。短期内，产业发展仍将以能力完善和路径探索为主；中长期看，随着量子计算风险逐步显性化，量子安全技术有望在更广泛的数字系统中加快部署，为产业规模持续增长奠定坚实基础。

07 量子安全生态结构调整，规则约束不断强化

随着量子安全相关技术和解决方案在更多实际场景中得到验证和应用，其发展重心逐步转向围绕长期运行、跨体系衔接和稳定应用展开的整体生态问题。2025年，量子安全的推进方式更加关注不同参与主体之间的关系结构，以及支撑其持续扩展的组织和规则条件。

图表 量子安全产业发展周期示意图



图注：不同技术路线在各阶段的成熟度存在差异，阶段划分反映主导发展重心而非绝对技术状态。

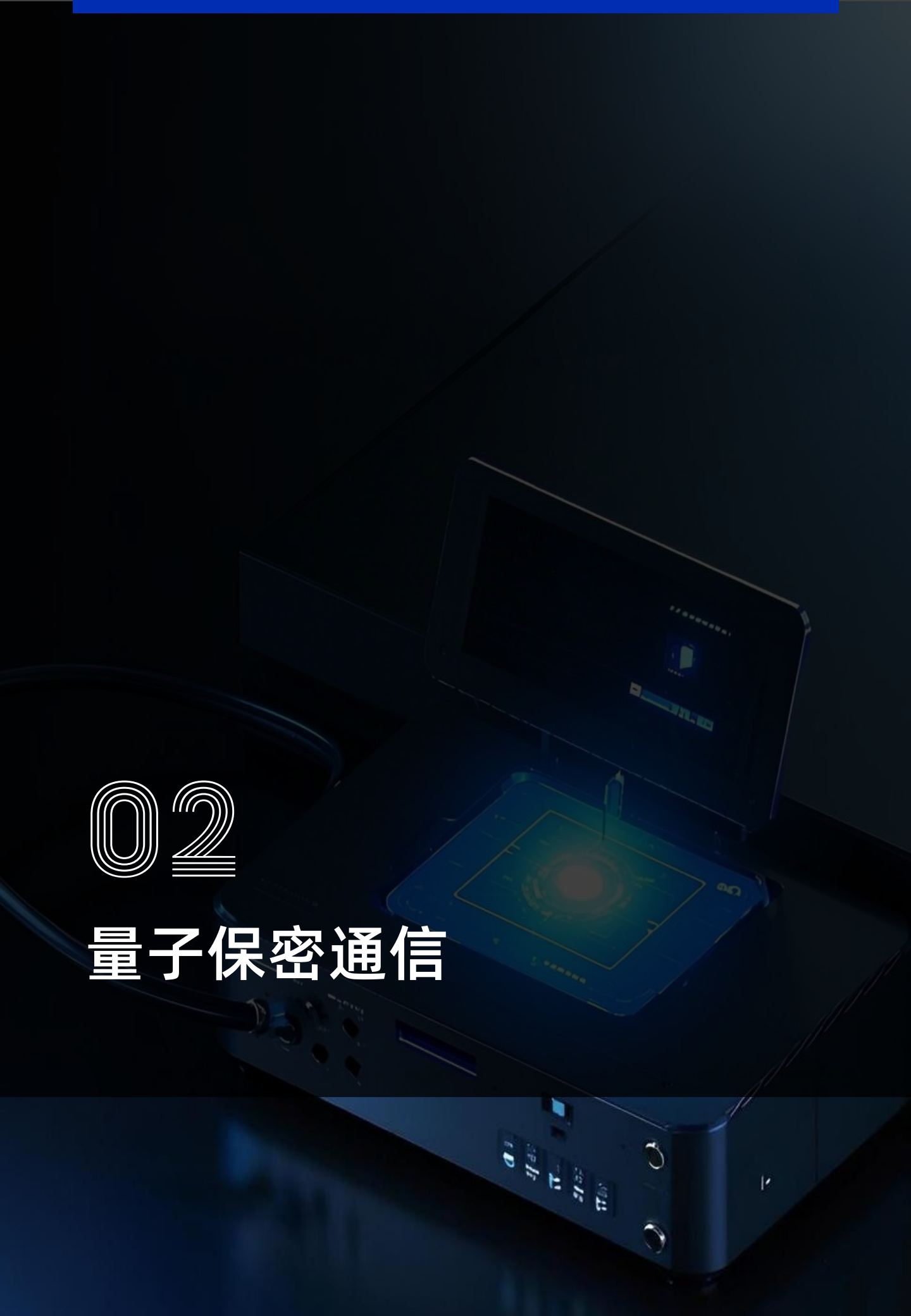
iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

从生态结构看，量子安全相关参与主体呈现出更加多元的分布格局。量子技术企业、传统信息安全厂商、通信相关主体以及行业用户之间的角色边界逐步清晰，各方在能力供给、系统嵌入和应用落地中的分工趋于明确。

从应用运行方式看，量子安全的部署开始与行业系统的调整节奏相互配合。在金融、政务、能源、电信等领域，相关能力逐步被纳入整体安全规划，与系统升级、架构调整和安全策略更新同步推进。关注重点由是否采用新技术，转向如何在既有体系中实现平稳衔接与持续运行。

在规则与治理层面，影响量子安全扩展的外部约束条件日益清晰。标准体系、合规要求以及跨区域协调机制，正在对技术部署路径和应用范围产生实质性影响。不同国家和地区在标准、认证和监管要求上的差异，使量子安全相关产品和服务在推广过程中需要更高程度的规则适配，也促使企业更加重视合规能力和生态参与深度。

总体来看，量子安全的发展正在更多体现为一种生态结构和运行机制的问题。企业之间的竞争不再局限于技术能力本身，而是逐步延伸至其在整体生态中的位置、与既有体系的适配程度以及对长期运行规则的响应能力。这一变化为量子安全在更大范围内的稳定应用提供了必要条件。



02

量子保密通信

目录

02
量子保密通信

01 协议演进与安全性增强

02 系统集成与工程化突破

03 网络建设与规模化部署

04 标准化工作进展

01 协议演进与安全性增强

2025年，量子保密通信协议的演进更加聚焦工程可实施性与网络化扩展能力。围绕构建可部署、可运行的量子安全网络，量子密钥分发、量子密钥共享与量子隐形传态在不同层级持续推进：量子密钥分发侧重于提升密钥生成能力与工程稳定性，量子密钥共享关注多用户协同与信任分配机制，量子隐形传态则为未来量子网络中的量子态传输和分布式处理提供基础支撑。三类协议在性能优化、安全验证与系统形态上的协同演进，逐步勾勒出面向实际网络环境的量子保密通信协议框架。

量子密钥分发：在现有条件下兼顾安全与效率

量子密钥分发仍是量子保密通信体系中最成熟、工程化程度最高的技术方向。2025年的研究重点，集中在长距离低成本部署、复杂环境适应能力、多用户网络化以及系统级安全性强化等方面。

长距离协议与成本可控实现取得实质性突破

01 实现了实用化的模式配对量子密钥分发系统

中国科学技术大学 University of Science and Technology of China　清华大学

基于商用激光器，成功构建了一套实用的高性能模式配对量子密钥分发系统。通过提出一种基于快速傅里叶变换的频率跟踪方案，有效克服了长距离传输中的相位波动难题。该系统在超过403公里（损耗76.5 dB）的标准光纤上实现了最优密钥率，比无中继器边界高出2.92倍，为长距离、低成本QKD部署提供了新方案。

02 异步测量设备无关协议的高性能实现

北京量子信息科学研究院 Beijing Academy of Quantum Information Sciences　中国人民大学 RENMIN UNIVERSITY OF CHINA

该研究开发了一种创新的后测量补偿方案，仅通过量子信号探测结果即可精确估算两台紧凑型激光器间的互频偏，从而消除了对光学参考光的依赖。在 2.5 GHz 时钟频率下，该系统在 201 公里 距离实现了 101 kbit/s 的安全密钥率，并在 100 公里 处结合超稳激光器达到了 1.03 Mbit/s，足以支持实时一次一密（OTP）视频加密。这一成果在 100-400 公里 范围内实现了测量设备无关架构下的最高密钥率，为构建高性能、低成本的规模化城际 AMDI-QKD 网络提供了重要方案。

自由空间与移动平台场景下的稳定性显著提升

面向空天地一体量子通信网络，研究重心从是否可行转向是否稳定、是否低复杂度。

01 面向移动平台的稳定量子通信新技术

ETRI Electronics and Telecommunications Research Institute　KAIST

联合团队创新性地提出了“测量保护”理论，并基于此开发了一套在卫星、船舶、无人机等移动环境中进行稳定量子通信的新系统。该系统能在无需随信道状态反复校准接收端的条件下完成QKD，在10米自由空间、30dB最大损耗的传输环境中，将量子比特误码率容限提升了20.7%，显著增强了恶劣条件下的通信稳定性。

02 全天候自由空间连续变量QKD系统

中国科学技术大学 University of Science and Technology of China　问天量子

提出并演示了一种新型高斯调制相干态连续变量QKD系统。该系统设计独特，可在白天甚至雨天的自由空间环境中稳定运行，而无需复杂的背景光过滤装置。在10 MHz调制频率下，系统保持了超过100 kbps的安全密钥速率，为构建低成本、高鲁棒性的自由空间量子通信链路奠定了基础。

网络化与多用户QKD迈出关键一步

为实现大规模量子网络的最终目标，2025年的实验在构建多用户、全连接的QKD网络方面迈出了关键一步。

01

全连接多用户QKD网络实验演示

南京大学 NANJING UNIVERSITY　中国科学技术大学 University of Science and Technology of China

通过将测量设备无关QKD协议与集成光学频率梳相结合，实验演示了一种基于波长复用技术的全连接多用户QKD网络。在每用户对约30 dB链路衰减条件下，实现了平均267比特/秒的安全密钥率，较以往基于纠缠的方案提高了三个数量级以上。首次实现了两对用户间的同步量子安全通信，为构建大规模实用化量子网络开辟了新途径。

工程实现环节成为新的关注重点

随着量子密钥分发系统逐步进入真实网络和工程部署环境，研究关注点开始从协议层的理论安全性，转向系统实现过程中由功耗、时序等工程因素带来的影响。

01

QKD系统的功耗侧信道攻击演示

U LISBOA UNIVERSIDADE DE LISBOA　PQI PORTUGUESE QUANTUM INSTITUTE

提出并实施了对QKD系统的功耗侧信道分析，通过利用控制QKD发射机电光元件的FPGA驱动器的功耗波动，成功预测了传输的量子比特信息，在100 MHz重复频率下最高准确率达到73.35%。该工作揭示了一个新的潜在攻击面，并讨论了相应的防护对策。

与经典光通信的共纤融合趋于成熟

连续变量QKD与现有光通信系统的融合部署在2025年取得实质性进展。

01 **创纪录距离的连续变量QKD与经典信号共纤传输**

Danmarks Tekniske Universitet DTU　Palacký University Olomouc

展示了连续变量QKD与完整填充的粗波分复用系统在同一光纤中的超长距离共存。通过本振的自然模式滤波和相位噪声缓解技术，在无需额外滤波的条件下，实现了超过120公里（20 dB损耗）的连续变量QKD传输，创造了该技术的光纤距离记录，验证了其在现有长距离光网络中即插即用部署的可行性。

02 **QKD与400G DWDM业务的并行传输验证**

PacketLight NETWORKS　NEC \Orchestrating a brighter world

两家公司联合完成了量子密钥分发与400G DWDM网络的并行传输验证。测试采用双纤物理隔离架构，NEC的QKD系统通过独立光纤传输量子密钥，与PacketLight设备的400G数据业务并行运行，在保证DWDM网络全性能的同时实现了量子级安全，为运营商提供了无需改造现有基础设施的高性价比量子加密解决方案。

新型光源与处理优化带来性能提升

探索新型量子光源和优化后处理模块，为突破QKD系统的性能瓶颈提供了新的技术路径。

01 **基于室温单光子源的城域QKD实验**

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE　NUS National University of Singapore

成功演示了使用基于氮化镓缺陷的室温单光子源在电信波长下进行QKD。他们在33公里光纤上执行了BB84等协议，并成功在30公里的已部署城域光纤上实现了QKD实验，为未来低成本、易集成的单光子源在商业QKD中的应用拓宽了前景。

协议改进提升系统对光源和信道的适应性

01 提出并实验演示了两种适用于非理想单光子源的QKD协议

利用基于巨型胶体量子点与纳米天线耦合的室温单光子源，通过调控双激子—激子级联发射的光子统计特性，引入截断诱骗态协议和预示纯化协议，在安全密钥生成允许的最大信道损耗方面实现显著提升，性能甚至超过理想弱相干态诱骗态方案约3dB。

02 基于软件实现的信道自适应CV-QKD协议

通过在发射端和接收端引入自适应滤波机制，使系统能够动态响应不断变化的信道条件，并在安全分析中避免依赖高斯极值假设，从而获得对窃听者信息更精确的界定。实验与仿真结果显示，该协议在光纤和卫星模拟等高损耗场景下，相较既有CV-QKD方案实现了数量级的密钥率提升，且无需对现有硬件系统进行改造，展现出良好的工程兼容性。

总体来看，这类协议层创新通过重新审视光源模型和信道假设，显著扩展了量子密钥分发在非理想条件下的性能空间，为QKD在复杂网络环境和新型应用场景中的进一步应用提供了更加灵活的技术选择。

量子隐形传态：迈向高维、集成与网络化

量子隐形传态是实现量子态远程传输与量子网络构建的关键基础能力，也是连接量子通信与分布式量子信息处理的重要技术环节。2025年，相关研究重心逐步从基础原理验证，转向更具工程可行性的方向，重点关注高维量子态传输、芯片级集成实现、与量子网络架构的兼容性，以及在复杂系统条件下的稳定运行能力。

芯片化与集成光学成为实用化重要路径

01 基于硅基光子芯片的高维CNOT门隐形传态

中国科学技术大学 University of Science and Technology of China　浙江大学 ZHEJIANG UNIVERSITY　硅臻 SILICON EXTREME

首次实现了基于高维路径编码硅基光子集成电路的量子受控非门隐形传态。在配备1公里互联光纤时，实现的平均纠缠保真度达94.07%±1.54%，门层析保真度达93.04%±1.09%，为基于芯片的大规模实用量子网络奠定了关键技术基础。

02 星形拓扑网络中的芯片到芯片光子隐形传态

清华大学　北京量子信息科学研究院 Beijing Academy of Quantum Information Sciences

在星形拓扑量子网络场景下，演示了光纤上的基于时间仓编码的芯片到芯片光子量子隐形传态。采用有源反馈系统抑制光纤长度波动后，成功在12.3公里光纤上实现了稳定的芯片间量子隐形传态，展现了芯片集成技术在扩展量子网络距离方面的巨大潜力。

新物理平台拓展隐形传态的应用频谱

01 基于超导电路的连续变量微波量子隐形传态

IBM

IBM团队在超导量子计算平台上，演示了基于连续变量的微波波段量子通信关键要素。利用一个非简并约瑟夫森混频器作为纠缠源，构建了一套量子隐形传态装置。该装置成功以73%的最大保真度隐形传态了真空态与相干态，超过了50%的经典极限。

量子密钥共享：面向多用户量子安全网络的信任机制

量子密钥共享是面向多方参与场景的重要量子安全技术，主要用于解决多节点之间的密钥协同生成与安全分发问题，在分布式安全架构和复杂业务系统中具有独特价值。

实用化与高效率协议实验取得关键突破

01 **源无关量子秘密共享的多用户实验演示**

南京大学 NANJING UNIVERSITY　中国人民大学 RENMIN UNIVERSITY OF CHINA　北京量子信息科学研究院 Beijing Academy of Quantum Information Sciences

实验演示了一种资源高效的源无关量子秘密共享协议。该协议利用纠缠光子对，在星型拓扑的量子网络中成功实现了三用户、四用户乃至五用户的密钥共享。证明了密钥速率可与用户数量无关，为在多用户量子网络中大规模部署该技术开辟了道路。

面向分布式计算的延伸探索

量子密钥共享的思想正被应用于更广泛的分布式安全计算场景，展现出构建未来量子安全基础设施的潜力。

01 **基于QSS的分布式安全量子计算验证**

UNIVERSITY OF OXFORD　UNIVERSITY OF BATH

首次实验演示了利用量子秘密共享原理来验证分布式量子计算的概念。这项工作将QSS的安全多方特性从单纯的密钥分发，拓展到了可验证的量子云计算领域，为未来量子计算的安全外包提供了一种创新范式。

总体来看，2025年量子保密通信协议的发展更加注重工程可行性、网络扩展能力与系统安全评估。协议层创新正与器件性能、网络架构和实现细节紧密结合，推动量子保密通信由实验室验证逐步走向可部署、可运行的网络形态。这一演进为量子安全通信在更复杂应用场景中的推广奠定了坚实的技术基础，也为后续规模化网络建设提供了现实支撑。

02 系统集成与工程化突破

2025年，量子保密通信的技术推进更加直接地受到工程约束条件的牵引。系统设计开始以部署复杂度、运行稳定性和维护成本为主要考量，对关键器件的选型与架构组合进行整体优化，使量子安全能力能够在现有通信和计算基础设施中实现更顺畅的集成。



量子随机数发生器：向芯片化与嵌入式形态演进

量子随机数发生器作为量子安全体系的基础信任源，其工程发展正在由独立设备向芯片级与模块化形态加速演进，以满足嵌入式部署和规模化应用需求。

芯片化与低功耗方案的突破

01 全球首款全功能QRNG芯片

中国科学技术大学 University of Science and Technology of China　仕佳光子 SHIJIA PHOTONS

首次报道了一款基于真空态涨落的全功能QRNG芯片，尺寸仅为16.6×7.8 mm^2。通过混合光子集成与系统级封装，该芯片在-40至85℃的工业温度范围内实现了5.2 Mbps的恒定实时输出，标志着QRNG芯片化迈出关键一步。

02 低功耗、高速QRNG方案

HERIOT WATT UNIVERSITY　TOSHIBA

基于集成光子干涉仪的紧凑型QRNG方案。通过巧妙的电路设计，用低功耗时序比较器替代高位模数转换器，将系统总功耗降至7.93 W，同时实现了高达2 Gbps的随机数生成速率，并成功应用于实时量子密钥分发系统的种子注入，为星载等严苛环境应用提供了方案。

利用量子计算或新算法特性来简化硬件

01 “全息深度热化”量子随机生成器

USC ILLINOIS

提出“全息深度热化”方法，在IBM量子云平台上仅用8个量子比特即实现了5量子比特的随机态生成。该方法大幅减少了所需的辅助系统规模，为未来基于中小规模量子处理器的随机数服务提供了新范式。

02 硅光子QRNG技术转移

இந்திய தொழில்நுட்ப கழகம் மெட்ராஸ்
भारतीय प्रौद्योगिकी संस्थान मद्रास
Indian Institute of Technology Madras

基于硅光子学的高速QRNG技术以1000万卢比许可给Indrarka Quantum Technologies公司，实现了从实验室到市场的跨越，旨在推动印度本土量子安全解决方案的部署。

产业链合作与新型服务模式

01 卫星QRNG服务合作

NuSpace Partisia

三方签署备忘录，计划将卫星搭载的QRNG与多方安全计算相结合，利用卫星的天然安全信道分发真随机数，为地面提供抗量子的安全计算服务，开创了“空天一体”的安全随机数服务新模式。

量子光源：走向高集成与稳定应用

量子光源是量子密钥分发系统中的关键部件，其工程化水平直接影响系统的密钥生成效率与长期运行稳定性。2025年，更加聚焦于提升纠缠光源的集成程度、降低结构复杂度，并在此基础上探索新材料和新实现路径，以满足实际部署对可靠性和可维护性的要求。

新型材料与集成光源探索

01 **基于菱面体氮化硼的片上纠缠光子对源**

利用菱面体氮化硼独特的光学非线性特性，成功在其波导结构中产生了纠缠光子对。这种二维材料为在芯片上直接制备高品质、可集成的量子纠缠源提供了新的材料平台，有望简化量子光路的复杂度。

02 **简化结构的0型自发参量下转换源**

团队报道了一种在同一块周期性极化晶体内，通过双通配置同时实现二次谐波产生和自发参量下转换的集成光子源方案。该设计无需复杂的光学对准，实现了完全光纤耦合，简化了硬件要求，提升了模块的实用性和稳定性。

高性能光源

01 **基于超导约瑟夫森结的芯片级相干光源综述与展望**

利用超导约瑟夫森结及其混合结构（如超导发光二极管）实现从微波到太赫兹乃至光学波段芯片级、电驱动、电可调谐相干光源的物理机制与技术路径。这类光源在功耗、集成度和频率调谐范围上具有独特优势，为未来量子信息系统提供了一种潜在的新型片上光源解决方案。

单光子探测器：性能提升与工程可用性同步推进

单光子探测器是量子通信系统中决定系统灵敏度、误码水平和长期运行稳定性的关键器件之一。随着量子通信从实验验证走向工程部署，不同类型探测器在性能指标与工程可用性之间的权衡逐渐成为研究和应用的核心关注点。

图表 单光子探测器分类及简介

类型	技术路线	主要性能优势	典型应用场景
超导单光子探测器（SNSPD）	超导纳米线	探测效率高、暗计数率极低、时间分辨率优异	长距离量子通信、骨干网、星地量子通信、高性能实验系统
半导体单光子探测器（SPAD/APD）	雪崩光电二极管	工作条件相对宽松、集成度高、成本较低	城域网、接入网、终端设备、嵌入式量子安全系统
混合集成探测模块	超导/半导体＋集成封装	在性能与工程可用性之间取得折中	多用户量子网络、工程示范系统
新型探测器探索方向	新材料/新结构	有潜在性能提升空间	前沿研究与下一代系统储备

iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

超导探测器性能优化

01 无电流拥挤的高性能SNSPD

Technical University of Munich MCQST

通过氦离子局部辐照技术，选择性修饰SNSPD直线部分的特性，成功抑制了弯曲处的电流拥挤效应。制备的SNSPD在780 nm波长下实现了94%的内部探测效率，同时将暗计数率压低至7 mHz，并允许在更低的偏置电流下工作，提升了器件的稳定性和使用寿命。

半导体探测器模型与应用优化

02 时间二进制编码系统中SPAD的精确响应模型

中国科学技术大学 University of Science and Technology of China

针对SPAD在时间编码QKD系统中的死时间效应，提出了一个能够精确描述其响应的实用模型。该模型不仅提高了增益预测的准确性，更关键的是揭示了死时间在早期与晚期时间仓之间引入的比特关联性及其安全风险，为设计更安全、更高密钥率的QKD系统处理算法提供了理论依据和优化方向。

未来单光子探测器的发展方向：

面向量子通信系统规模化和高速化的发展需求，单光子探测器的技术演进正呈现出多维度并行推进的特征。总体来看，未来的发展重点主要体现在以下几个方面：

一是持续提升光子探测能力上限，通过材料、器件结构和读出方式的综合优化，进一步提高有效探测概率，增强系统在长距离和复杂环境下的稳定表现；

二是围绕噪声控制与稳定运行能力，加强对暗计数、后脉冲等非理想因素的抑制，从系统层面改善信号判读质量，为长期运行和多用户应用提供更可靠的基础；

三是面向高速量子通信和多通道并行需求，推动探测器在响应速率和读出带宽上的进一步提升，以适配更高频率、更高吞吐量的通信场景；

四是强化工程集成导向，在保持探测性能提升的同时，推进探测器模块化、小型化和高度集成设计，使其更易于嵌入终端设备和大规模量子网络体系之中。

专用芯片：支撑系统集成与规模部署的关键基础

专用芯片是实现量子保密通信系统小型化、规模化和成本下降的核心环节，其成熟度直接影响产业落地速度。

前沿功能芯片

01 接收与操控非经典光的量子相控阵芯片

团队展示了一个集成了超过1000个功能组件的片上系统。该系统通过32个超材料天线阵列实现了自由空间量子光到芯片的直接接口，并能同时以量子极限灵敏度接收、成像和空间操控压缩光。

02 无漏洞量子导引非定域性演示芯片

北京量子信息科学研究院 Beijing Academy of Quantum Information Sciences 北京邮电大学

在完全芯片-光纤集成的系统中，首次实现了时间-比特纠缠的无探测漏洞量子导引演示。设计制备了低损耗硅基光子芯片用于高效纠缠产生，并通过相位编码适配时间自由度，系统测量切换速率高达1.25 GHz，为基于量子非定域性的安全通信应用提供了坚实的芯片化实验平台。

商业化安全芯片

01 SEALSQ Corp在Q+AI 2025大会上发布了首款硬件嵌入式抗量子安全芯片Quantum Shield QS7001，该芯片直接在硅基硬件中集成了NIST标准的PQC算法，为未来抗量子威胁提供硬件级安全保障。

02 三星系统LSI在2025年推出了搭载硬件PQC能力的安全芯片，为移动终端提供量子抗性安全能力，这些进展标志着量子安全芯片从试验产品向实际供给能力稳步演进。

03 网络建设与规模化部署

2025年，量子信息网络建设的工作重点明显发生转移，从早期以点对点链路和原型网络验证为主，逐步转向面向体系化工程的推进与规模化部署准备。各国关注的核心问题已不再是单条量子链路是否可行，而是在成本、稳定性和运维可控的前提下，如何实现跨区域量子态的高保真分发，并将量子链路纳入既有通信网络的工程体系之中。

从全球技术路线看，量子网络的发展主要沿三个方向同步推进：一是以量子中继、量子存储为代表的关键支撑技术持续取得进展，为超远距离量子互联提供现实路径；二是光纤骨干网与城域接入网的建设不断加快，与现有通信网络的融合验证同步展开；三是星地一体化量子通信从单点试验逐步迈向面向组网与服务能力的工程规划。这三个路径相互牵引，使量子通信网络开始从科研验证形态，向具备工程特征的网络形态演进。

量子中继：从原理验证走向实用化探索

量子中继被普遍视为突破光纤传输损耗限制、实现远距离量子通信的关键环节。2025年，研究的关注重点已从基础物理原理的可行性证明，转向对效率、容错能力以及实际实现成本的系统评估。

在这一背景下，不同技术路线的量子通信中继逐渐形成相对清晰的分类，其工程可行性与应用时间窗口也开始出现分化。

图表 量子通信中继的主要类型

类型	核心原理	技术特征	工程成熟度
基于纠缠交换的量子中继	通过纠缠生成与纠缠交换实现长距离传输	理论体系成熟，对存储与同步要求高	处于实验室与小规模验证阶段
基于量子存储的量子中继	利用量子存储器缓存量子态并分段传输	可缓解时序与损耗问题，对存储寿命要求高	关键器件仍是主要瓶颈
全光量子中继	依赖非线性光学或测量诱导操作	结构简化，无需量子存储	实用性受限，容错能力不足
混合型量子中继方案	结合纠缠、存储与经典控制	在工程可行性与性能之间折中	被视为近期重点探索方向

架构与协议创新：追求更高效率与可行性

01 基于图态的容错全光量子中继新方案

团队提出利用复杂连接性的图态作为资源，能够更高效地建立远程纠缠。该方案在灵活性和容错能力上更具优势，并系统分析了其资源开销，为设计可扩展的量子中继网络提供了新范式。

02 证明双向协议在实用化参数下的优越性

提出一种结合多路复用与智能蒸馏的双向量子中继协议。理论分析表明，在拥有高质量量子存储器的实用化网络假设下，双向操作架构相比传统单向方案，能持续获得更高性能且资源开销更低，纠正了此前认为单向更优的认知。

性能优化与容错分析：为工程化铺平道路。

01 基于QLDPC码的容错测量中继器框架

团队设计了一种基于量子低密度奇偶校验码的模块化测量中继器协议。该方案能在任意距离上维持恒定的纠缠分发率，并通过数值模拟确立了其容错操作的错误率阈值，为构建未来大规模、可容忍组件缺陷的量子互联网奠定了坚实的理论基础。

物理实现路径探索：多种平台竞相发展

01 原子-光子混合量子中继方案

中国科学技术大学 University of Science and Technology of China 山西大学 SHANXI UNIVERSITY

提出一种结合里德堡原子阵列（处理器）与光学腔的混合方案。理论模拟显示，该架构在城域距离可实现有意义的纠缠分发速率，为基于冷原子系统的量子中继器描绘了一条清晰的近期实验路径。

02 基于高性能单光子源的模块化中继演示

中国科学技术大学 University of Science and Technology of China 清华大学

实验演示了一个采用确定性单光子源的模块化量子中继原型。在包含三个节点的网络中，系统以304.52 MHz的高重频运行，并在300公里光纤上成功生成安全密钥，首次在实验上将高性能单光子源与中继架构紧密结合，验证了其巨大潜力。

03 面向线性光学的硬件高效单向量子中继架构

UNIVERSITY OF COPENHAGEN

针对线性光学系统，团队设计了基于级联环图码的简洁架构。该方案所需物理量子比特数少，测量方式简单，且分析证明其对传输损耗和操作错误均具有强容错能力，为基于现有光子技术的实用化中继器提供了一个极具吸引力的方案。

总体来看，2025 年量子中继研究已从原理可行性论证，逐步转向围绕效率、容错阈值和资源开销的工程化评估阶段。不同技术路线在实现难度和应用时间窗口上的差异开始显现，量子中继正由统一概念走向多路径并行探索的实用化阶段。

量子存储：性能突破与网络集成验证并行

量子存储器是量子中继与网络同步的关键组件。2025年的进展呈现两条并行主线：一条是效率、噪声与寿命等指标持续提升，另一条是系统形态向紧凑化、机架化、光纤耦合等工程可部署方向演进，并开始在更复杂的网络任务中进行集成验证。

性能极限的持续突破：向高效率、低噪声、长寿命迈进

01 实现接近单位效率的低噪声宽带存储

华东师范大学 中国科学技术大学 University of Science and Technology of China 山西大学 SHANXI UNIVERSITY

通过揭示光-自旋波转换的时空映射并创新性采用智能光操控策略，在热原子蒸汽拉曼存储器上取得了里程碑式进展。实验实现了高达94.6±1%的存储效率，同时将噪声压制至极低的每脉冲0.026个光子。在存储17ns的相干态时，无条件保真度达到98.91%，首次在同一系统中同时满足了高效率、高保真度和低噪声的实用化基准，为高速量子网络奠定了器件基础。

02 高效固态自旋波量子存储器

ICFO Iaac Advanced Architecture Barcelona

基于Pr^{3+}:Y_2SiO_5晶体和原子频率梳协议，团队实现了具备按需读取功能的固态自旋波存储器。该器件在单光子水平下操作，存储效率达(40±2)%，信噪比优异，且从激发态到自旋态的双向转移效率高达83%，并通过存储预示单光子验证了其保持量子非经典关联的能力，是构建固态量子中继器的理想候选。

03 稀土离子光学陶瓷的长相干存储

中国科学技术大学 University of Science and Technology of China 南方科技大学 PSL 哈尔滨工业大学 HARBIN INSTITUTE OF TECHNOLOGY 江苏师范大学 JIANGSU NORMAL UNIVERSITY

在Eu^{3+}:Y_2O_3光学陶瓷中，团队实现了422μs的光学相干时间和超过30小时的自旋态寿命，并演示了基于原子频率梳的相干光存储。该工作为基于高稳健性固态材料的实用化量子存储器开发提供了新的材料体系选择。

实用化与集成化创新：面向可部署与可扩展

01 紧凑型腔增强原子蒸气存储器

团队开发了一种基于离共振级联吸收（ORCA）的腔增强量子存储器。该设计无需原子囚禁或低温冷却，在保持高效率和GHz带宽的同时，实现了更小尺寸和更低功耗，验证了构建大规模、超紧凑量子存储器阵列的可行性，极大降低了未来量子网络节点的硬件复杂度。

02 独立式移动量子存储系统

实现并系统分析了一种可移动、机架式部署的独立运行温原子蒸汽量子存储系统。在单光子条件下保持稳定存储性能，验证了量子存储器脱离实验室环境、面向工程化与移动部署应用的可行性。

03 光纤耦合的“循环-切换”存储器平台

团队展示了一种直接与光纤耦合的“循环-切换”量子存储器。其直通效率达54%，并演示了在数十纳秒到微秒量级的不同存储时间下，对单光子偏振量子比特的高保真存储与检索，突出了在存储寿命与量子比特快速访问之间的灵活权衡能力，适用于不同的网络应用场景。

网络功能与应用验证

01 用于量子密码学原语的存储器集成验证

研究团队将冷原子量子存储器直接集成到一个威斯纳不可伪造量子货币的密码学协议中，利用存储步骤替代动态过程来实现安全机制。该实验不仅演示了协议，更对存储器的效率和噪声水平提出了具体、严苛的定量要求并成功达标，证明了量子存储器在高级量子网络应用中的关键作用。

02 揭示实际系统中的非理想效应与抑制策略

通过对基于氮空位中心的存储器进行精细化建模，团队发现邻近能级与非期望耦合会导致实际存储效率的评估出现严重偏差，甚至在经典噪声可忽略时引入量子噪声。这项工作为所有量子存储器平台提供了重要的性能评估与优化方法论，强调了从“理想模型”转向“全系统物理建模”对实用化至关重要。

综合来看，量子存储器在性能指标持续突破的同时，其工程形态正加速向可部署、可集成方向演进。随着存储器逐步进入实际网络功能和应用验证环节，其角色已从单一器件，转变为量子网络中不可或缺的系统级支撑组件。

量子通信网络：走向标准化与生态化推进阶段

2025年，全球量子通信网络建设进入体系化推进阶段，网络规模扩展、标准与互操作工作以及产业生态组织同步加速。

图表 2025年全球量子通信网络建设与规模化部署重点项目

国家/地区	项目/计划名称	牵头/参与机构	网络类型	建设阶段（2025）
瑞士（欧洲）	日内瓦量子网络	日内瓦大学、CERN、ID Quantique	城域量子通信网络	正式运行
美国	国防级纠缠量子网络	Qunnect、AFRL	城域纠缠量子网络	工程验证/部署
美国	分布式量子网络关键组件	Rigetti、QphoX、AFRL	关键节点技术	工程集成验证
美国	电信波段量子接口	IonQ、AFRL	量子网络关键接口	实验验证
中国	城域/多用户量子网络扩展	上海交通大学、上海电力大学	城域量子网络	实验网络扩展
中国	星地量子通信系统	中科大、上海量子科学研究中心	星地一体化QKD网络	在轨验证
欧洲（德国）	QuNET空地量子通信	DLR	空地量子通信	工程试验
欧洲/全球	天基QKD商用计划	Colt、霍尼韦尔、诺基亚	全球天基量子通信网络	明确路线图
加拿大	蒙特利尔量子安全网络	诺基亚、霍尼韦尔、Numana	区域量子安全网络	生态建设/部署
沙特阿拉伯	国家量子网络联盟	KACST、沙特阿美、微软、思科	国家级量子网络生态	联盟启动

尽管各国推进路径有所差异，但总体上更加注重可复制的工程方案、与现有通信网络的融合验证，并通过联盟与标准化机制，将早期试点经验转化为可推广的建设模式。



美国： 军方需求牵引，企业组件化推进

美国在量子网络方面呈现军方牵引、初创企业活跃、产学研协同紧密的特点，重点在于将关键组件尽快推向可部署形态。

- **面向分布式量子网络的量子处理器—光纤接口验证。**

rigetti QPHOX

获得美国空军研究实验室（AFRL）580万美元合同，合作将超导量子比特与微波-光量子换能器集成，旨在实现量子态在光纤上的传输，目标直指分布式量子计算与安全通信网络。

- **纠缠量子网络向城域规模和国防规范验证推进。** Qunnect

获得美国空军合同，以推进其基于商用光纤的城域规模纠缠量子网络技术的国防应用部署，旨在验证国防级规范，加速国家安全场景下的量子通信技术落地。

- **量子处理器与现有电信光纤的直接对接验证。** IONQ

在空军研究实验室支持下，成功演示了将离子阱系统光子从可见光到电信波段的频率转换，这一里程碑进展使其量子处理器能直接利用现有电信光纤进行长距离量子信息传输，极大增强了量子网络的可扩展性。



中国： 网络规模探索与异构互联验证并重

中国侧重扩大网络规模上限、验证多用户协议与实现网络间互联，为更大尺度的量子互联网形态探索架构路径。

- **多用户量子网络的互联与规模扩展验证。**

成功演示了基于多用户纠缠交换的两个独立量子网络的“融合”，将两个10用户网络合并为一个拥有18个用户的更大网络。 上海交通大学 Shanghai Jiao Tong University 山东师范大学 SHANDONG NORMAL UNIVERSITY 上海量子科学研究中心 Shanghai Research Center for Quantum Sciences

➢ **全光量子网络向更高用户规模扩展。**

利用超透镜阵列实验生成了一个5×5的连续变量EPR纠缠阵列，并基于此构建了目前连续变量体系中规模最大的五用户全光量子态共享网络，保真度超越经典极限，为构建大规模全光量子网络提供了创新平台。

➢ **量子网络中可信纠缠验证机制的实验实现。**

华东师范大学、山西大学等联合团队：在量子网络中实验实现了与测量设备无关的纠缠见证。该方法能抵御因测量设备不可信而导致的虚假纠缠认证攻击，为构建安全可信的量子网络提供了至关重要的检测工具。

欧洲:跨国协同与基础设施平台化推进

欧洲强调跨国协作、统一框架与基础设施共建，形成可复用的区域创新平台。

➢ **以区域协同网络和标准体系建设为双重抓手推进量子网络。**

日内瓦量子网络正式启用：由日内瓦大学、欧洲核子研究中心、ID Quantique等机构合作建设的日内瓦量子网络正式启用。该网络全长262公里，基于城市现有光纤，连接了主要研究和工业场所，是一个大规模、多功能的量子通信与计量实验平台，成为欧洲区域协同创新的典范。

➢ **空天地一体化量子通信的工程可行性验证。**

德国航空航天中心（DLR）：在QuNET国家计划框架内，于机载量子通信研究中取得重要进展，实现了飞机与地面站间通过多个量子通道传输光子至离子阱系统，并对多种QKD方法进行了验证，为构建空天地一体化安全通信网络奠定了基础。

➢ **通过标准体系建设强化量子网络规则主导权**

ETSI成立量子技术委员会：如前所述，这一举措旨在系统性制定覆盖量子通信、网络、传感的全套欧洲标准，强力支撑 “欧洲量子通信基础设施” 等战略项目，确保欧洲在量子网络规则制定中的话语权。

其他国家与地区：以联盟与合作切入，建设本土生态

加拿大、澳大利亚、沙特阿拉伯等国家通过产业合作、学术研究等方式，积极切入量子网络赛道，旨在培育本土产业并参与全球竞争。



- **加拿大：以产业协同方式推动量子安全网络商业化落地。**

产业合作推动商业化。诺基亚、霍尼韦尔与Numana公司建立战略合作伙伴关系，旨在推进加拿大蒙特利尔及全球的量子安全网络，加速企业和服务提供商对下一代安全网络技术的采用。



- **沙特阿拉伯：通过国家级联盟构建量子网络创新生态。**

启动国家联盟构建生态。阿卜杜勒阿齐兹国王科技城联合沙特阿美、微软、思科等国家与全球巨头，启动了沙特量子网络联盟，旨在建立综合生态系统，加强国家数据与通信安全，将沙特定位为区域量子创新中心。





- **澳大利亚与芬兰：以前沿理论探索未来量子网络商业范式。**

前沿学术研究探索网络新范式。悉尼科技大学与阿尔托大学联合研究提出基于“潜行者网络”和交易纠缠的商业化量子网络设想，并分析了使用量子低密度奇偶校验码在资源效率上的优越性，为未来大规模商用量子网络提供了新颖的理论框架。

星地一体化量子网络：从单点演示走向路线图与在轨融合

星地一体化被普遍视为扩展量子网络覆盖范围的重要方向。2025年的变化在于：技术路线更加多元，目标更加明确，部分产业主体开始把服务落地时间表写进规划。

图表 2025全球各国家地区量子通信系统分布情况



iCV TA&K | 2026.2

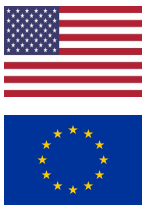
向微小型化与可组网形态收敛

中国继续保持工程推进优势，发展重点从大型科学实验系统转向低成本、可复制的微小型系统。

工程突破：量子微卫星与便携式地面站实现重大轻量化

中国科学技术大学 University of Science and Technology of China

成功研制并报告了新一代量子微卫星及其便携式地面站。卫星有效载荷重量降至约23公斤，地面站重量约100公斤，均较上一代系统降低了1-2个数量级。该微卫星系统成功演示了与多个地面站的量子密钥分发，在单次卫星过境期间实现了高达107万比特的安全密钥共享，并首次在星地链路上将双向经典光通信与量子通信进行同光路复用，实现了密钥的实时提炼与安全通信。



产业联盟驱动商业化时间表

欧美力量正通过组建强大的产业联盟，整合航天、通信与网络安全巨头，制定了清晰的天基量子安全网络商用计划，旨在抢占未来全球量子服务市场。

商业计划：发布全球天基QKD服务明确时间表

COLT Honeywell NOKIA

三方宣布合作，计划利用低地球轨道卫星测试抗量子加密技术，核心目标是评估天基QKD在超远距离（特别是跨洋）密钥传输中的应用。该联盟公布了清晰的商用路线图：计划于2026年第三季度利用QEYSsat卫星构建演示平台进行初期测试；并瞄准2027年第三季度通过发射QKDsat卫星，正式推出覆盖全球企业节点的商用QKD服务。

技术融合：在轨部署抗量子密码与区块链新应用

SEAL SQ semiconductors + quantum WISeSat

EALSQ与WISeSat公司：合作研发的WISeSat 3卫星成功发射。该卫星的独特之处在于，首次在太空直接部署了符合NIST标准的抗量子密码硬件，实现了PQC算法的在轨密钥生成与管理。同时，卫星集成了SEALCOIN区块链平台，旨在构建一个“轨道级去中心化物理基础设施网络”，支持安全的天地间代币交易与身份验证。

04 标准化工作进展

2025年，随着量子保密通信在多个国家和地区由示范验证逐步走向工程化部署，标准化问题的重要性进一步凸显。

由于尚未形成统一、成熟的行业标准，不同国家和企业在技术路线选择、系统架构设计和工程实现方式上仍存在明显差异，难以形成规模效应和稳定的协同机制。这种分散发展不仅带来了重复研发和资源配置效率偏低的问题，也在一定程度上推高了系统建设和运维成本，制约了量子保密通信在更广泛场景中的应用推广。

在此背景下，2025年全球量子保密通信标准化工作的推进逻辑，仍以政府部门和国际标准化组织牵头为主，通过标准制定与协调，引导产业在相对统一的框架下有序发展。与早期侧重技术探索和原型验证不同，各国政府更倾向于将标准作为制度性引导工具，在不提前固化具体技术路线的前提下，逐步明确关键技术指标、接口规范和工程实施要求，为产业协同创造基础条件。



政府牵头推进标准化，引导量子保密通信走向协同发展

从全球实践看，各主要国家和地区在2025年普遍延续了以政府主导、产业和科研机构共同参与的标准化推进路径。

一方面，政府通过支持标准立项、发布技术规范和推动标准试点应用，引导企业围绕网络安全要求、系统互操作性和工程可实施性等共性问题开展研发，避免在基础能力层面形成无序竞争；

另一方面，国际标准化组织通过协调不同国家和技术路线的需求，为量子保密通信的跨系统互联和跨区域应用提供共同参考框架。

这种由政府牵头、多方协同推进的标准化模式，正在成为缓解量子保密通信领域碎片化问题的重要手段。通过逐步明确安全要求、工程边界和运行管理规则，相关标准在不同技术路线之间建立起最小共识，为后续更大范围的产业协同与网络互联奠定基础。

标准化工作逐步向实用化与工程化推进

图表 全球量子保密通信标准制定进程概况

2023.12

国盾量子
北京邮电大学
循态量子等

由中日（韩）联合立项发起，国盾量子作为中方主要代表

中国工业和信息化部

- 《量子密钥分发与经典光通信共纤传输技术要求》(YD/T 4632-2023)
- 《量子密钥分发(QKD)系统测试方法 第2部分:基于高斯调制相干态协议的QKD系统》

国际电信联盟电信标准化局（ITU-T）

- 批准通过5项量子密钥分发（QKD）网络协议相关标准，包括QKD网络的协议框架（Q.4160）、Ak接口协议（Q.4161）、Kq-1接口协议（Q.4162）、Kx接口协议（Q.4163）、Ck接口协议（Q.4164）

2024.01

欧洲电信标准化协会（ETSI）

- 量子密钥分发：通用标准保护配置文件——对准备与测量
- 量子密钥分发模块

2024.03

国盾量子牵头/参与多项标准的制定

中国国家市场监督管理总局、国家标准化管理委员会

- 中国首个关于量子通信术语的正式标准《量子通信术语和定义》

2024.04

中国通信标准化协会归口，国科量子牵头，联合国盾量子、新加坡国立大学共同制定

国际电信联盟

- 《量子密钥分发节点保护的安全要求》国际标准

中国工业和信息化部

- 《基于BB84协议的量子密钥分发(QKD)用关键器件和模块 第4部分:诱骗态调制模块》

2024.10

由国盾量子、中国信通院、中国信科集团等单位牵头制定

中国工业和信息化部

- 批准发布了6项量子密钥分发（QKD）领域行业标准

2024.12

济南量子技术研究院、国盾量子等参与起草

中国工业和信息化部

- 发布《量子密钥分发（QKD）网络安全技术要求》
- 《基于传输层密码协议的量子保密通信应用设备技术规范》

2025.04

由TC312归口，中国科学技术大学、国盾量子等共同参与

国际电信联盟

- 发布 QKD 网络控制与运维管理标准
- 发布 QKD 网络 QoS 参数测量方法标准

中国科学院

- 起草《空间量子密钥分发（QKD）系统技术要求》

2025.07

由中国通信标准化协会归口上报，中国信息通信研究院、国盾量子等产学研各方参与

中国工业和信息化部

- 发布《量子密钥分发（QKD）网络 网络管理技术要求 第5部分：网元管理系统（EMS）功能》
- 《量子随机数发生器技术规范》

iCV TA&K | 2026.2

总体而言，2025年量子保密通信的标准化工作仍处于持续完善阶段，尚未形成全球统一、覆盖全面的标准体系，但其在引导研发方向、减少重复投入和推动产业协同方面的作用已逐步显现。随着应用规模扩大和跨行业需求增加，政府牵头的标准协调机制有望在未来进一步深化，成为支撑量子保密通信长期发展的重要制度基础。



03

抗量子密码

目录 03 抗量子密码

01 抗量子密码算法

02 关键工程技术与抗量子密码芯片

03 抗量子密码迁移路线与落地进展

04 标准化工作进展

01 抗量子密码算法

抗量子密码算法是指在经典计算机和未来量子计算机攻击模型下，仍能够保障信息机密性、完整性与真实性的一类公钥密码算法体系。随着量子计算能力持续提升，传统依赖大数分解和离散对数难题的公钥密码体制面临潜在失效风险，抗量子密码已逐步成为全球信息系统实现长期安全的重要技术基础。



从算法确立走向安全体系完善

2025年，抗量子密码算法的发展重心出现明显转变。在核心算法体系基本确立的背景下，全球研究与产业界的关注点不再集中于“选择哪一种算法”，而是转向如何构建具备长期韧性和风险分散能力的整体密码结构，以应对未来可能出现的数学突破和实现层风险。

这一变化的直接体现，是主流标准体系开始有意识地引入多数学基础并行的算法布局。2025年3月，美国国家标准与技术研究院（NIST）宣布选定HQC算法，作为抗量子加密体系中的补充性候选方案，用于在通用密钥封装机制（ML-KEM）之外提供备用选择。HQC基于纠错码理论，其安全假设与当前主流的格密码路线存在明显差异，旨在降低长期运行中对单一数学结构的依赖风险。NIST同时明确，HQC并非替代现有主算法，而是作为风险管理层面的补充，并将在后续阶段推进标准草案与工程研究。

这一进展释放出清晰信号：抗量子密码标准体系在既有多算法框架基础上，开始进一步强调数学基础的多样化与冗余配置：在以格密码方案为核心工程路径的同时，引入基于不同困难问题的备选算法，以降低对单一路线的集中依赖，提升长期安全的韧性与风险可控性。

从全球范围看，欧洲、亚太等地区在2025年的相关研究与应用评估中，也普遍延续这一思路。在将已标准化算法作为工程基础的同时，持续跟踪和评估其他数学路线的安全性与实现可行性，以避免技术路径过度集中。这表明，抗量子密码算法的发展已进入以体系安全和长期可控性为核心的新阶段。

抗量子密码算法的主要分类体系

从数学基础和安全假设角度看，抗量子密码算法通常可划分为若干主要类别，包括基于格、基于编码、基于多变量、基于哈希函数以及其他路线。各类算法在安全假设、计算复杂度、密钥与签名规模以及实现成本等方面存在显著差异，适用于不同的系统环境和应用场景。

图表 抗量子密码算法分类及简介

1	基于格的算法	➢ 基于格的算法以高维格问题为安全基础，在理论成熟度、性能与工程可实现性之间取得相对平衡，是目前抗量子密码体系中的主流路线。 ➢ 该类算法广泛应用于密钥封装和数字签名等核心场景，易于集成到现有通信协议和系统架构中，因此在全球范围内率先进入规模化部署阶段。
2	基于编码的算法	➢ 基于编码的算法依托纠错码相关数学难题，具有清晰的安全模型和较长的研究历史。主要挑战在于密钥尺寸和通信开销，但在安全多样性方面具有重要补充价值。随着备用算法机制的引入，该类算法在抗量子密码整体体系中的战略地位进一步凸显。
3	基于多变量的算法	➢ 该类算法基于多变量多项式方程组求解问题，主要面向数字签名应用，具有计算效率较高的优势。 ➢ 由于部分方案在历史上出现过安全性下降，其工程化应用仍以审慎推进为主，更多用于研究验证和特定场景探索。
4	基于哈希函数的算法	➢ 基于哈希函数的算法依赖哈希原语的安全性假设，结构相对简单且安全性稳健，适用于对长期可信性要求极高的数字签名场景。 ➢ 该类算法通常在签名长度和状态管理方面存在一定工程成本，但在高安全等级应用中具备独特价值。
5	其他算法	➢ 除上述类别外，还包括基于同源映射等其他数学结构的抗量子算法。这些算法在学术研究和实验性系统中持续推进，但受限于复杂度和验证周期，2025 年仍主要处于探索阶段。

综合来看，2025年抗量子密码算法的发展呈现出清晰的阶段性特征：

一是从“确定可用算法”转向“构建可持续的算法体系”，通过多数学基础并行降低长期系统性风险；

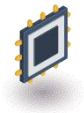
二是更加重视算法在真实系统中的运行稳定性和可演进能力，而非单纯追求理论最优指标；

三是为后续的系统集成、芯片实现和大规模迁移奠定了更加稳固、可扩展的算法基础。

02 关键工程技术与抗量子密码芯片

随着抗量子密码算法逐步进入实际应用与工程验证阶段，其能否稳定运行、长期维护，越来越取决于工程实现能力本身。

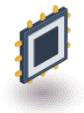
2025年，全球范围内的研究与产业实践表明，抗量子密码已不再只是算法问题，而是涉及计算架构、系统集成与硬件实现的综合工程体系。安全芯片及相关工程技术，正在成为支撑抗量子密码可部署、可运维与可演进的重要基础。



工程化实现成为抗量子密码落地的关键条件

抗量子密码算法在计算结构上普遍涉及多项式运算、随机采样、数论变换以及矩阵与向量的模运算等复杂过程。在通用计算平台上，这些运算具备可实现性，但在通信网络、终端设备和关键基础设施等长期运行场景中，对时延、吞吐和能耗的约束更为严格。

2025年的工程实践显示，越来越多系统在设计阶段即同步考虑算法选择与实现路径，通过架构划分、算子优化和计算调度，使抗量子密码在既定资源条件下保持稳定运行。这一趋势表明，工程实现能力已与算法安全性一道，成为决定系统整体安全水平的核心因素。



软硬件协同成为主流实现路径

在实际部署中，抗量子密码既需要保持算法和协议层面的灵活性，又必须满足执行效率和安全隔离要求。2025年，软硬件协同的实现方式逐步成为主流路径。

在该模式下，软件层负责算法调度、协议适配与系统集成，硬件层则通过专用计算单元或安全模块承担高频运算、密钥保护和可信执行等任务。将抗量子密码功能集成至安全芯片或SoC的安全子系统，可在不改变系统整体架构的前提下，提升执行效率并增强安全边界的可控性。

这种协同方式并不固化具体算法，而是通过模块化和接口化设计，为参数调整和算法更新预留空间，有利于抗量子密码在不同系统环境中的持续部署。

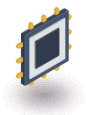


面向不同应用场景的芯片设计呈现差异化

随着抗量子密码应用范围不断扩大，其芯片实现开始呈现明显的场景分化特征。

在终端设备、物联网节点和部分移动通信场景中，设计重点通常放在能效与资源占用控制上。通过优化计算路径、采用混合密码模式以及合理分配软硬件职责，抗量子密码得以适配资源受限环境，从而推动其向更广泛的终端侧场景延伸。

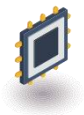
在云计算平台、数据中心和通信骨干网络等场景中，实现方案则更强调吞吐率、并行处理能力和长期运行稳定性，以支撑高频密钥协商和大规模认证需求。这类系统中，抗量子密码芯片往往依托多核或并行架构，与系统级调度和负载管理机制协同工作。



从算法安全走向工程实现安全

在工程实现过程中，抗量子密码系统同样面临实现层安全挑战。随机采样、模运算和密钥相关操作在执行过程中，可能通过功耗、电磁或时间特征泄露信息，从而引入侧信道风险。

2025年的相关实践显示，侧信道防护正逐步被纳入抗量子密码芯片和系统设计流程。通过在关键模块中引入防护电路结构、运算随机化以及运行状态监测机制，可在一定程度上降低实现层攻击风险。这类措施通常与算法层安全设计配合使用，共同提升系统整体防护水平。



系统对算法更新的适应能力不断增强

由于抗量子密码算法仍处于持续演进阶段，系统设计须具备适应算法更新和参数调整的能力。进入2025年，加密敏捷性逐渐成为抗量子密码芯片与系统架构中的重要设计目标。

通过可配置计算单元、模块化接口以及可升级固件设计，系统能够在不更换硬件的情况下支持不同算法和参数组合。这种设计思路有助于降低长期运维风险，并提升系统对未来标准演进的适应能力，为抗量子密码在关键系统中的长期应用提供支撑。

总体来看，2025年抗量子密码关键工程技术与安全芯片的发展，呈现出算法设计与工程实现协同推进的特征。通过软硬件协同、场景化芯片设计、实现层安全防护以及加密敏捷性等工程手段，抗量子密码在多种系统环境中的可部署性和可持续性不断提升，为后续规模化迁移与应用奠定了更加稳固的技术基础。

03 抗量子密码迁移路线与落地进展

抗量子密码迁移（PQC Migration）是一项典型的长链条系统工程，既包括算法与协议的替换，也涵盖密码资产治理、供应链协同、性能与互操作验证以及合规与审计要求适配等多维度工作。

图表 抗量子密码迁移路线图



iCV TA&K | 2026.2

当前主流的抗量子密码迁移路径已被拆解为若干可执行的工程阶段，通常包括准备与基线理解、规划与执行、以及监控与评估等环节。这一路线图的意义不在于规定统一节奏，而在于为组织提供一套可对齐风险、资源与业务连续性的迁移框架，使迁移从概念层面的应对量子威胁转化为可落地的工程任务。



迁移重点由算法替换转向整体治理与渐进部署

在全球范围内，抗量子密码迁移的工程方法已逐步形成共识：加密资产清单与依赖关系梳理是迁移工作的起点。通过系统性识别密钥、证书、协议与算法的实际使用情况，组织能够明确量子风险的分布位置，并据此制定迁移优先级，而非盲目追求全面替换。

在此基础上，混合部署成为过渡期的主流实践路径，即在关键系统中同时运行传统算法与抗量子算法，以在安全性、兼容性与系统稳定性之间取得平衡。这种方式避免了对现有业务造成结构性冲击，也为性能评估和工程验证留出缓冲空间。

与此同时，密码敏捷性逐步被纳入系统架构设计的核心要求。通过模块化、可配置的密码接口，系统能够在不重构整体架构的前提下切换算法或参数组合，使迁移从一次性工程转变为可持续演进的能力建设。



多算法与多标准并行增强迁移稳定性

迁移策略的长期稳健性，在很大程度上取决于算法体系对不确定性的适应能力。随着抗量子密码标准体系逐步成熟，不同数学基础的算法被纳入同一安全框架，为关键系统提供差异化的安全备份路径。

这一变化并不意味着简单增加算法数量，而是促使组织在系统设计和采购阶段，提前考虑算法组合与切换机制。在实际迁移实践中，关注点正从“采用哪一种算法”转向“是否具备可演进、可替换的算法体系”，从而为关键业务系统的长期运行预留回旋空间。



不同国家和地区采取差异化推进路径

在具体落地层面，不同国家和地区基于自身安全治理模式与产业结构，形成了差异化的迁移推进方式，但总体均围绕路线图规划、试点验证与产业供给能力建设并行展开。



美国：
美国更加注重通过完善治理工具，并在公共部门中同步推进应用

在公共部门层面，迁移工作的起点集中于加密资产的系统性识别与风险评估。例如，SandboxAQ与国防相关部门首席信息官达成长期合作协议，围绕加密资产发现、清点与管理展开工作，为后续替换和优先级排序奠定基础。

在产业供给侧，抗量子密码能力以产品化形式进入政府采购体系。Carahsoft与QuSecure的合作，使具备密码敏捷能力的抗量子网络安全产品通过既有政府采购渠道进入公共部门，加速试点和推广进程。

与此同时，抗量子密码也开始嵌入更广泛的行业系统中，包括智慧城市平台、专用5G无线电单元以及高性能计算与GPU服务器环境，表明迁移正从传统IT网络向OT、边缘计算和关键基础设施延伸。



英国：
在迁移推进中更侧重长期规划与阶段性目标管理

英国国家网络安全中心（NCSC）发布的抗量子密码迁移路线图，为组织设定了明确的风险评估、策略制定与分阶段实施框架，并提出在中长期内完成系统性过渡的目标。

在此基础上，通过试点项目将路线图要求转化为可执行流程。例如，Arqit入选NCSC主导的抗量子密码试点项目，为金融、电信和关键基础设施等领域提供“发现—评估—规划”的迁移服务路径。

此外，在电信网络层面，Arqit与Sparkle在运营商骨干网络中完成的抗量子加密概念验证，展示了在不显著影响链路性能的情况下引入抗量子能力的可行性，反映出英国在高可靠通信场景下推进迁移的现实关注重点。



欧盟：
注重机制规范与互操作性建设

欧洲电信标准协会（ETSI）发布的抗量子安全技术规范TS 104 015，为混合密钥交换和访问控制提供了统一实现框架，有助于降低跨运营商、跨行业系统在迁移过程中的互操作风险。这类标准的出台，使抗量子密码迁移能够在多供应商、多国家环境中以更低成本复制扩展，契合欧盟跨区域基础设施和统一市场的应用需求。



韩国：
以公共系统试点为切入点，并逐步向终端和用户侧延伸

在政务和关键业务系统层面，LG Uplus参与将抗量子密码模块应用于韩国通信委员会（KCA）的核心系统，包括VPN、VDI及在线测试平台等，完成了实际运行环境下的验证。

同时，韩国在终端与身份认证场景推进较快，金融科技企业推出基于抗量子密码的认证解决方案，三星电子也在移动终端的Secure Wi-Fi服务中引入抗量子密码机制，使迁移成果逐步转化为用户可感知的安全能力。



中国：
产业协作与行业场景牵引并行推进

一方面，通过产业链上下游联合研发，将抗量子密码能力嵌入云平台、智能终端和行业应用系统。例如，车企与云服务提供商围绕抗量子安全算法开展合作，将相关能力扩展至智能汽车、车联网及关联的数字基础设施。

另一方面，围绕量子信息与密码技术的标准化体系建设持续推进，相关标准化技术委员会的筹建为抗量子密码在接口规范、测试方法和工程实践层面的统一提供制度基础，有助于降低迁移过程中的重复投入并提升可复制性。

总体而言，各国和地区在抗量子密码迁移中采取了不同的实施路径，但均通过路线图规划、试点项目和产业能力建设等方式推动迁移从概念走向工程实践。差异化推进模式的并存，反映出抗量子密码迁移在全球范围内仍处于探索与加速并行阶段。



平台化能力和交付体系逐步完善

随着云平台、操作系统和终端厂商将抗量子密码能力纳入基础产品功能，迁移的实施门槛正在显著降低。通过标准接口和托管服务，抗量子密码逐步从安全团队的专项工程，转变为可直接调用的通用能力，对整体迁移节奏产生放大效应。

从交付视角看，迁移已形成较为清晰的链条：前期通过资产可见化和风险评估支撑决策，中期通过试点和工程验证评估性能与兼容性，后期将迁移成果纳入合规审计与运维体系，使抗量子能力成为长期治理的一部分。

总体而言，抗量子密码迁移正由准备与探索阶段，迈向工程化、体系化实施阶段。尽管不同国家和行业在节奏与侧重点上存在差异，但分阶段推进、混合部署和可持续演进已成为普遍特征。短期内全面替换传统密码体系仍面临现实约束，但围绕资产治理、平台化能力和标准规范构建的迁移路径正在逐步清晰，并持续向通信网络、公共系统、终端设备和云平台等关键领域扩展。

04 标准化工作进展

在抗量子密码由算法确立迈向工程部署的过程中，标准化已成为影响迁移能否有序推进和规模化落地的关键因素。

抗量子密码的引入并非简单的算法替换，而是会系统性影响密钥交换、数字签名、证书与密钥管理、密码模块验证、协议兼容性以及性能约束等一整套工程环节。如果缺乏统一、可对齐的标准和测试框架，不同厂商和行业用户在算法选型、参数配置、实现路径和合规证明上的分散决策，容易导致生态碎片化、互操作难度上升，并显著增加迁移成本。

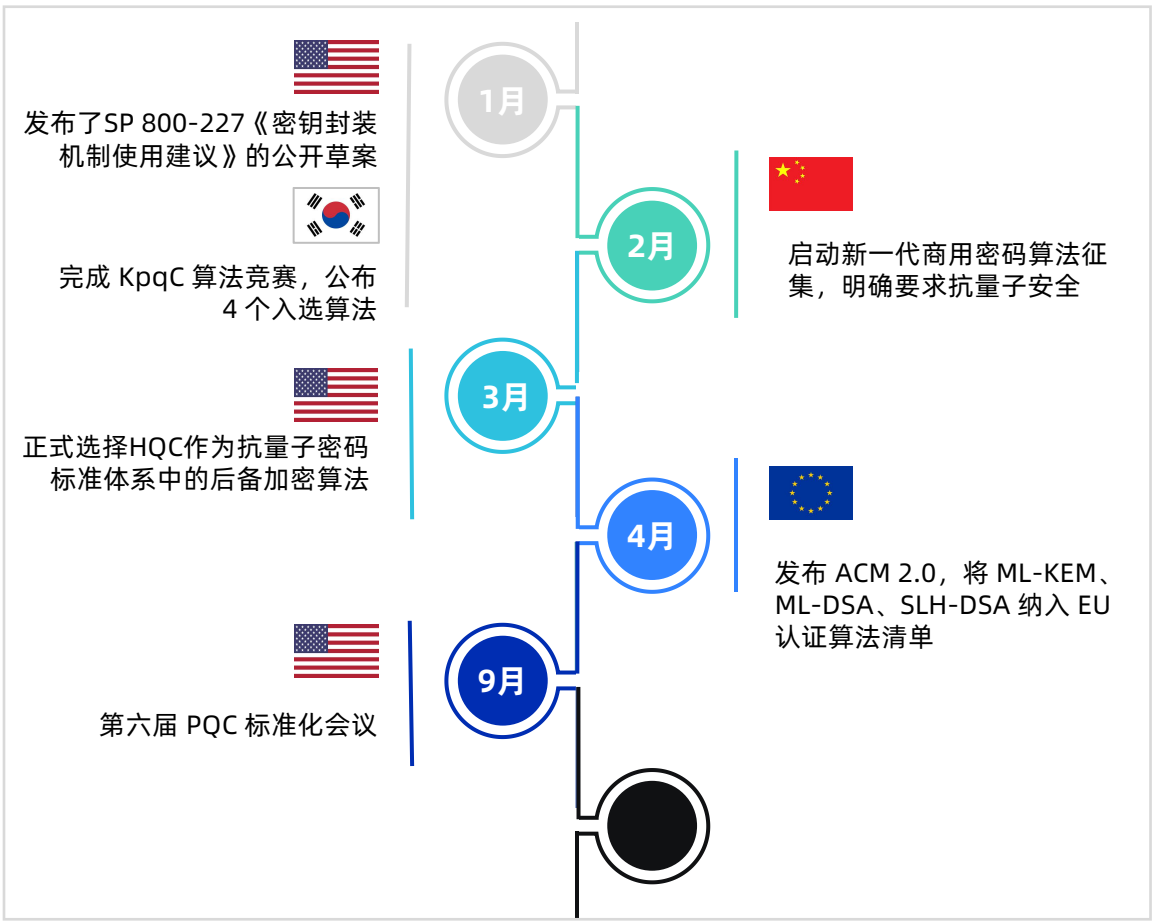
与此同时，抗量子密码迁移在实践中更接近一项长期治理任务，而非一次性技术升级。抗量子能力需要在通信、安全服务、软件更新、身份体系以及终端和物联网设备等多类系统中逐步引入，并在不影响业务连续性的前提下完成演进。这一过程进一步凸显了标准体系的基础性作用：一方面，将安全目标转化为可执行的工程规范，明确算法组合、接口要求、性能边界和审计规则；另一方面，为跨供应链协同提供统一参考，支撑平台商、设备商与行业用户开展测试、验收和规模部署。

从全球趋势看，抗量子密码标准化正在由顶层治理逐步向工程层面细化推进。国家和区域层面通过路线图和合规要求拆解迁移任务，国际标准组织加快机制规范与互操作框架建设，而平台型企业则通过密码库、操作系统、浏览器和云服务等实现路径，将相关标准转化为可直接使用的能力。

综合来看，当前抗量子密码标准化工作的重心已逐步集中到三条主线：

面向迁移全过程的治理框架建设、支撑跨系统协同的工程互操作规范，以及服务于产业落地的实现与验证体系。

图表 2025全球抗量子密码标准化工作进展



iCV TA&K | 2026.2

国家级标准与治理主体

美国:NIST（国家标准与技术研究院）

由算法定型转向工程化治理

2025年，在抗量子密码算法标准已完成制定并落地实施的背景下，美国国家标准与技术研究院将工作重心转向工程化与体系完善。

在算法体系层面，NIST正式宣布选择基于错误校正码的密钥封装算法HQC，作为抗量子密码标准体系中的后备加密算法。HQC采用准循环Hamming码构造，代表了与格密码不同的密码学技术路线。其引入并非针对现有主算法的性能或安全性缺陷，而是出于长期风险管理的考量，为抗量子密钥封装机制提供数学基础上的多样性冗余。

在工程规范层面，NIST发布了SP 800-227《密钥封装机制（KEM）使用建议》的初稿公开草案，并启动公众征求意见程序。该文件并不定义新的密码算法，而是围绕已标准化和候选的抗量子KEM，系统说明其在实际系统中的使用方式，包括混合部署原则、密钥生成与派生流程、协议集成注意事项以及实现层面的安全要求。

在标准治理与持续演进机制方面，NIST于2025年继续通过抗量子密码标准化会议推动全球协同与技术收敛。第六届PQC标准化会议于9月24日至26日举行，会将重点讨论现有标准的实施反馈、附加数字签名方案的评估进展，以及未来标准维护与扩展方向。通过这种定期、公开的评估机制，NIST试图确保抗量子密码标准并非一次性定型，而是能够随着密码分析进展和工程实践不断修正与演进。

总体来看，2025年的NIST抗量子密码工作呈现出明显的阶段特征：算法体系更加稳健，工程使用规则逐步清晰，标准治理进入常态化运行。这一阶段性变化表明，美国已将抗量子密码视为需要长期维护和持续治理的国家级安全基础能力，而不仅仅是一轮算法替换工程。这种从标准发布走向工程与制度配套的推进方式，正在对全球抗量子密码迁移路径产生示范效应。

图表 美国NIST主导的抗量子密码项目时间线概览





中国：国家密码管理局主导

抗量子密码标准化的推进与阶段性布局

中国政府在抗量子密码标准化方面正通过顶层规划与行业标准制定体系积极布局，强调在新一代密码算法标准中纳入抗量子安全性要求，并逐步构建自主标准框架。

2025年2月，国家密码管理系统下的商用密码标准研究院发布了《关于开展新一代商用密码算法征集活动的公告》，面向全球征集新一代公钥密码、杂凑算法和分组密码算法方案，明确提出了应对量子计算威胁、推动新算法标准制定的总体安排。此次征集活动覆盖国内外算法方案，旨在通过公开评估与遴选，为后续商用密码标准的更新与抗量子密码算法融入提供基础。

从整体路径看，中国已将抗量子密码能力明确纳入新一代商用密码标准体系的规划与准备阶段，并通过算法公开征集、技术评估与标准预研等机制，持续推进相关标准化工作。

虽然目前中国尚未发布正式的国家级抗量子密码算法标准，但从政策导向、征集要求与组织方式看，中国正在为后续标准制定与工程化应用打基础、搭框架，其标准化进程已进入持续推进的关键阶段。



欧盟：ENISA（欧盟网络与信息安全局）

通过认证体系与实施指南推进抗量子密码落地

2025年，欧盟在抗量子密码（PQC）领域的工作重点并不在于推出新的算法标准，而是放在迁移统筹、合规指引与认证体系建设上，力图通过制度工具推动成员国有序过渡。

在政策基础上，欧盟延续了此前的总体安排。欧盟委员会于2024年发布的《向抗量子密码过渡的协调实施路线图建议》为成员国确立了统一的迁移方向，并明确由ENISA等机构参与算法评估与实施支撑。这一文件在2025年继续作为欧盟层面推进PQC迁移的核心政策参考。

在具体落地层面，2025年4月，欧盟网络安全认证机构ECCG 在ENISA支持下发布了《商定加密机制清单（ACM）2.0》。这是欧盟首次在网络安全认证框架中系统性纳入抗量子密码算法。清单收录了NIST已标准化的主要算法，包括ML-KEM、ML-DSA、SLH-DSA，同时也保留了FrodoKEM等欧洲长期关注的方案。

与此同时，ENISA还联合ETSI等机构，持续强调混合密码作为过渡期的现实选择，即在现有系统中并行使用传统公钥算法与抗量子算法，以降低迁移风险并保持系统兼容性。这一建议已成为欧盟技术指南中的共识性原则。

总体来看，欧盟尚未独立制定新的抗量子密码算法标准，而是选择在技术选型上与国际主流保持一致，通过路线图、认证清单和实施指南引导成员国推进统一的PQC迁移。



韩国：TTA（韩国电信技术协会）

通过国家级算法竞赛形成自主抗量子密码标准

韩国在2025年实现了本国抗量子密码标准化进程中的关键节点，成为少数通过自主算法遴选推进PQC标准落地的国家之一。其推进路径以国家安全需求为牵引，强调本土算法能力与标准体系的协同构建。

自2021年起，韩国国家情报院（NIS）和国家安全研究所（NSR）联合主导开展“韩国抗量子密码（KpqC）算法竞赛”，围绕数字签名和密钥封装等核心能力，对候选算法进行系统评估。该竞赛于2025年1月正式公布最终结果，选定四种算法作为韩国抗量子密码标准的基础，其中包括两种数字签名算法HAETAE和AIMer，以及两种公钥加密/密钥封装算法SMAUG-T和NTRU+。

按照韩国既定的PQC推进路线，这四种算法将由韩国电信技术协会（TTA）在2025年底前后完成国家标准制定并发布。这一进展标志着韩国已从算法研究阶段，迈入以国家标准为核心的工程化与应用准备阶段，为后续在通信、政务和关键基础设施中的实际部署奠定基础。

国际与区域标准组织

ISO/IEC（国际标准化组织/国际电工委员会）推进抗量子密码算法与通信协议的国际标准预研布局

2025年，ISO/IEC在抗量子密码标准化方面的工作重心进一步展开，呈现出同时覆盖算法层与协议层的推进态势，但整体仍以预研和工作组阶段为主。

在算法层面，ISO/IEC JTC 1/SC 27（信息安全技术分委员会）持续跟踪NIST抗量子密码标准化进程，并在此前阶段已将FrodoKEM等候选算法纳入ISO标准草案体系，作为对NIST主流算法选择的补充。

在协议与系统层面，ISO/IEC 的动作更为明确。2025年，ISO/IEC JTC 1/SC 6（通信系统间信息交换分委员会）启动了面向抗量子安全通信协议的国际标准预研项目。在2025年6月于伦敦召开的SC 6会议上，由中国专家牵头提出的“抗量子攻击的通信网络安全协议设计指南”预研项目获得成员国一致认可。

总体来看，ISO/IEC在2025年加快了对抗量子密码相关标准的前期布局，尤其在通信协议与工程方法论方面开始形成清晰研究路径。



ETSI（欧洲电信标准协会）

围绕混合加密机制发布面向工程落地的量子安全规范

2025年，ETSI在抗量子密码标准化方面的工作重点，集中于为通信系统提供可工程化落地的过渡方案，尤其强调混合加密机制在现实网络中的可用性。

2025年3月25日，ETSI正式发布ETSI TS 104 015技术规范《高效量子安全混合密钥交换及隐藏访问策略》。该规范提出了一种具备访问控制能力的密钥封装机制（KEMAC），即Covercrypt方案。其核心思路是在混合加密框架下，将会话密钥与访问属性绑定，使访问策略在加密封装过程中被隐式表达。只有满足既定策略的授权用户，才能成功解封并获得会话密钥，即便攻击者具备量子计算能力也无法绕过访问控制。

除具体规范外，ETSI还与ENISA在多份指南和技术建议中明确提出，过渡阶段应优先采用混合加密模式，即在密钥协商或加密过程中同时使用传统公钥算法（如ECC）与抗量子算法。这种做法旨在在保持现有系统兼容性的同时，引入面向未来的安全冗余，降低一次性切换带来的工程与运维风险。

总体来看，ETSI在2025年并未推出针对单一抗量子算法的独立标准，而是通过Covercrypt等规范和配套指南，重点回应产业在过渡期面临的工程实施问题。其标准化路径更加偏向通信系统与访问控制层面的实用方案，为运营商和设备厂商提供了可直接参考的技术框架。

ITU-T（国际电信联盟电信标准化部门）

聚焦量子安全通信架构，开展QKD与PQC协同研究

2025年，ITU-T在量子安全方向的工作重点，仍然放在通信体系层面的整体安全架构研究上，尤其关注量子密钥分发与抗量子密码在现实网络中的协同应用方式。

ITU-T第17研究组（SG17）延续了此前启动的“混合量子安全通信密钥管理”研究工作。相关技术报告系统分析了现有量子安全通信方案的工程差距，指出单独依赖QKD在设备成本、部署复杂度和网络覆盖方面存在现实限制，而PQC虽更易集成，却仍面临标准、协议细化与长期安全评估等问题。因此，报告提出在过渡阶段结合QKD与PQC的混合密钥管理策略：在关键场景中同时引入由QKD分发的密钥和由PQC机制生成的密钥，以提高整体安全冗余和抗失效能力。

该研究并未给出具体算法或协议的推荐，而是着眼于用例划分、需求分析和附加安全要求，为后续制定ITU-T的量子安全通信建议提供参考框架。其目标更多在于明确“如何用”“用在何处”，而非直接定义“用什么算法”。

截至2025年末，ITU-T尚未发布专门针对抗量子密码算法本身的正式推荐标准。其量子安全相关规范仍主要集中在QKD网络接口、量子随机数等领域，PQC在通信协议层面的具体应用仍处于研究和准备阶段。

IETF（互联网工程任务组）

推进抗量子密码算法与通信协议的国际标准预研布局

2025年，IETF在抗量子密码标准化方面的工作重点，集中于将PQC机制平稳引入现有互联网安全协议，尤其是TLS体系的升级路径。

在TLS 1.3框架下，IETF TLS工作组持续推进抗量子混合密钥交换方案的标准化。相关草案《Post-Quantum Hybrid ECDHE-MLKEM for TLS 1.3》在2025年进入较为成熟的阶段（发布第03版草案），系统定义了将传统ECDHE密钥交换与抗量子密钥封装机制并行使用的多种协商方式，用于TLS握手阶段的密钥协商。

这一混合方案的核心目标是在不破坏现有协议兼容性和部署基础的前提下，引入面向量子计算威胁的安全冗余。即使未来传统椭圆曲线算法受到量子攻击影响，会话密钥仍可依赖格密码部分维持安全性。由于工程可行性较高，该组合方案已在业界被广泛试验，并逐渐形成事实上的过渡实现路径。

除TLS之外，IETF在2025年还同步推进了X.509证书、S/MIME等基础设施中引入抗量子算法的相关草案，为后续更大范围的互联网协议升级奠定基础。

整体来看，IETF的标准化工作已从概念讨论阶段，进入面向实际部署的收敛期。

其他：科技企业以平台与产品落地，加速抗量子密码标准应用

微软（Microsoft）

以操作系统和开发平台为载体推进抗量子密码落地

微软公司在抗量子密码标准化方面扮演了积极角色。早期阶段，微软研究院深度参与了NIST抗量子密码算法的评估与实现工作，曾与学术界合作推进包括SIKE、FrodoKEM、Picnic等多条技术路线的研究与测试。尽管部分算法在竞争过程中被淘汰，但微软在格密码与实现安全方面积累了大量工程经验，并通过开源实现和性能评估为NIST的算法遴选提供了重要支撑。

进入标准落地阶段后，微软的重心明显转向平台级集成。2025年，微软在Windows与.NET生态中系统性引入对NIST已选定抗量子算法的支持，在操作系统、加密API以及开发框架层面完成基础能力铺设。通过对CNG（Cryptography Next Generation）框架和证书接口的扩展，开发者可以在现有应用中调用ML-KEM与ML-DSA，并与传统算法进行混合协商或双轨使用。

通过保持对TLS、VPN、代码签名和身份认证等常见场景的兼容性，微软有效降低了企业迁移门槛，使抗量子密码不再停留在实验或专用系统中，而是自然融入主流IT架构。

总体来看，微软并未试图主导算法选择，而是通过操作系统与开发平台的普及优势，将既定标准转化为大规模可用能力，其工程路径对整个产业的迁移节奏具有显著示范意义。



谷歌（Google）

在浏览器与云平台中率先验证抗量子密码的可用性

谷歌在抗量子密码领域的特点，并不在于主导算法标准，而在于其长期、持续地在真实互联网环境中验证新机制的可行性。早在十年前，谷歌便在浏览器和内部网络中开展抗量子密钥交换实验，积累了关于性能、稳定性和兼容性的第一手经验。

随着NIST标准落地，谷歌在2025年明显加快了商用落地节奏。通过在Google Cloud的密钥管理和签名服务中引入对标准化抗量子算法的支持，谷歌为企业用户提供了可测试、可回滚的实际使用环境，使抗量子密码不再只是规范文本，而成为可直接接入业务流程的功能模块。

在此过程中，谷歌持续推动混合架构思路：既不急于完全替换传统算法，也不回避未来风险，而是在现有协议和系统基础上逐步叠加抗量子能力。这一路径与IETF在TLS等协议中的混合方案形成呼应，也与谷歌自身大规模基础设施的稳定性要求高度一致。

从更宏观的角度看，谷歌的实践证明，抗量子密码完全可以在不显著牺牲性能和用户体验的前提下融入互联网核心服务。其价值不在于单次产品更新，而在于通过真实流量和长期运行，为整个行业提供了可复制的工程经验。



IBM公司

深度参与抗量子算法制定，并推动企业级部署实践

IBM在抗量子密码标准化进程中，处于极为核心的位置。由IBM研究人员参与设计的CRYSTALS-Kyber 和 CRYSTALS-Dilithium，最终成为NIST首批正式标准化的关键算法，使IBM成为少数在算法层面直接塑造国际标准走向的企业之一。这一成果源于其在格密码、同态加密等方向长期积累的基础研究能力。

2025年，IBM通过“Quantum Safe”相关工具和服务，将抗量子密码能力引入云平台、主机系统和硬件安全模块（HSM）环境，帮助企业开展加密资产盘点、风险评估和迁移验证。这类工具更强调流程与治理，而非单点算法替换。

同时，IBM在国际标准与行业协作层面保持高度活跃。其技术人员持续参与ISO/IEC、IETF等组织的讨论，分享在大型企业环境中部署抗量子密码的实践经验，并推动不同平台间的互操作与验证机制建设。通过联盟、白皮书和试点项目。

整体而言，IBM的独特价值在于其贯通能力：既参与定义“用什么算法”，也参与解决“如何在复杂系统中使用”。这一角色使其在全球抗量子密码生态中，长期处于技术与产业之间的枢纽位置。



04

全球主要国家现状与分析

目录

04
全球主要国家现状与分析

01 美国：以标准落地为牵引，推动量子安全进入系统性迁移阶段

02 中国：体系化推进与自主创新协同，构建完整产业生态

03 欧盟：统一战略牵引与基础设施先行，推进量子安全区域化建设

04 澳大利亚：围绕优势方向推进布局，并以国际协作为主要抓手

05 日本：积极部署，加大投入与对外协同并行

06 韩国：以标准推进与应用落地，推动量子安全实用化进程

07 加拿大：以国家迁移路线图为牵引，推进量子安全的场景化部署

01 美国：以标准落地为牵引，推动量子安全进入系统性迁移阶段

作为全球量子技术研发和网络安全产业的重要集聚地，美国在量子安全领域的推进呈现出以政策引导为先、市场逐步跟进的特征。进入2025年，围绕抗量子密码标准的落地实施，美国通过立法完善、监管指引和产业配合等多种方式，持续推动量子安全从战略规划层面走向可执行的迁移安排和工程部署阶段。

在政策与立法层面，量子安全迁移责任逐步制度化

- **明确关键基础设施迁移责任。**由众议员Haley Stevens首次提出、Claudia Tenney共同发起的立法修正案，旨在修订《国家量子倡议法案》和《网络安全研发法案》，其核心内容是明确指示美国国家标准与技术研究院（NIST）为关键基础设施等高风险实体提供实施抗量子加密工具的技术支持，从而系统性提升国家关键数字基础设施的长期安全性
- **推动联邦系统统一迁移规划。**参议员彼得斯与布莱克本提出的《国家量子网络安全迁移法案》，旨在要求白宫科技政策办公室牵头制定国家战略，以协调联邦系统向抗量子安全标准的全面过渡。
- **强化量子威胁的风险评估机制。**众议员Suhas Subramanyam向众议院科学、空间和技术委员会提交了《量子加密准备和弹性法案》，该法案旨在要求相关部门评估并报告量子计算带来的网络安全与国家安全风险，并提出应对策略。

在产业与市场层面，企业快速承接标准落地任务

- **主流云平台率先提供迁移能力。**微软Azure与谷歌云平台等已将NIST抗量子密码标准化算法集成至其核心云服务，为企业客户提供一键迁移的量子安全解决方案。

- **初创企业聚焦工程化应用场景。**初创企业如Project Eleven在种子轮融资中获得600万美元，专注于开发面向混合云环境的量子安全网络架构。

从资本市场表现看，尽管2025年全球量子安全领域融资规模整体趋于理性，美国相关企业仍保持较高的交易活跃度和相对稳定的单笔融资水平，显示出资本对其工程化路径和商业模式的持续关注。

总体来看，美国已进入以标准确定为前提、以迁移执行和合规交付为核心的量子安全发展阶段。通过立法明确责任主体、由产业体系承接实施任务，美国正在构建一条从标准发布到规模化迁移的完整路径，该模式为抗量子密码的工程落地提供了制度与市场基础，并将持续对全球量子安全实践产生示范效应。

02 中国：体系化推进与自主创新协同，构建完整产业生态

依托国家层面的持续投入与组织能力，中国通过统一规划重大工程、同步推动核心技术攻关与产业化应用，在较短时间内形成了从基础研究、关键器件到网络建设和行业应用的完整链条。

在“十五五”规划启动背景下，量子科技被纳入强化国家战略科技力量和数字安全能力的重要方向。国家层面进一步强化顶层设计，围绕量子通信网络规模化建设、抗量子密码算法自主研发以及关键设备国产化替代等任务展开统筹部署，推动相关技术从科研示范向工程化、产业化演进。

- 中国在星地量子通信工程方面取得阶段性进展。中国科学技术大学联合科大国盾量子等单位推进小型化量子卫星地面站建设与工程验证，并在此基础上实现万公里级星地量子密钥分发能力验证，推动星地量子通信由科研示范向工程化应用过渡，为构建覆盖全球的量子通信网络奠定了坚实工程基础。

- 技术产业协同层面，产学研用一体化创新体系成效显著。

  中国科学技术大学联合科大国盾量子、中国电信量子研究院，在商用光纤条件下实现了高功率经典光信号与量子密钥分发信号的稳定共纤传输，刷新了经典—量子共纤传输多项关键技术指标，验证了量子保密通信与现有光通信网络深度融合的工程可行性，为后续规模化部署奠定了技术基础。

- 下游应用层面，以合肥市量子保密通信城域网为代表的一批城市级网络已完成建设并投入运行，为区域内的政务、金融数据传输提供了自主可控的安全信道。同时，国家电网、银行等关键行业龙头已启动基于国产抗量子密码算法的核心系统迁移试点，标志着抗量子密码技术进入实质性行业应用阶段。

- 量子安全技术与新型基础设施的融合不断深化，其与5G网络切片安全、工业互联网数据加密传输等场景的结合已进入工程化验证与标准制定阶段，为构建未来一体化安全基础设施奠定了基础。

中国在量子安全领域形成了以国家战略牵引、重大工程推动和产业化应用协同发展的推进模式。依托统一的国内市场、持续的工程投入以及逐步完善的产业配套，量子保密通信网络建设和抗量子密码迁移实践正在同步推进，并在通信、电力、金融等关键行业进入实质性应用阶段。在此基础上，“量子+”融合应用逐步展开，量子安全能力开始嵌入5G网络、云平台和工业互联网等数字基础设施之中，探索形成可复制的行业级安全方案，为新一代信息基础设施提供长期可信的安全支撑。

03 欧盟：统一战略牵引与基础设施先行，推进量子安全区域化建设

欧盟的推进方式以整体规划和跨境协同为主要特征。通过统一战略框架、集中资源建设跨国基础设施，并在成员国之间推动标准与工程协同，欧盟试图将分散于各国的科研与产业能力整合为可持续运行的区域体系，为量子安全技术的长期部署奠定制度和工程基础。

2025年，欧盟在量子安全相关政策与项目推进上呈现出明显的系统化特征。欧盟委员会正式发布《量子欧洲战略：变化世界中的量子欧洲》，为未来一段时期内欧盟量子技术发展提供总体指引。在量子安全相关目标上，战略提出推进量子芯片试点产线建设、部署量子互联网与通信测试设施，并规划在2030年前形成初步联通的地面—空间量子通信体系，为成员国开展量子安全应用提供统一的基础条件。

在具体工程与产业层面，欧盟通过旗舰项目推动技术落地与生态构建

- 欧洲航天局（ESA）主导的EAGLE-1量子通信卫星项目完成全部地面测试，计划于2026年初发射，将成为欧洲自主量子天基网络的关键节点。
- 由法国、德国、荷兰等国共建的欧洲量子通信基础设施（EuroQCI）进入大规模部署阶段，多国光纤量子骨干网启动互联互通测试。
- 产业生态上，欧洲量子产业联盟（QUIC）联合多家企业与研究机构，成功演示了跨域量子密钥分发与经典加密的混合组网方案，为金融、政务等高安全需求场景提供了欧洲解决方案。

欧盟量子安全的发展重点不在于单个成员国或企业的快速突破，而在于构建一个具备持续运行能力的区域性体系。通过统一战略文件、跨境基础设施建设以及多国参与的工程验证，欧盟正在形成一种以制度协调和工程整合为基础的量子安全推进路径。未来，其影响力更多体现在为成员国提供共同的技术底座和协同框架，并在区域层面推动量子通信和安全技术的兼容与对接，而非以单一技术路线主导全球发展方向。

04 澳大利亚：围绕优势方向推进布局，并以国际协作为主要抓手

依托开放的科研体系、成熟的基础研究能力以及其在AUKUS框架中的特殊位置，澳大利亚逐步形成了以优势领域突破、国际协同推进为特征的发展模式，在南半球量子技术版图中占据独特位置。

政策与标准层面

澳大利亚的发展延续了2023年发布的国家量子战略所确立的总体方向。该战略明确提出，到2030年前推动关键系统完成向抗量子加密能力的过渡。进入2025年后，政策重点从宏观目标转向具体实施路径与标准参与度提升。同年7月，澳大利亚标准机构发布《量子计算参考指南》草案，尝试在国际标准讨论中提前占位，为后续参与量子与抗量子安全相关标准工作奠定基础。

产业实践与国际协作方面

- 核心策略是深度融入以AUKUS（澳英美联盟）为支柱的安全技术同盟，并在此基础上拓展多元合作。这不仅体现在与美、英在量子安全及传感等领域的联合研发上，也表现为通过四方安全对话（Quad）等多边框架促进区域技术协作。
- 澳大利亚在2024年宣布的对美国量子计算公司PsiQuantum的重大投资，依然对2025年的产业生态产生着持续影响，巩固了其通过引入国际顶级资源来提升全球产业参与度的战略路径。

未来，澳大利亚在量子安全领域大概率将延续以优势方向为重点、以国际协同为抓手的发展路径。一方面，其有望继续在量子随机数发生器、量子精密测量等具备比较优势的细分领域加大投入，推动技术成熟与商业化应用，形成具有辨识度的产业能力输出。另一方面，凭借连接亚太与西方技术体系的独特位置，澳大利亚将进一步依托 AUKUS 等多边合作机制，参与并影响盟友间量子安全技术标准、供应链布局和协作规则的构建。

总体来看，澳大利亚并不追求在全球量子安全领域的全面主导地位，而是以专业能力和协同价值为核心，在特定方向上发挥稳定而持续的影响力。

05 日本：积极部署，加大投入与对外协同并行

在量子技术快速演进的背景下，日本逐步调整其发展思路，试图将长期积累的基础研究能力转化为可持续的产业竞争力。

2025年，日本在量子安全相关领域明显强化了政策牵引与资源投入，一方面通过国际同盟合作拓展外部空间，另一方面以集中财政支持推动国内技术与产业体系建设，力图在全球量子安全格局中争取更具实质性的参与位置。

国际协同与规则嵌入：强化同盟中的量子安全角色

- **推动量子安全合作常态化。**美日韩在首尔与东京连续举行量子工业安全三边研讨会，围绕量子技术生态保护与安全风险应对展开讨论，标志着三国在量子科技领域的合作由交流层面走向机制化与务实化。
- **双边协议将量子技术纳入战略合作框架。**日美签署《技术繁荣协议》（TPD），将量子技术明确列为核心合作领域之一，旨在通过协调标准、加速研发和强化供应链安全，提升双方在关键前沿技术领域的协同能力。

国家投入与产业牵引：以财政手段推动规模化布局

- **国家层面以超大规模投入明确产业化导向。**日本政府将2025年定位为“量子产业化元年”，并在当年追加预算中投入一万亿日元级别资金，用于下一代芯片和量子计算机研发，清晰释放出由基础研究转向举国推动技术商业化的政策信号。

关键技术与能力积累：硬件、算法与测量并行推进

- **构建自主可控的量子计算硬件体系。** 在量子计算硬件方面，日本正加速构建自主可控的供应链体系。理化学研究所与富士通正致力于开发超导量子计算机，并计划于未来几年推出更高量子比特系统。

- **在抗量子密码算法领域取得国际突破。**东京大学、NTT等机构联合研发的数字签名算法QR-UOV，作为唯一源自日本的方案进入NIST抗量子密码标准化竞赛第二轮，显示出日本在核心密码算法层面的技术积累，并为其参与未来国际标准讨论提供了重要支点。
- **夯实量子通信安全的基础测量能力。**日本产业技术综合研究所（AIST）在2025年提出覆盖光通信C波段的“光子标尺”技术，为高速量子密码系统的安全评估和性能验证提供了关键测量工具，补齐了工程化应用中的基础能力环节。

总体来看，日本量子安全正由以研究驱动为主，逐步转向以产业应用和生态构建为重点的发展阶段。政府通过高强度公共投入，试图在Q-STAR 等产业联盟框架下带动企业、研究机构与传统产业形成协同。然而，日本仍面临初创企业数量有限、创新活力偏弱等结构性约束。

未来，能否在保持制造与材料优势的同时，加快技术成果向可复制、可推广产品的转化，将直接影响其在全球量子安全体系中的实际角色。整体而言，日本更可能以稳健推进、深度参与的方式，在国际产业链与规则体系中持续扩大影响，而非通过激进扩张实现快速跃升。

06 韩国：以标准推进与应用落地，推动量子安全实用化进程

在量子安全领域，韩国的发展路径呈现出鲜明的产业导向特征。依托成熟的信息通信技术体系和完整的电子制造产业链，韩国正将标准制定与应用落地同步推进，试图通过可复制的产品和场景积累，在区域乃至全球量子安全体系中扩大实际影响力。2025年，韩国明显加快了量子安全由研发验证向工程应用转变的节奏，其政策与产业动作更加聚焦、连续。

国家战略与标准牵引：明确技术方向与投入重点

- **将量子安全能力纳入国家战略技术体系。**韩国科技信息通信部依据《国家战略技术特别法》，正式将量子随机数生成器（QRNG）与自动驾驶 AI 芯片并列认定为国家战略技术，明确了量子安全在国家技术布局中的优先级。双边协议将量子技术纳入战略合作框架。
- **推动本国标准向区域与国际层面输出。**韩国电子通信研究院主导制定的量子密钥分发（QKD）设备国家标准正式实施，并被积极推荐为亚洲量子安全标准联盟的候选标准，显示韩国正尝试通过标准提升区域话语权。
- **通过同盟机制强化标准与技术协同。**韩国通过与美国签署《技术繁荣协议》，在量子技术相关标准协调、技术保护与供应链安全方面深化合作，将量子安全嵌入更广泛的同盟技术体系。

产业体系嵌入：依托既有优势实现工程化落地

- **在消费电子端构建量子安全信任。**三星电子展示了集成量子随机数生成器和轻量级抗量子密码算法的安全芯片原型，并计划应用于新一代旗舰智能手机和物联网设备，尝试在大规模终端中率先引入量子安全能力。

- **由通信运营商推动服务级部署。**LG Uplus于5月宣布将基于抗量子密码的安全系统应用于韩国通信委员会（KCA）关键系统，并于6月向企业客户提供基于PQC的认证系统AlphaKey，用于增强其CRM平台 Re:catch的安全性。

重点行业示范：验证关键基础设施应用可行性

- **在能源系统中验证量子安全通信能力。**韩国电力公司与韩国电信在济州岛联合建设基于量子密钥分发的智能电网安全通信示范网络，验证了量子安全技术在国家级能源基础设施中的工程可行性与可靠性。
- **推动量子安全进入支柱产业体系。**现代集团于2025年宣布参与全国性量子安全网络基础设施建设项目，表明量子安全正被系统性引入韩国的核心产业与国民经济关键环节。

从整体趋势看，韩国量子安全的发展路径与其电子制造、通信网络和能源产业等既有优势高度绑定。通过国家战略技术认定、标准先行与行业示范并行推进，韩国正在形成一条从核心器件、通信系统到行业应用的渐进式部署路线。依托其在全球半导体和电子产品供应链中的关键位置，韩国具备将量子安全功能前置嵌入芯片和设备设计的现实条件。这种以标准牵引、以应用验证、以产业体系承载的发展方式，或将使韩国在特定行业场景中积累可复制的量子安全实践经验，并在区域层面形成持续影响力。

07 加拿大：以国家迁移路线图为牵引，推进量子安全的场景化部署

量子安全领域，加拿大的推进方式呈现出明显的政策牵引与应用导向特征。2025年，加拿大将工作重点放在抗量子密码的系统性迁移安排上，通过明确政府层面的实施路径，并引导本土企业在关键行业开展应用验证，逐步构建可执行、可评估的量子安全技术体系。

在政策与标准层面

- 加拿大网络安全中心联合共享服务加拿大和财政部秘书处，正式发布了《联邦政府抗量子密码迁移路线图》，确立了其国家级别的行动纲领。

在技术与产业应用层面

- 能源技术公司Energy Plug Technologies宣布与本土企业Quantum eMotion合作，通过量子加密技术保护关键能源资产，标志着抗量子安全技术开始服务于国家关键基础设施的早期部署。
- BTQ Technologies正式发布其量子安全区块链共识框架Léonne，旨在解决区块链的“不可能三角”难题；
- BTQ Technologies宣布与QBits合作开发“世界上第一个量子安全托管金库基础设施”，致力于为数字资产构建可证明的量子安全环境。

整体来看，加拿大量子安全的发展路径强调节奏可控与责任明确。通过国家层面的迁移路线图，加拿大为抗量子密码的实施建立了可操作的治理框架；通过在能源与金融等高价值场景中的试点应用，本土企业则在验证技术可行性的同时积累工程经验。

未来，加拿大更可能在“如何组织和管理抗量子迁移”这一问题上形成示范意义，其影响力不在于技术规模，而在于制度设计与实施路径的可参考性。

05

投融资分析



目录

05
投融资分析

01 融资规模：总额回落、事件数持平，投资结构趋于理性

02 融资分布：欧美主导格局强化，亚太力量稳步崛起

03 融资轮次：以成长期为主体，发展阶段趋于明晰

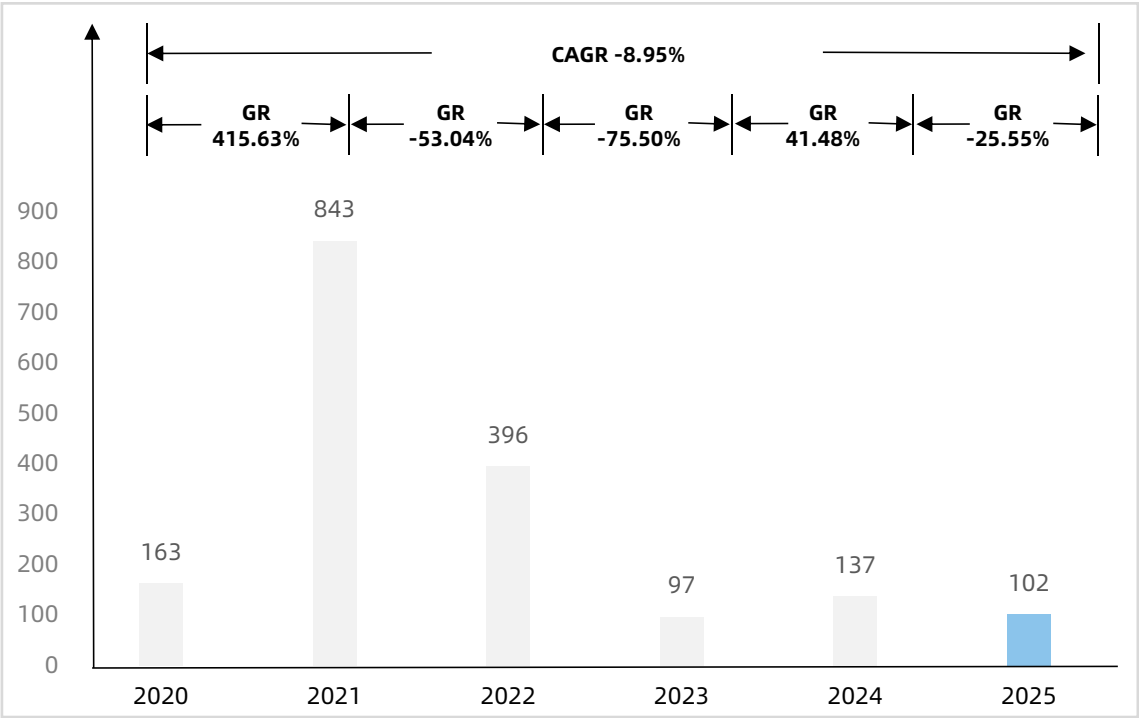
04 融资领域：PQC与QKD双主线并进，技术融合态势初显

05 融资趋势：政策资本深入介入，产业整合预期增强

01 融资规模
总额回落、事件数持平，投资结构趋于理性

2025年，全球量子安全领域公开披露的投融资总额为1.02亿美元，全年共发生融资事件11起。结合历史数据来看，年度融资总额继2021年达到8亿美元峰值后，连续三年呈下滑态势，至2024年的1.37亿美元，2025年则在此基础上进一步温和回调。这一曲线清晰地描绘出产业从概念热潮期（2021-2022年）步入理性回调与价值重估期（2023-2025年）的完整周期。

图表 2020-2025年全球量子安全领域融资总额（单位：百万美元）



iCV TA&K | 2026.2

此次融资回调并不意味着市场信心发生根本性变化，而更像是资本配置逻辑的阶段性调整。相比此前覆盖面较广、以技术前景为主要判断依据的投资方式，资金开始更加集中地评估项目在核心技术成熟度、商业路径清晰度以及团队执行能力等方面的现实表现。

从数据上看，2025年量子安全领域的融资事件数量与2024年基本持平，但整体融资规模有所回落，反映出单笔融资规模趋于理性。资金逐步减少对概念性项目的投入，同时向已完成初步商业验证、具备明确应用场景的企业集中。这一变化表明，资本市场正在主动降低对不确定性的容忍度，通过结构性调整提升投资质量。

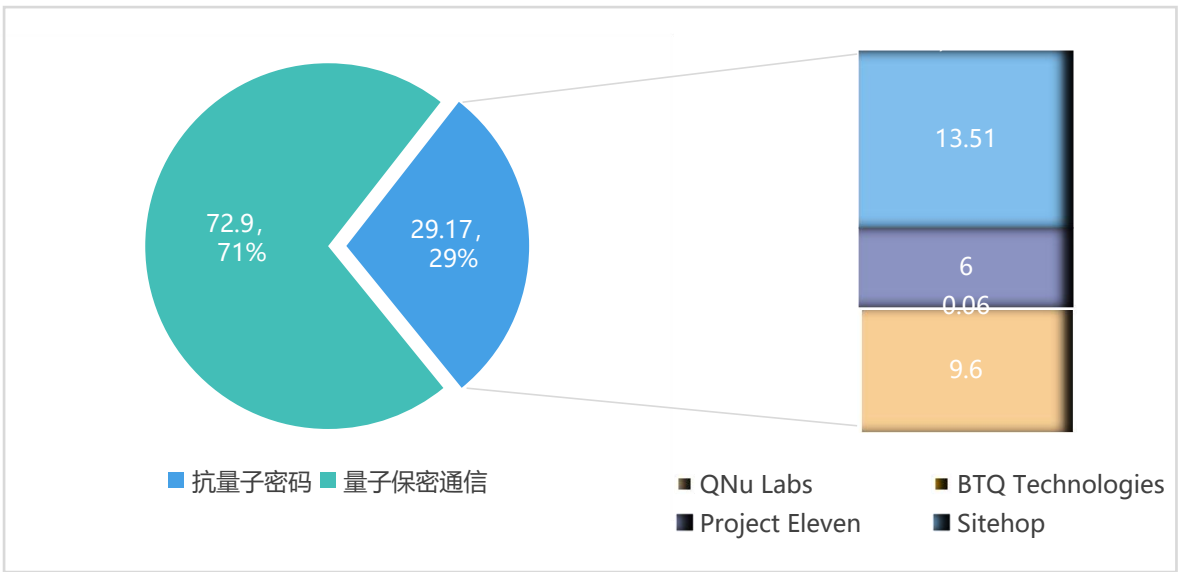
2025年，量子安全领域的投融资活动保持稳步推进，产业发展正从初期探索迈向应用验证与生态构建的关键阶段。在抗量子密码与量子安全网络领域，多家企业获得资本青睐，融资活动展现出技术路线、发展阶段与地域分布的多元化特征。

- 印度QNu Labs公司在A轮融资中成功获得960万美元，其发展获得了印度国家量子计划（NQM）的积极支持，彰显出该国在构建自主量子技术生态方面的战略布局。
- 加拿大BTQ Technologies与Coxwave共获韩国政府“AI Voucher”计划11.7万美元资助，其中BTQ Technologies获得了一笔5.85万美元的赠款支持，共同开发用于量子物理教育和研究的AI聊天机器人解决方案。
- 美国Project Eleven公司在种子轮融资中筹集了600万美元
- 英国Sitehop公司在A轮融资中成功获得1351.38万美元

以上获得投资的企业，其融资轮次涵盖了从早期研发支持、种子轮到成长期A轮的多个阶段，表明量子安全产业各细分赛道均在不同成熟度上同步发展，既有面向长期战略的前沿探索，也有聚焦产品化与商业化的务实推进。

整体而言，资本正以更加理性和精准的方式，支持那些具备清晰技术路径、明确应用场景和可持续商业模式的企业，推动全球量子安全产业在务实中向前发展。

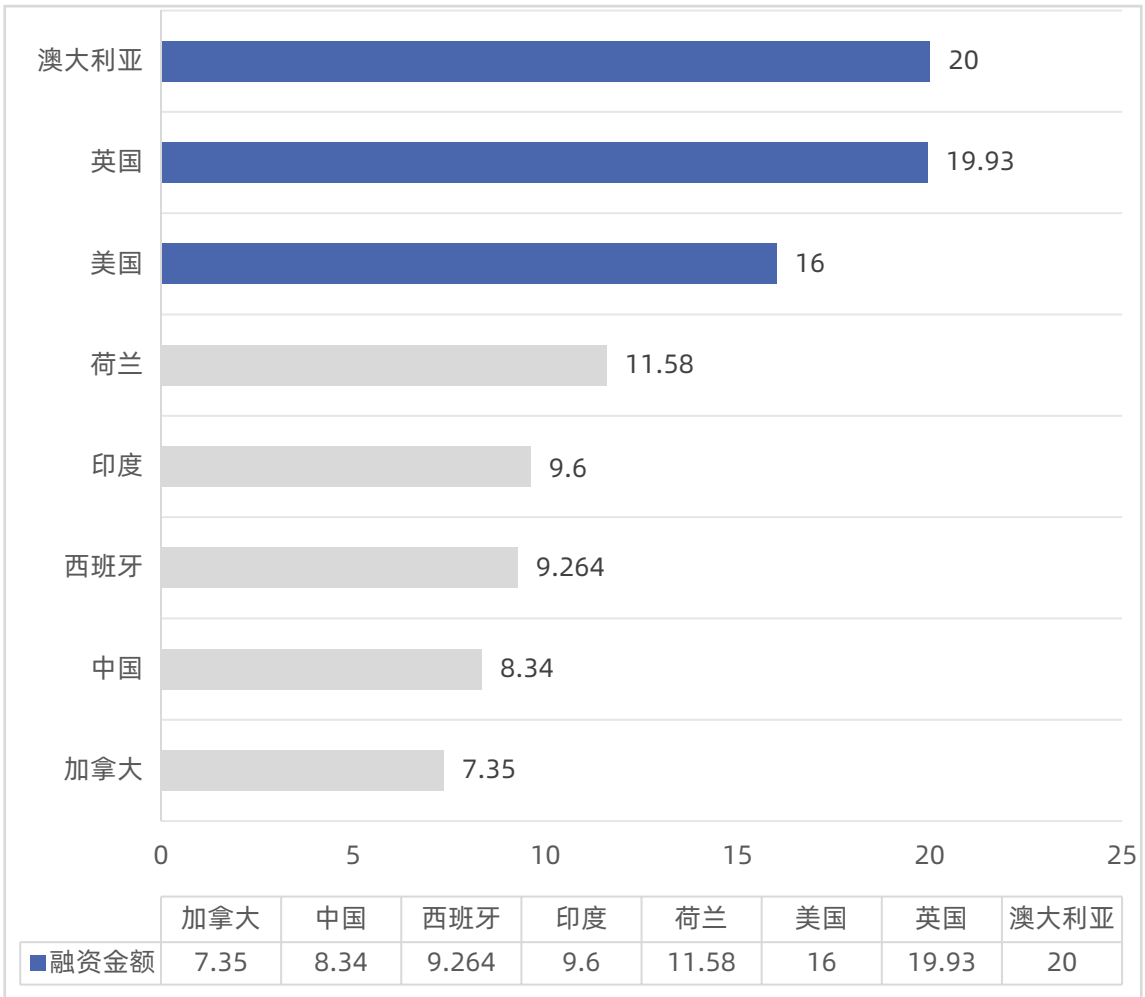
图表 2025全球量子安全领域抗量子密码融资分布及占比情况（单位：百万美元）



02 融资分布
欧美主导格局强化，亚太力量稳步崛起

从地理分布看，2025年的融资活动进一步巩固了以北美和欧洲为双核心的全球格局。在11起融资事件中，英国（Quantum Base，Sitehop）、芬兰（Q*Bird）加拿大（BTQ Technologies，Quantum eMotion）、美国（Project Eleven，Qunnect）和西班牙（LuxQuanta Technologies SL）等欧美国家贡献了主要份额。这表明上述地区凭借深厚的研究基础、活跃的风险投资生态以及对前沿科技的战略性扶持，持续吸引着全球资本。

图表 2025全球各国量子安全领域的融资总额（单位：百万美元）



	加拿大	中国	西班牙	印度	荷兰	美国	英国	澳大利亚
融资金额	7.35	8.34	9.264	9.6	11.58	16	19.93	20

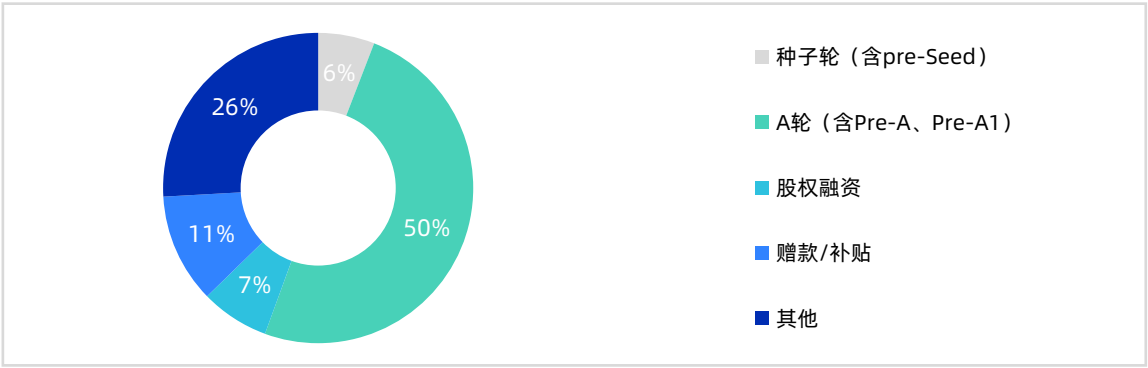
iCV TA&K | 2026.2

同时，亚太地区的力量不容忽视。印度和澳大利亚均有企业获得融资，显示出该区域在量子安全领域的创新活力与市场潜力正在加速释放。中国虽在2025年公开融资事件较少，但其产业生态仍展现出持续发展的韧性，构成了全球产业版图中另一极重要力量。全球融资格局正从美欧绝对主导，向美、欧、亚多极并进的态势演进。

03 融资轮次
以成长期为主体，发展阶段趋于明晰

从融资轮次分布来看，2025年量子安全领域的投资明显向成长期企业集中。在11起融资事件中，A轮融资达到5起，占据主导地位，反映出多数获投企业已顺利完成技术研发与原型验证，进入产品迭代、市场拓展和商业模式探索的关键阶段。此外，种子轮、政府赠款/补贴及其他形式的早期支持仍占一定比例，表明行业在推动成熟企业发展的同时，也持续为早期创新保留空间。

图表 2025年全球量子安全领域公司及融资轮次分布情况



全球量子安全公司的融资轮次情况

融资轮次	QKD	QRNG	PQC	其他
种子轮			Project 11	
A	LUXQUANTA	Q→NU 国腾量子 NATIONAL-QUANTUM	Q→NU Q→NU sitehop	Qunnect
股权融资		quantum emotion		
赠款/补贴	Q*bird quantum connectivity		BTQ	
其他	Quintessence Labs	Quintessence Labs		Quantum Base

轮次分布的阶段性特征，清晰映射出量子安全产业的生命周期位置：

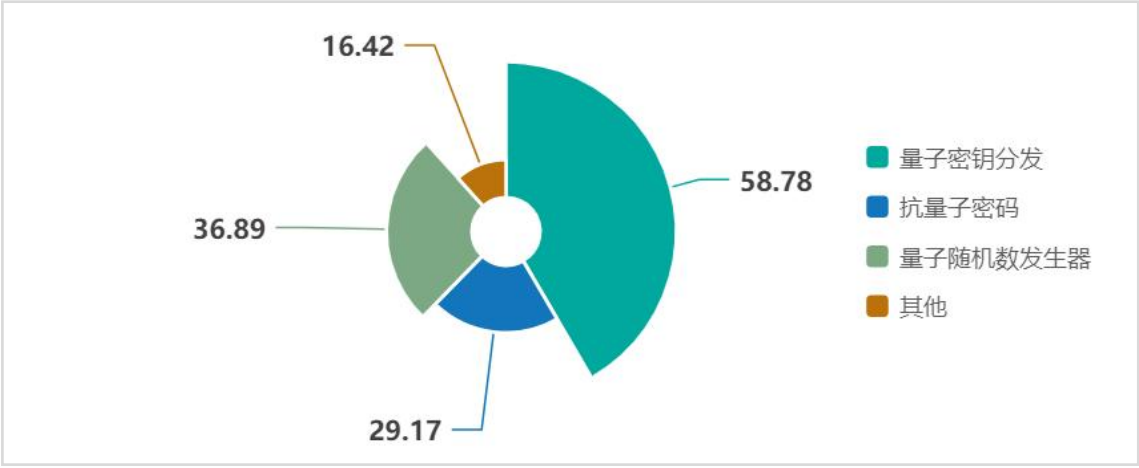
行业整体已跨越技术萌芽期，正处于从“技术可行”向“商业可用”加速过渡的关键阶段。资本更倾向于支持那些已具备产品雏形、初步客户验证和清晰增长路径的企业，投资逻辑更趋务实与审慎。

04 融资领域
PQC与QKD双主线并进，技术融合态势初显

从融资的技术领域分布分析，抗量子密码与量子密钥分发仍是资本重点布局的两大主线，分别发生4起和5起融资事件。具体而言，PQC领域企业包括美国Project Eleven、英国Sitehop、印度QNu Labs和加拿大BTQ Technologies；QKD方向则包括芬兰Q*Bird、印度QNu Labs、澳大利亚QuintessenceLabs、西班牙LuxQuanta Technologies SL以及中国广东国腾量子科技。这一分布格局反映出资本市场对两种主流技术路径的持续认可，同时也体现出部分企业在技术路线选择上的多元化特征。

在基础安全模块领域，量子随机数发生器获得3起融资关注，涉及加拿大Quantum eMotion、印度QNu Labs和澳大利亚QuintessenceLabs。其他融资事件还包括英国Quantum Base和美国Qunnect，这些企业分别聚焦于量子安全硬件技术和量子网络通信等细分方向。值得注意的是，印度QNu Labs和澳大利亚QuintessenceLabs等企业在多个技术领域均有布局，展现了量子安全产业中技术融合的发展趋势。

图表 2025年量子安全各领域融资额分布情况（单位：百万美元）



iCV TA&K | 2026.2

从投资逻辑分析，当前资本更青睐具备技术整合能力和系统解决方案提供潜力的企业。一方面，纯技术路线的单一性投资正在减少，取而代之的是对能够实现“核心模块—系统集成—融合方案”价值延伸的企业给予更多关注；另一方面，企业的地域分布和技术路线的多元化选择也表明，投资者正在通过分散化布局来应对量子安全产业发展的不确定性。这种投资策略的转变，反映出资本市场对量子安全产业长期发展前景的谨慎乐观态度，同时也预示着产业将进入技术整合与生态构建的新阶段。

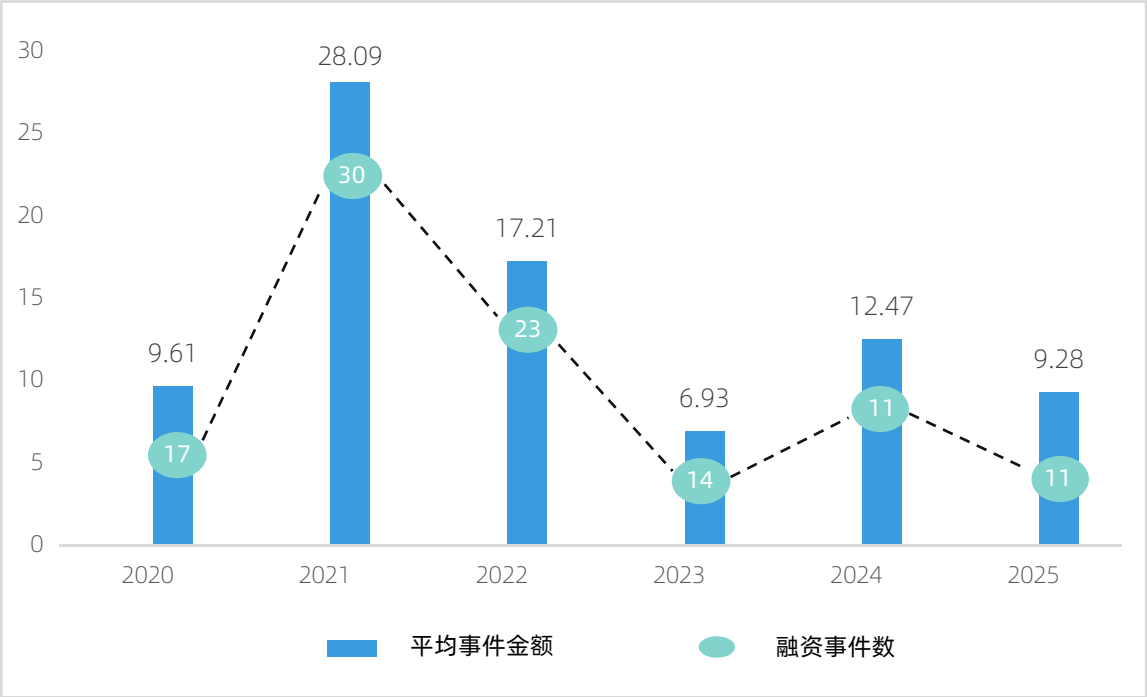
05 融资趋势
政策资本深入介入，产业整合预期增强

全球量子安全领域的投融资将呈现出政策引导强化、产业整合加速和投资标准趋严的总体趋势。

政策性资本的引领作用将持续增强

随着量子安全被各主要经济体纳入国家安全和数字主权框架，政府引导基金、主权财富基金以及政策性金融机构将更深度参与相关投资。这类资本关注的不仅是短期回报，更强调对国家战略目标的支撑，其重点投向预计集中在标准体系建设、量子保密通信基础设施、核心密码芯片研发以及金融、能源、政务等关键行业的迁移示范项目。各国对抗量子密码迁移路线图的明确化和合规要求的落地，将成为驱动相关投资的重要政策因素。

图表 2020-2025年全球量子安全融资事件数量及平均金额 （单位：百万美元）



iCV TA&K | 2026.2

产业并购与整合窗口有望逐步打开

随着技术路线趋于稳定，市场竞争重心正由技术验证转向产品成熟度、解决方案完整性和客户覆盖能力。未来两到三年内，具备特色技术但缺乏规模化交付能力的中小企业，可能成为网络安全厂商、传统ICT设备商、云服务提供商及半导体企业的并购目标。通过并购整合，头部企业有望加快补齐技术与产品体系，推动行业集中度提升。

投资逻辑将更加聚焦商业可行性

资本对单一技术概念的容忍度明显下降，评估重点转向工程化能力、合规适配程度以及真实市场需求。能够在现有IT或工业系统中稳定部署、提供清晰迁移路径并形成可持续收入模式的企业，将更容易获得持续资本支持。总体来看，资本更倾向于选择能够帮助客户在真实业务环境中降低风险、完成安全升级的解决方案提供方，而非单纯依赖技术领先性的企业。

06

供应商评价



目录

06
供应商评价

01 量子密钥分发供应商分析

02 量子随机数发生器供应商分析

03 抗量子密码供应商分析

04 量子安全代表性厂商分析

供应商分析

随着量子安全由可用验证逐步迈向可规模交付，供应商竞争的衡量标准正在发生明显变化。市场关注点不再局限于单项性能指标或实验结果，而是更加看重解决方案能否以可控成本接入既有网络与安全体系，是否具备跨厂商互通能力，以及在合规审计、密钥管理、故障定位和持续运维等方面是否形成成熟、可复制的工程化交付能力。

从全球供给侧看，量子安全技术路径已大体形成两类主线：一类以量子密钥分发和量子随机数发生器为代表，侧重在密钥生成与分发等关键环节引入量子物理机制，在高价值链路中提供更强的密钥安全保障和入侵可检测能力；另一类以抗量子密码为核心，通过算法替换或升级，提升现有系统在面对未来量子计算威胁时的整体安全性与可迁移性。实际应用中，两类技术更多以分层组合的方式部署：抗量子密码用于广域系统和存量业务的规模化覆盖，量子密钥分发和量子随机数发生器，则在关键链路、核心节点或高敏感数据通道中提供针对性加固，并在金融、电信、政务和云平台等场景中逐步形成可复制的部署模式。

图表 量子安全供应商分析框架与分类

供应商分类	核心关注点	供应商能力侧重
量子密钥分发供应商分析	长距离传输、网络化能力、工程稳定性	设备成熟度、网络部署经验、与运营体系的融合能力
量子随机数发生器供应商分析	随机性质量、接口形态、系统嵌入性	芯片化与模块化能力、与密码系统和平台的集成能力
抗量子密码供应商分析	算法支持、迁移路径、合规适配	加密敏捷性、工具链与治理能力、行业落地经验
量子安全代表性厂商分析	多技术融合与整体交付能力	端到端解决方案、行业应用与规模化服务能力

01 量子密钥分发供应商分析

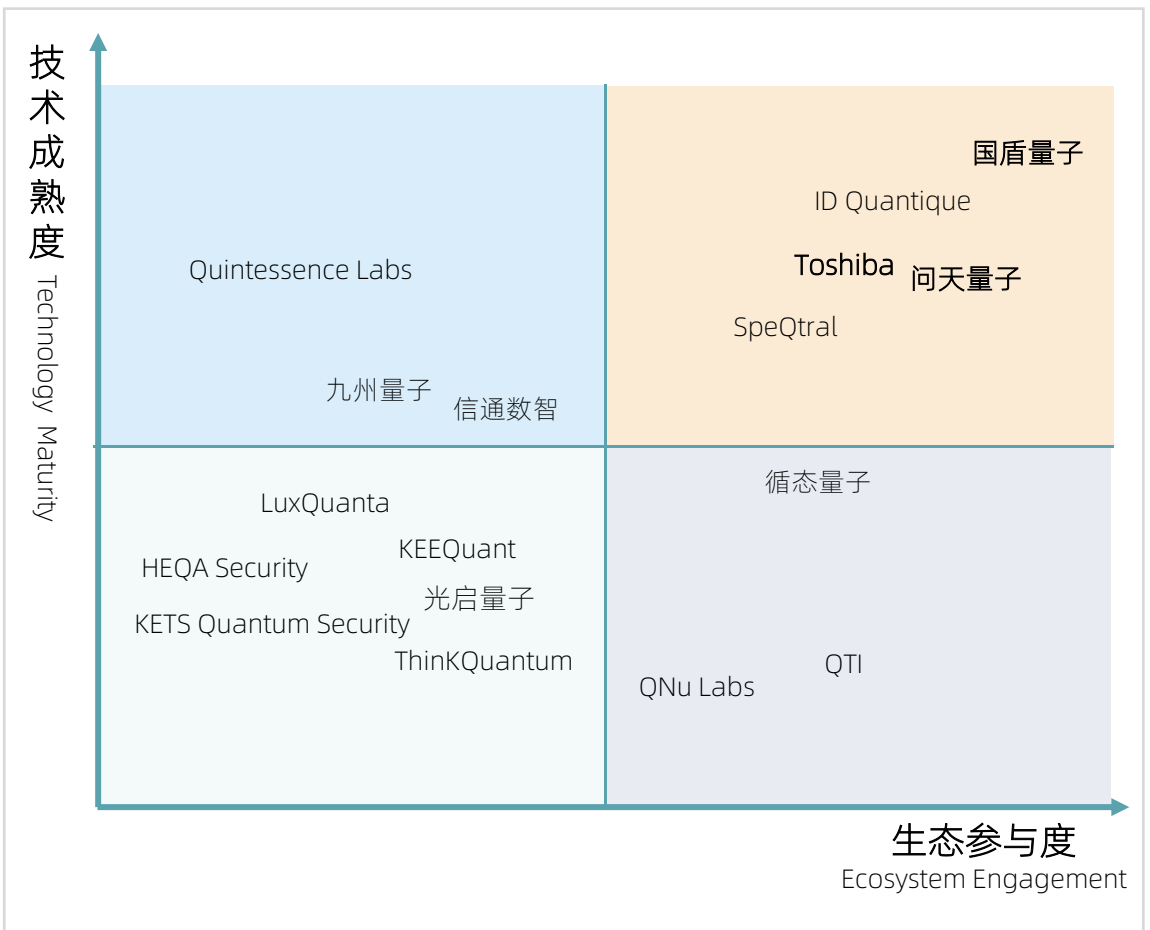
QKD设备供应商：技术成熟度主导的 Q-EMC 分布

在设备侧 Q-EMC 模型中，技术成熟度仍是决定厂商位置的首要变量。2025 年，QKD 设备厂商整体呈现出核心能力集中、生态参与度分化的格局。

模型右上区域聚集了一批技术路径成熟、具备工程化交付能力的设备型厂商，包括国盾量子、ID Quantique、Toshiba、问天量子、SpeQtral 等。这类企业在量子光源、单光子探测器、系统集成及协议实现等关键环节形成了稳定能力，是当前 QKD 工程化落地的主要支撑力量。

模型左上区域则以技术能力突出但生态参与度相对有限的设备厂商为主，例如 Quintessence Labs、九州量子、信通数智等。这类企业在特定器件或系统方案上具备较强技术基础，但其应用多集中于专用系统或定制化场景，尚未深度嵌入大规模网络体系。

图表 量子密钥分发供应商（设备方面）的Q-EMC模型



模型左下区域主要分布着处于技术验证或新路径探索阶段的设备厂商，包括 LuxQuanta、KEEQuant、光启量子、ThinkQuantum、HEQA Security、KETS Quantum Security 等。这类企业在自由空间、卫星 QKD 或新型架构方面具备前瞻性，但整体仍处于工程能力与市场应用的积累阶段。

模型右下区域企业数量相对有限，主要体现为部分生态参与度较高、但设备成熟度仍待提升的厂商，其后续位置取决于能否完成从原型系统向稳定工程产品的跃迁。

总体来看，设备侧 Q-EMC 模型显示：技术成熟度决定设备厂商的准入门槛，而生态适配能力正在成为决定其长期分化的关键变量。

》QKD 网络供应商：生态参与度与工程能力主导的 Q-EMC 分布

在网络侧 Q-EMC 模型中，厂商位置更多由生态参与度与工程化部署能力共同决定。

模型右上区域集中了一批已具备持续运行与网络级部署能力的网络型供应商，包括中电信量子集团、SpeQtral、Quantum Xchange 等。这类厂商能够将 QKD 能力嵌入既有通信网络或行业专网体系，推动量子安全从示范链路向可运营网络形态演进。

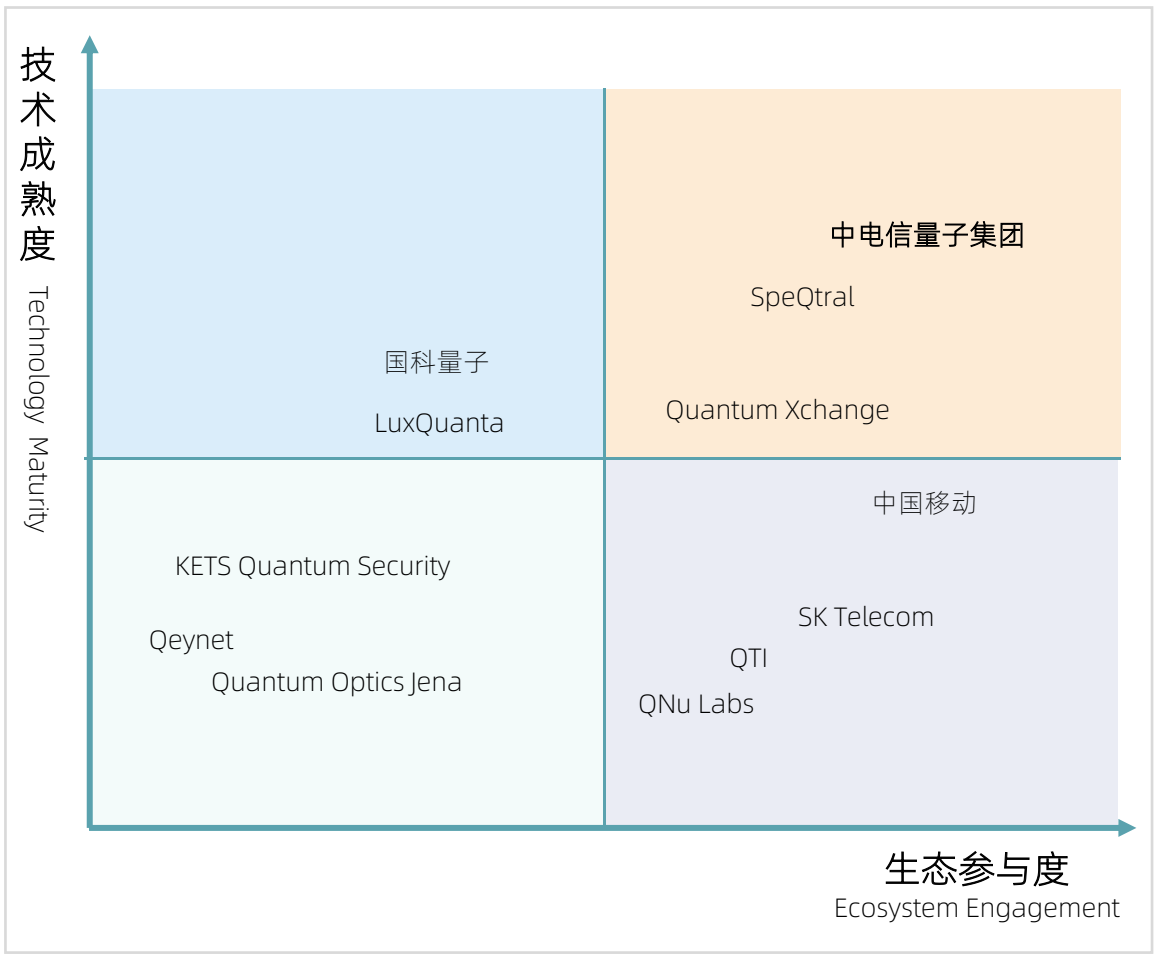
模型左上区域以具备一定网络技术能力、但生态嵌入程度有限的厂商为主，代表性企业包括国科量子、LuxQuanta 等，其网络实践多集中在试点或区域级部署，尚未形成跨区域扩展能力。

模型右下区域则分布着一批生态参与度较高、但整体工程能力仍在爬坡阶段的厂商，包括中国移动、SK Telecom、QTI、QNu Labs 等。这类企业往往依托运营体系或产业合作进入量子安全网络建设，但在 QKD 网络的独立运营经验与管理平台成熟度方面仍需积累。

模型左下区域主要是以新型网络形态为主的探索型企业，如 Qeynet、Quantum Optics Jena、KETS Quantum Security 等，其在卫星量子通信或新架构方面具备创新性，但整体仍处于工程验证和早期应用阶段。

总体来看，网络侧 Q-EMC 模型表明：网络级 QKD 的竞争核心，在于工程能力与生态协同能力的叠加，而非单一技术或设备指标。

图表 量子密钥分发供应商（网络方面）的Q-EMC模型



iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

综合设备侧与网络侧 Q-EMC 模型可以看出，2025 年量子密钥分发产业呈现出设备能力与网络能力并行推进、相互约束的发展特征。

设备侧厂商，如国盾量子、ID Quantique 等通过器件与系统工程能力，直接影响 QKD 设备的关键性能指标、长期稳定性与运行可靠性；网络侧厂商，如中电信量子集团、Quantum Xchange 等则更多通过网络架构、运维体系与服务交付能力，影响 QKD 在现网中的部署范围、业务化供给形态及商业化拓展空间。

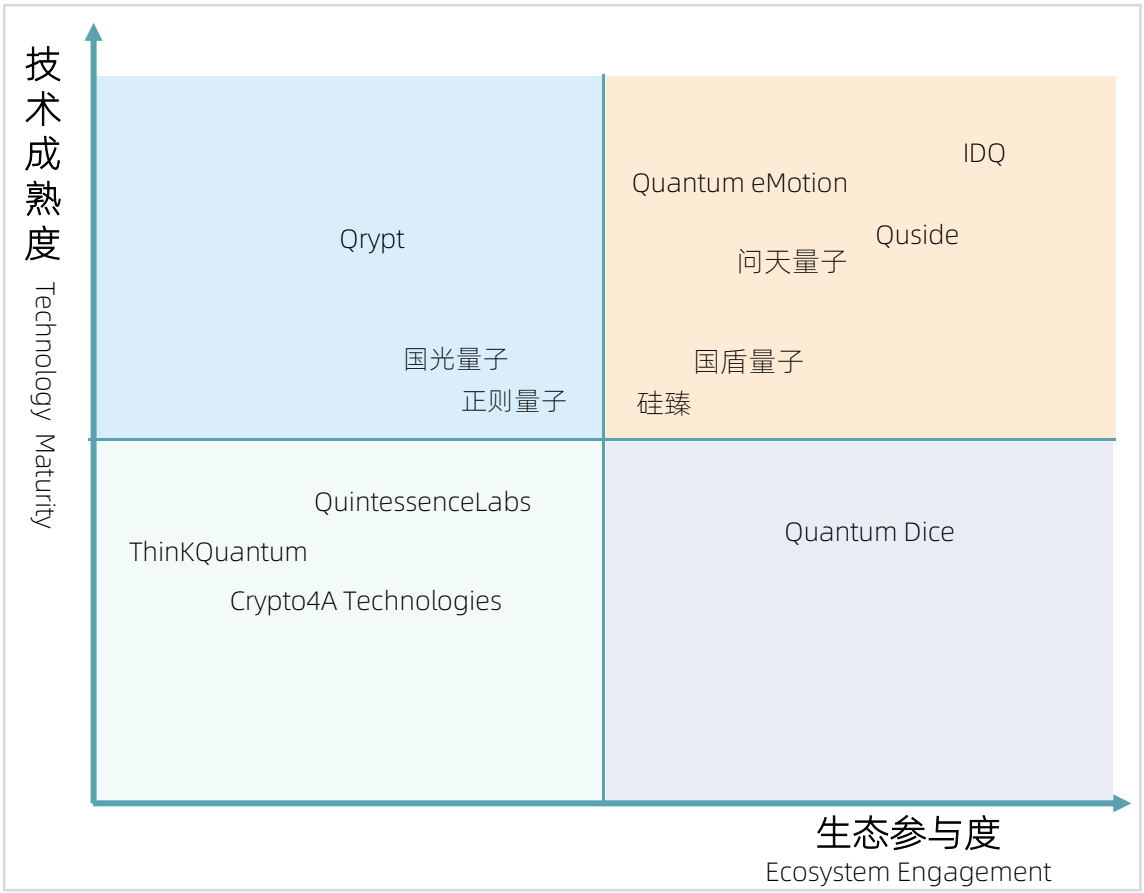
总体而言，从产业演进看，设备成熟度决定 QKD 是否具备落地可行性，而网络化能力则直接影响其应用上限。随着两类能力在工程体系中的持续融合，QKD 的竞争逻辑正在向系统化、网络化方向集中。

02 量子随机数发生器供应商分析

2025 年，QRNG 已逐步从专用安全硬件，演化为支撑密码系统与安全基础设施的底层能力，其产业竞争逻辑随之加速重构。

模型右上区域形成了一批技术与生态均较为成熟的供应商，包括 IDQ、Quantum eMotion、Quside、问天量子、国盾量子 等。这类厂商在量子熵源实现、统计验证和长期稳定运行方面具备成熟基础，其产品已被广泛嵌入通信设备、HSM、数据中心和云平台，逐步演化为安全体系中的底层能力模块。

图表 量子随机数发生器供应商的Q-EMC模型



iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

模型左上区域聚集了一批在特定技术路径上具备优势的厂商，如国光量子、正则量子、Qrypt 等，其在高带宽、低功耗或嵌入式实现方面形成差异化能力，但仍需通过系统级集成来巩固竞争位置。

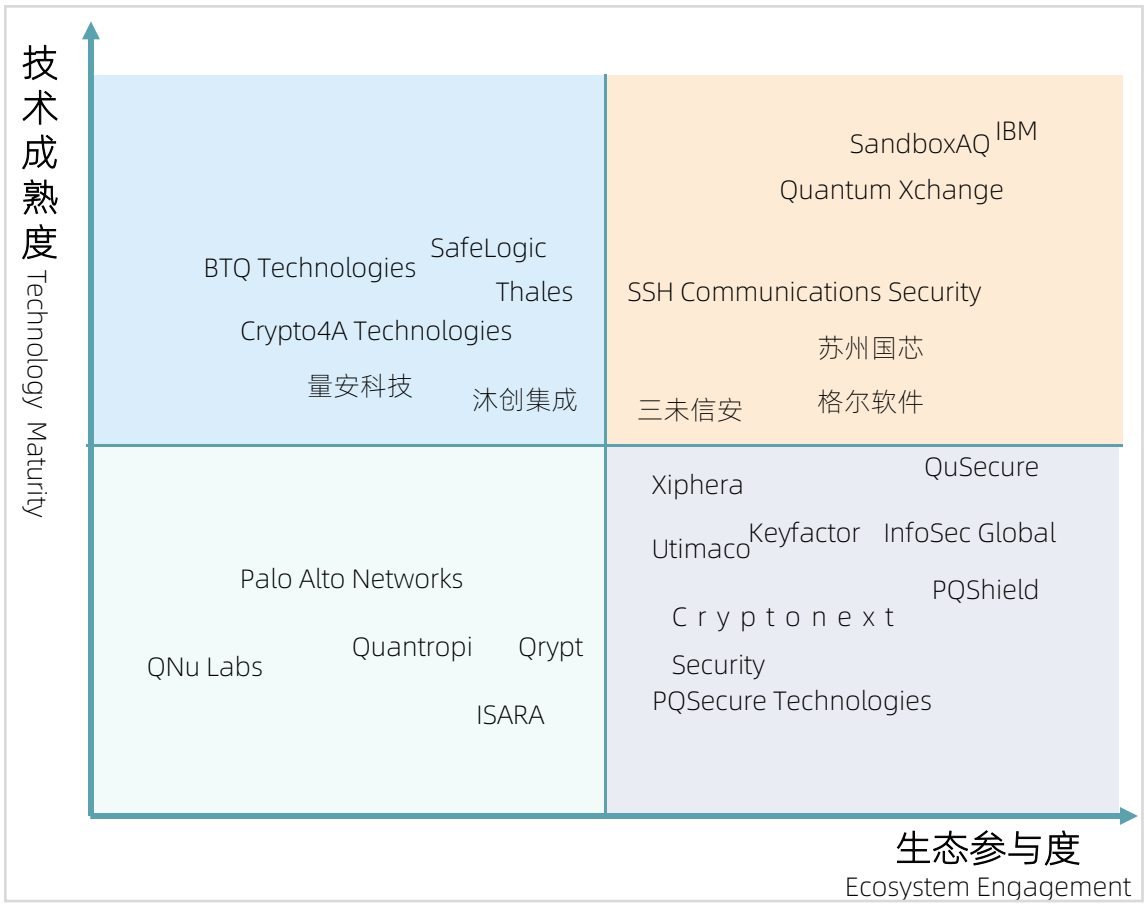
模型右下区域以 硅臻、Quantum Dice等为代表，体现出较强生态参与度但技术成熟度仍在提升中的发展状态。

总体来看，QRNG 领域的竞争已从单一性能指标，转向技术成熟度与生态嵌入能力的双重比拼。

03 抗量子密码供应商分析

2025 年，抗量子密码产业竞争的核心不再局限于算法能力本身，而是更加集中于与既有安全体系的融合深度和工程实施能力。

图表 抗量子密码供应商的Q-EMC模型



ICV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

模型右上区域集中了 IBM、SandboxAQ、Quantum Xchange、SSH Communications Security、三未信安、苏州国芯、格尔软件 等厂商。这类企业在算法实现之外，更强调与云平台、芯片、HSM 及行业应用的协同，其竞争优势已转向迁移实施、治理体系与长期运维能力。

模型右下区域则包括 QuSecure、Keyfactor、InfoSec Global、PQShield 等厂商，其生态参与度较高，但在工程稳定性和规模化迁移经验方面仍处于演进阶段。

模型左上区域以 SafeLogic、Thales、Crypto4A Technologies、BTQ Technologies 等为代表，其在密码工程或合规体系方面具备扎实基础，但在生态协同深度上仍有提升空间。

模型左下区域厂商数量持续收缩，仅保留如 QNu Labs、ISARA、Qrypt 等少数企业，反映出缺乏生态连接能力的抗量子密码技术正逐步被边缘化。

总体来看，抗量子密码的竞争重心已由算法能力转向迁移能力、治理能力与生态协同能力的综合比拼。

04 量子安全代表性厂商分析

2025年，全球量子安全产业的竞争格局在技术路线与市场策略上进一步分化。各国厂商基于自身优势，呈现出不同的发展路径：欧美厂商多依托强大的资本市场和技术生态，在前沿算法、融合应用与标准联盟上引领创新；中国厂商则凭借系统工程的实施能力，持续推进量子保密通信网络的基础设施化；而加拿大、澳大利亚等国的厂商则更加聚焦于特定垂直领域的深度解决方案。

图表 全球量子安全代表性厂商分析

国家\地区	代表性厂商	主导技术路线	发展特征
美国	Palo Alto Networks；Keyfactor；QuSecure；SandboxAQ；Quantum Xchange；Qrypt	以PQC迁移与密码敏捷为主，叠加平台化治理与网络安全产品嵌入	抗量子密码标准落地，竞争重心转向迁移实施与合规交付能力。
欧洲	Thales；Q*Bird；PQShield；CryptoNext Security；ID Quantique；LuxQuanta	工程项目牵引下的QKD网络化落地+PQC合规工程并行，多厂商互操作突出	工程项目牵引，量子安全加速由示范验证走向网络化与体系化落地。
中国	中电信量子集团；国盾量子；硅臻量子；国光量子；光启量子；国科量子；三未信安；格尔软件；苏州国芯	以QKD基础设施化为主，推进QKD+PQC融合与行业工程应用	以中电信量子集团为牵引，多主体协同推进量子安全体系化落地
澳大利亚	QuintessenceLabs	QRNG/密钥与策略管理为底座，借助安全巨头生态扩散	国家资本牵引、产业协同加速的澳大利亚量子安全路径
加拿大	QEYnet；Crypto4A；Quantum eMotion；ISARA；InfoSec Global	星地/空间QKD + PQC/密码敏捷 + HSM/秘密管理平台并行	逐步进入可部署与可验证阶段
印度	QNu Labs	国家安全场景牵引，QKD+PQC一体化交付与工程部署优先	以国家安全场景牵引的印度量子安全落地路径
日本	Toshiba	QKD工程化与服务化，逐步与PQC组合成商业服务	以长期技术积累和大型企业主导，稳步推动量子安全走向商业化应用
新加坡	SpeQtral	以国际协同带动星地链路与金融试点并进	由合作应用迈向全球枢纽

美国：抗量子密码标准落地，竞争重心转向迁移实施与合规交付能力

图表 美国量子安全代表性厂商



iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

2025年，美国量子安全产业进入以迁移执行为核心的新阶段。在抗量子密码标准体系明确的背景下，产业关注点不再集中于算法本身，而是转向三个更具现实约束的问题：

一是存量系统中加密资产的识别与分级；二是抗量子算法在现有网络、身份与密钥体系中的可替换性与兼容性；三是迁移过程能否满足监管、审计与合规要求。在这一阶段，具备平台化工具、工程方法论和交付经验的厂商开始显现优势。

Palo Alto Networks成立于2005年，是美国领先的综合型网络安全厂商，核心产品覆盖下一代防火墙、云安全与安全运营平台。其量子安全路径并非独立推出专用产品，而是将量子准备能力嵌入既有安全平台。

2025年，公司发布量子安全准备相关解决方案，引入加密资产可视化与密码转换能力，并与IBM联合提出面向企业的抗量子迁移路线框架，标志着抗量子安全开始以“平台功能”的形式进入主流网络安全体系。

Keyfactor成立于2001年，是美国数字身份与PKI管理领域的重要厂商，长期聚焦证书生命周期自动化与密钥管理。其技术路线以PKI为切入点，将抗量子密码纳入证书与密钥的日常运维流程。

2025年，Keyfactor在其核心平台中持续增强对抗量子算法和混合证书的支持，并通过测试与演练环境帮助企业提前验证迁移路径，体现出其在“身份体系抗量子化”方向的工程化推进能力。

QuSecure成立于2019年，定位于抗量子网络安全与密码敏捷解决方案提供商，核心产品为QuProtect平台。公司技术路线以迁移管理平台为核心，覆盖加密资产发现、风险评估与替换执行。

2025年，QuSecure推出面向生产环境的QuProtect R3版本，并通过融资与渠道合作推动其在联邦政府与关键行业中的部署，显示出其方案已从概念验证阶段迈入实际应用阶段。

PQSecure Technologies成立于2017年，聚焦抗量子密码在嵌入式系统、安全芯片与硬件IP中的工程化实现，强调算法实现与物理安全并重。其技术路线以可验证实现为核心，覆盖抗量子算法实现、侧信道防护与硬件集成。

2025年，公司多项抗量子算法实现通过美国密码算法验证计划（CAVP），并在可重构硬件平台上推进工程集成，表明抗量子密码已开始进入更底层的硬件部署阶段。

Qrypt成立于2019年，专注于量子熵与量子安全密钥服务，其技术路线并非QKD网络，而是通过高质量量子熵增强现有加密体系。

2025年，Qrypt围绕先收集后解密风险提出量子安全过渡方案，并通过与协作通信平台的联合解决方案，将量子熵能力引入具体应用场景，体现其以底层安全增强为切入点参与抗量子迁移的路径选择。

SandboxAQ在2025年重点推动其量子安全能力进入公共部门与高监管环境，其AQtive Guard产品获得FedRAMP Ready等资质，并在国防与政府机构中用于加密资产自动化发现与抗量子迁移准备。

SafeLogic则继续发挥其在密码模块验证与合规工具链方面的积累，通过扩展CryptoComply与RapidCert等产品，对抗量子算法及混合加密模式的验证流程进行适配，为抗量子密码在既有监管体系内的引入提供现实可行的工程支撑。

Quantum Xchange围绕加密可视化与网络级迁移问题持续推进产品演进，通过CipherInsights与Phio TX平台帮助用户识别量子风险、规划迁移路径，并在高监管行业中验证混合加密方案的部署可行性。

这些厂商的技术路径虽不相同，但均围绕抗量子迁移在真实业务环境中的可实施性与合规可验证性展开。

总体来看，2025年的美国量子安全产业已明显进入标准确定后的执行阶段。头部网络安全与PKI厂商通过平台化能力承载抗量子迁移，专注型企业在迁移管理、硬件实现、量子熵与合规验证等细分环节形成补充，共同构建起覆盖“发现—替换—验证—合规”的完整工程链条。美国量子安全的竞争优势，正在从技术前瞻性转向迁移效率、交付能力与合规成熟度。

中国：以中电信量子集团为牵引，多主体协同推进量子安全体系化落地

图表 中国量子安全代表性厂商



iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

中电信量子集团成立于2023年5月，总部位于安徽合肥，围绕量子密钥分发与抗量子密码在运营级网络中的融合应用，构建量子安全基础设施、密码服务平台及行业应用一体化能力体系，推动量子技术规模化落地。2025年，公司入选工业和信息化部未来信息应用方向领军企业，并入围未来产业创新任务揭榜挂帅单位，面向量子通信核心技术开展集中攻关，进一步确立其在中国量子安全产业中的引领地位。

2025年，中电信量子集团在标准体系、核心技术与规模化应用三方面实现系统性突破。

在标准与生态层面，公司主导立项《支持IMS加密语音业务的量子保密通信终端设备技术规范》，并深度参与量子密码基础设施标准技术联盟建设。

在关键技术方面，发布全球首个融合“QKD+PQC”的分布式密码体系，入选《中央企业科技创新成果推荐目录》，并攻克“通量密一体传输技术”。

在基础设施与应用层面，公司率先建成全球规模最大、技术先进、应用最广泛的量子安全基础设施，在全国40个城市规模化建设，服务覆盖31个省（自治区、直辖市），并推进小型化量子卫星地面站建设与应用验证，支持星地量子通信链路的工程化测试与示范应用。

在应用落地方面，公司以政务、金融、医疗、交通、政法等行业为重点推动量子加密专线和安全服务能力规模化交付，并在重大活动保障场景中开展工程化应用验证；同时，将量子安全能力进一步延伸至物联网终端侧，推动量子加密安全模组在水表、燃气表、摄像头、车载定位等设备中的集成应用，形成网络侧到终端侧的分层防护体系。

国盾量子成立于2009年，总部位于安徽合肥，是中国目前唯一的量子科技上市公司。公司长期聚焦量子密钥分发（QKD）设备、量子通信网络系统及量子安全整体解决方案，推出了包括国盾密语、国盾密盘、国盾密邮等在内的量子安全应用产品，逐步构建起面向多场景的量子安全应用支撑能力。

2025年，国盾量子持续推进量子通信技术在网络化、工程化和场景化层面的落地。一方面，公司加强与中电信量子集团等单位的协同，参与量子通信网络与经典通信网络的融合组网与运营级部署，支撑量子城域网和骨干网的稳定运行及应用扩展；另一方面，在星地量子通信方向，国盾量子持续推进自主产品研发，其微纳量子卫星地面站（型号：QCGS-S280-MN）作为一款面向星地量子密钥分发的自由空间QKD设备，具备体积小、重量轻、可快速部署等工程特点，可协同量子卫星开展星地QKD、星地激光通信及数据传递，为跨区域、跨海乃至跨国用户提供量子密钥共享与安全数据传输能力。



合肥硅臻芯片成立于2020年，总部位于安徽合肥，是中国领先的光量子集成芯片与量子安全产品供应商，聚焦量子随机数发生器（QRNG）等量子安全核心芯片研发。公司致力于将量子基础技术转化为可规模部署的安全硬件，服务于加密系统与智能终端等应用场景。

2025年，合肥硅臻芯片在量子安全芯片产业化方面取得关键进展，其核心产品QRNG-10量子随机数发生器芯片获评安徽省首台套重大技术装备，成为中国首个实现自主供应、具备规模化商用能力的量子安全芯片。在此基础上，公司持续推进量子随机数芯片在通信终端、物联网及关键基础设施中的应用落地，实现批量交付，进一步巩固了其在量子安全底层硬件领域的领先地位。



中科国光量子成立于2021年12月，总部位于北京，由中国科学技术大学博士团队创办，是国内率先布局光量子芯片设计与产业化的企业之一。公司聚焦光量子芯片核心器件研发，产品体系覆盖量子随机数、量子编解码、单光子探测阵列等关键方向，目前已获授权发明专利75项、软件著作权21项，构建起具备自主可控特征的相位编码QKD核心专利体系。

2025年，国光量子围绕光量子技术的工程化应用，持续推进标准体系建设与规范化实践。公司深度参与量子密码与器件相关标准体系建设，作为多项国家与行业标准成员单位，参与《器件无关量子随机数发生器通用要求》（GB/T 45240-2025）等标准制定，为光量子芯片在安全、测量与工业领域的规范化应用奠定基础。

光启量子成立于2025年11月，总部位于河北，是一家面向实用化场景的全栈式量子通信解决方案提供商。公司汇聚了来自中国科学技术大学等高校的资深研发团队，专注于高效并行CV-QKD、非平衡基矢DV-QKD及量子密钥与抗量子密码混合加密架构等前沿技术，是国内少数同时具备连续变量（CV）与离散变量（DV）双制式量子通信设备交付能力的厂商之一。

2025年，光启量子在成立之初即完成了关键技术与市场资源的系统性整合，确立了以高效并行CV-QKD为代表的国际领先技术路线，并在石家庄裕华区落地了“智能大数据信息安全系统”示范项目，建成以量子密钥中心为核心、覆盖23个政务子节点的量子保密通信网络，实现了量子加密技术在政务外网与大数据传输场景中的实际应用。公司同步推进量子安全网关、嵌入式量子安全模块、小型化QKD设备等产品的研发与部署，积极响应国家量子科技发展战略，致力于成为国内量子通信领域的领军企业。

国科量子成立于2016年11月，由中国科学院控股联合中国科学技术大学等发起，总部位于上海，是国家级高新技术企业和国际电信联盟成员单位。公司专注于量子通信技术与网络解决方案，参与国家级量子骨干网建设与标准制订，推动量子通信与信息通信技术融合，在量子安全网络体系与端到端加密服务等领域具备深厚技术积累与工程交付能力。

2025年，量子通信在中国量子科技体系中的产业化和工程化建设持续深化，作为中国量子通信技术力量的重要组成部分，国科量子在量子通信网络体系建设与行业合作中继续稳步前进，并借助量子产业大会等平台加强与生态伙伴的协同，助力推动量子通信从技术示范向规模部署转化。

苏州国芯科技股份有限公司成立于2001年，总部位于江苏苏州，是中国领先的自主可控嵌入式CPU及安全芯片设计企业。公司长期专注于自研芯片、模组与安全解决方案，产品广泛应用于信息安全、网络通信、物联网等领域。

2025年，苏州国芯在量子安全芯片与抗量子密码产品研发与产业化推进上实现显著进展。一方面，其抗量子密码卡产品CCUPHPQ01完成内部测试并进入样品交付阶段；另一方面，与合作伙伴共同研发的抗量子POS芯片CUni360SQ-ZX进一步扩展了公司在信息安全终端与物联网领域的产品应用范围。

三未信安科技股份有限公司成立于2008年8月，总部位于北京，是中国密码基础设施与信息安全产品供应商。公司专注于商用密码技术与产品创新，覆盖密码芯片、密码机、密钥管理、身份认证、抗量子密码产品及整体安全解决方案。

2025年，三未信安围绕“抗量子密码技术与产业化应用”进一步深化研发与行业协同。一方面，公司在2025量子科技和产业大会等权威技术平台集中展示抗量子密码产品与系统方案；另一方面，通过参与《金融业抗量子密码前沿应用研究报告》的编制，推动其技术成果与行业应用路径在金融业务中获得更广泛讨论与认可。

格尔软件成立于1998年3月，总部位于上海，是中国商用密码与数字身份安全领域的骨干企业。公司长期以公钥基础设施（PKI）为核心，构建以身份治理为中心的数字资产安全整体解决方案。

2025年，格尔软件围绕既有PKI与密码基础设施体系，持续推进抗量子密码技术的产品化与应用验证，加快传统密码系统向量子安全体系的平滑迁移。通过完善抗量子密码核心产品、参与权威机构测试验证以及依托G60量子密码应用创新中心深化产业协同，公司在推动抗量子密码由技术探索走向工程化应用方面取得积极进展。

欧洲：
由示范验证走向网络化与体系化落地。

2025年，欧洲量子安全产业的整体特征更加清晰：发展重心不再停留在单点技术或实验验证，而是围绕欧盟与成员国主导的工程项目，推进量子安全在现有通信网络中的部署、互操作与运行管理。

量子密钥分发被视为支撑数字主权和关键基础设施安全的重要技术路径，同时抗量子密码工程化能力也逐步向身份、芯片和平台层延伸。能否适配现网、能否跨厂商协同、能否形成可持续运行的网络体系，成为衡量欧洲厂商能力的重要标准。

图表 欧洲量子安全代表性厂商



iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

THALES
Together • Safer • Everywhere

Thales成立于2000年（由Thomson-CSF于2000年正式更名而来），是欧洲在量子安全领域最具系统集成与工程交付能力的代表性企业之一，长期服务于政府、防务、航空航天及高等级数字身份场景。

2025年，该公司发布多款面向政府与国防场景的抗量子密码产品，包括高等级加密设备与量子抗性智能卡，将PQC能力纳入既有身份与通信安全体系；同时，Thales持续参与欧洲层面的量子通信与空间QKD项目，在EuroQCI框架下推进量子通信服务验证，显示其在欧洲量子安全体系中的枢纽型地位。

Q*Bird成立于2022年，源自荷兰代尔夫特理工大学，是欧洲量子通信初创企业中，向网络化与平台化演进较为突出的代表。公司以测量设备无关量子密钥分发（MDI-QKD）为核心技术路线，重点面向跨域、跨运营环境下的高安全通信需求。

2025年，QBird获得欧盟EIC Accelerator 2025项目支持，为其量子安全网络的规模部署提供资金保障；同时正式推出量子域控制器（QDC），以平台方式实现QKD网络的集中配置、监控与运维；在应用层面，Q*Bird与合作伙伴完成贝内卢克斯地区首个跨境MDI-QKD链路，验证了其方案在多运营环境下的可部署性。

在量子密钥分发设备与工程部署层面

QTI、ThinkQuantum、KeeQuant 、KETS Quantum Security等企业围绕设备小型化、现网兼容性与多厂商互操作能力，持续在运营级通信网络、防务通信与跨域链路场景中推进测试与示范应用。

在核心器件与物理可信性方向

Quantum Optics Jena通过纠缠光子源的独立认证，提升了基于纠缠方案的量子通信在工程可靠性与可验证性方面的基础能力。围绕连续变量量子密钥分发与云、数据中心等新型网络架构，LuxQuanta Technologies在2025年进一步推动CV-QKD系统与现有电信与云基础设施的融合验证。

在量子随机数与底层安全组件层面

Quside与Quantum Dice持续推动量子随机性在数据中心、硬件安全模块与合规体系中的工程化应用。

在抗量子密码工程实现方向

PQShield、CryptoNext Security、Xiphera以及SSH Communications Security等企业，分别从密码库、芯片IP、硬件安全与高等级网络加密设备等角度，推动抗量子密码在欧洲监管环境与关键基础设施中的可部署应用。

这些分布在不同技术层级的实践，共同构成了欧洲量子安全从器件、系统到网络与合规的多层次技术支撑体系。

总体来看，2025年的欧洲量子安全产业已由初创活跃期，进入以工程项目和网络体系建设为牵引的落地阶段。大型系统集成商在高等级安全产品与国家级项目中发挥主导作用，初创企业则在QKD网络化、关键器件和细分技术方向形成补充。欧洲量子安全的竞争优势，更多体现在工程协同能力、跨厂商互操作以及与既有通信网络的深度融合上，为其后续规模化部署奠定了坚实基础。

澳大利亚：国家资本牵引、产业协同加速的澳大利亚量子安全路径

图表 澳大利亚量子安全代表性厂商



iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

Quintessence Labs

QuintessenceLabs成立于2008年，总部位于澳大利亚堪培拉，是澳大利亚最早、也是全球范围内具有代表性的量子安全企业之一。公司长期聚焦量子增强网络安全方向，围绕量子随机数发生、量子密钥分发以及面向关键基础设施的密钥与策略管理能力构建产品体系。

在政府层面

QuintessenceLabs公司获得澳大利亚国家重建基金（NRF）1500万美元战略性投资支持，资金重点用于量子随机数与量子安全密钥管理能力的规模化部署与本土制造能力强化，显示量子安全已被纳入澳大利亚国家级关键技术与安全产业布局。

在产业合作层面

QuintessenceLabs与全球网络安全巨头Fortinet达成量子安全合作，将量子随机数与密钥可信能力引入主流网络安全与防护体系，推动量子安全从“专用高端场景”走向更广泛的企业级与网络级应用。

在国际影响力层面

QuintessenceLabs在世界量子日（World Quantum Day）期间被作为澳大利亚量子初创企业代表重点展示，其在量子随机性与抗量子安全基础能力方面的工程化成果，被视为推动澳大利亚量子技术实现“从科研突破到产业跃迁”的典型案例。

整体来看，2025年的QuintessenceLabs已由以技术领先见长的量子安全厂商，进一步演进为在国家资本支持、全球安全生态协同与关键基础设施部署中发挥核心作用的量子安全平台型企业，体现出澳大利亚在全球量子安全版图中的独特路径与影响力。

加拿大：逐步进入可部署与可验证阶段

2025年，加拿大量子安全产业呈现出鲜明的工程化取向：相比侧重平台与标准治理的美国，以及以网络工程牵引的欧洲，加拿大更加聚焦可部署硬件、量子熵与空间量子通信等具备工程可验证特征的技术方向。在国家量子战略与航天体系支持下，量子安全相关能力正从实验与概念验证，逐步转向可测试、可集成、可交付的产品形态，形成以硬件可信根与空间链路为特色的发展路径。

图表 加拿大量子安全代表性厂商



iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

Qeynet成立于2016年，总部位于加拿大安大略省，是加拿大在空间量子密钥分发（QKD）方向最具代表性的企业之一。公司以微卫星与自由空间光通信为核心技术路线，致力于构建面向全球的星地量子密钥分发能力，突破地面光纤在距离与地理条件上的限制。

2025年，Qeynet获得加拿大空间局超过CA$1.4百万（约US$973,000）的资助，用于推进低成本星地QKD技术的开发与演示，涵盖量子载荷在轨测试、星地密钥生成与更新能力验证。同时，加拿大首颗专门面向量子通信研究的卫星任务QEYSSat在2025年持续推进系统测试与任务准备工作，为未来空间QKD的飞行验证与规模部署奠定工程基础，标志着加拿大在空间量子安全方向迈入实质性实施阶段。

Quantum eMotion成立于2012年，源自加拿大高校科研体系，是加拿大在量子随机数与量子安全芯片方向的重要代表。公司围绕硅基量子随机数微芯片与量子熵源，构建面向金融、国防与关键基础设施的硬件级安全能力，强调可量产、可集成的工程路径。

2025年，Quantum eMotion公司完成首代QRNG混合芯片设计并提交台积电制造，该65纳米CMOS芯片基于量子隧道效应，具备超过1 Gbit/s的量子随机数生成能力，标志着其从设计验证阶段迈向可规模生产。同时，公司通过与Jmem Technology合作，将量子随机数、PUF与抗量子密码模块进行集成，并同步推进FIPS 140-3验证流程，显示其产品正逐步对接北美高合规市场需求。

其他围绕抗量子密码工程化与安全基础设施的代表性企业

Crypto4A Technologies持续深化其量子安全硬件安全模块（HSM）与秘密管理平台能力，通过推出具备加密敏捷性与主权控制特征的QxVault™等产品，推动抗量子密码在政府与关键基础设施中的可控部署；

ISARA则以混合密码体系为核心，推进抗量子算法在身份、PKI与智能卡体系中的行业试点应用；

Quantropi围绕量子安全通信平台，通过跨大西洋安全链路示范与量子熵开放接口，验证其方案在高安全网络中的可用性；

InfoSec Global则从加密资产发现与密码敏捷治理切入，其平台能力在2025年获得FedRAMP授权并通过并购整合进入更大规模的PKI与证书管理体系。

总体来看，2025年的加拿大量子安全产业已逐步形成以空间量子通信、量子随机数与安全硬件为核心特色的发展格局。在国家航天体系与安全需求牵引下，加拿大厂商更加注重技术的工程可验证性与硬件可信基础，其量子安全路径强调“先可部署、再规模化”，为后续在国际量子安全生态中的差异化定位奠定了基础。

印度：以国家安全场景牵引的印度量子安全落地路径



QNu Labs成立于2016年，总部位于班加罗尔，是印度最早将量子密钥分发（QKD）与抗量子密码（PQC）工程化并推向商用的企业。公司以“量子原生网络安全”为定位，形成覆盖密钥管理、网络加密与通信链路保护的产品体系，重点服务政府、国防、金融与航天领域。

在产业合作层面

QNu Labs与VIAVI Solutions建立合作关系，联合推进量子安全网络的测试、验证与部署，加速量子安全从实验环境向运营级网络演进。

在航天安全领域

QNu Labs的本土量子加密技术成功支撑印度一家领先的全栈空间工程解决方案提供商完成全球首个投入商业运营的量子安全卫星发射，实现对关键任务卫星通信的端到端量子级保护。

在规模化应用方面

QNu Labs的量子安全加密体系已在2025年保护1200余家用户与3个战略级数据中心，并为国家关键基础设施部署长达300公里的量子安全网络，实现对高价值视频与业务数据的不可破坏传输，直接服务国家安全与公共安全需求。

在金融基础设施领域

全球领先的支付基础设施机构与QNu Labs达成合作，实现100%的抗量子密码（PQC）合规，显示其技术已具备支撑高并发、高合规要求核心金融系统的能力。

总体来看，印度量子安全产业以少数具备完整产品体系的企业为核心，通过国家安全与重大工程场景实现快速落地，其发展路径更强调“先用起来”，而非全面铺开。

日本：以长期技术积累和大型企业主导，稳步推动量子安全走向商业化应用

Toshiba成立于1875年，总部位于日本东京，是一家拥有百年技术积累的全球综合性高科技企业，在量子通信与量子安全方向拥有超过20年的研究与工程化经验。Toshiba在量子密钥分发（QKD）领域一直处于国际领先地位，提供涵盖QKD设备、量子安全网络平台与密钥管理系统的完整解决方案，并与多家运营商推进商业化应用。

在技术示范层面

- Toshiba与美国合作伙伴Quantum Corridor成功在商业光纤网络上演示了跨州量子密钥分发（QKD）安全通信，在现有运营级光纤基础设施上实现连续量子安全密钥生成与高吞吐量加密传输。
- 在欧洲市场，Toshiba与Orange Business联手推出了法国首个商业化量子安全网络服务“Orange Quantum Defender”，标志着QKD技术在运营级商业网络中的首次大规模应用。
- Toshiba与KDDI Research等合作开发的高容量QKD复用技术实现了在单纤上同时传输高容量数据与量子密钥（33.4 Tbps、80 km），这一突破显著提高了QKD在数据中心互联和高带宽场景中的可用性与经济性，是迈向大规模部署的重要技术进步。

总体来看，日本量子安全的发展更多体现为“以成熟技术推动稳健落地”的路径，由少数具备深厚工程与产业基础的龙头企业持续推进，在全球量子安全商业化进程中扮演着稳定而关键的角色。

新加坡：由合作应用迈向全球枢纽



SpeQtral成立于2017年，总部位于新加坡，是一家专注于量子密钥分发与量子安全通信的高科技企业。公司开发基于光纤与卫星QKD技术的端到端量子安全解决方案，并构建可覆盖陆地和空间链路的量子安全网络架构。

全球互联量子安全网络与商业化推进

SpeQtral与全球卫星运营商SES签署合作备忘录（MoU），双方将共同开发可互操作的光学地面站（OGS），以建立从亚洲到欧洲的长距离卫星量子密钥分发链路，为未来跨洲量子安全通信的互联铺设基础

在金融业网络应用层面

新加坡金融管理局（MAS）联合行业伙伴发布了QKD概念验证沙盒的技术报告，报告显示由SPTel与SpeQtral联合提供的量子密钥分发解决方案在金融服务场景的敏感数据传输中展示了实现可行性。

空间量子通信

SpeQtral的首颗自主开发的量子通信卫星“SpeQtre”已于2025年成功搭载SpaceX Transporter-15发射，并进入轨道，该12U立方星搭载了SpeQtral自主量子光学载荷并与英国RAL Space合作推进载荷调试与未来量子实验，是新加坡与英国合作下的空间量子通信重要工程节点，象征SpeQtral在空间量子链路验证方面实现从地面到空间的跨越式推进。

总体来看，新加坡量子安全的发展以国际协同和应用牵引为主要特征，依托其金融枢纽地位与航天合作基础，逐步形成面向区域互联与跨洲通信的量子安全网络节点，在全球量子安全体系中占据连接区域网络的重要位置。



07

新型应用场景分析

目录

07

新型应用场景分析

01 金融领域

02 电网

03 电信

04 军事国防

05 公共政务

06 其他关键新型场景

新型应用场景

随着量子安全技术逐步走出实验验证阶段，其应用形态正在发生实质性变化。过去以示范工程和技术可行性论证为主的推进方式，已难以满足关键行业对长期安全、稳定运行和合规可控的现实需求。

2025年，量子安全开始更多地嵌入行业核心业务系统，围绕真实业务流程展开部署和验证，其价值不再体现在技术指标本身，而是体现在是否具备可部署、可运维、可审计和可持续演进的工程能力。

从应用路径分析

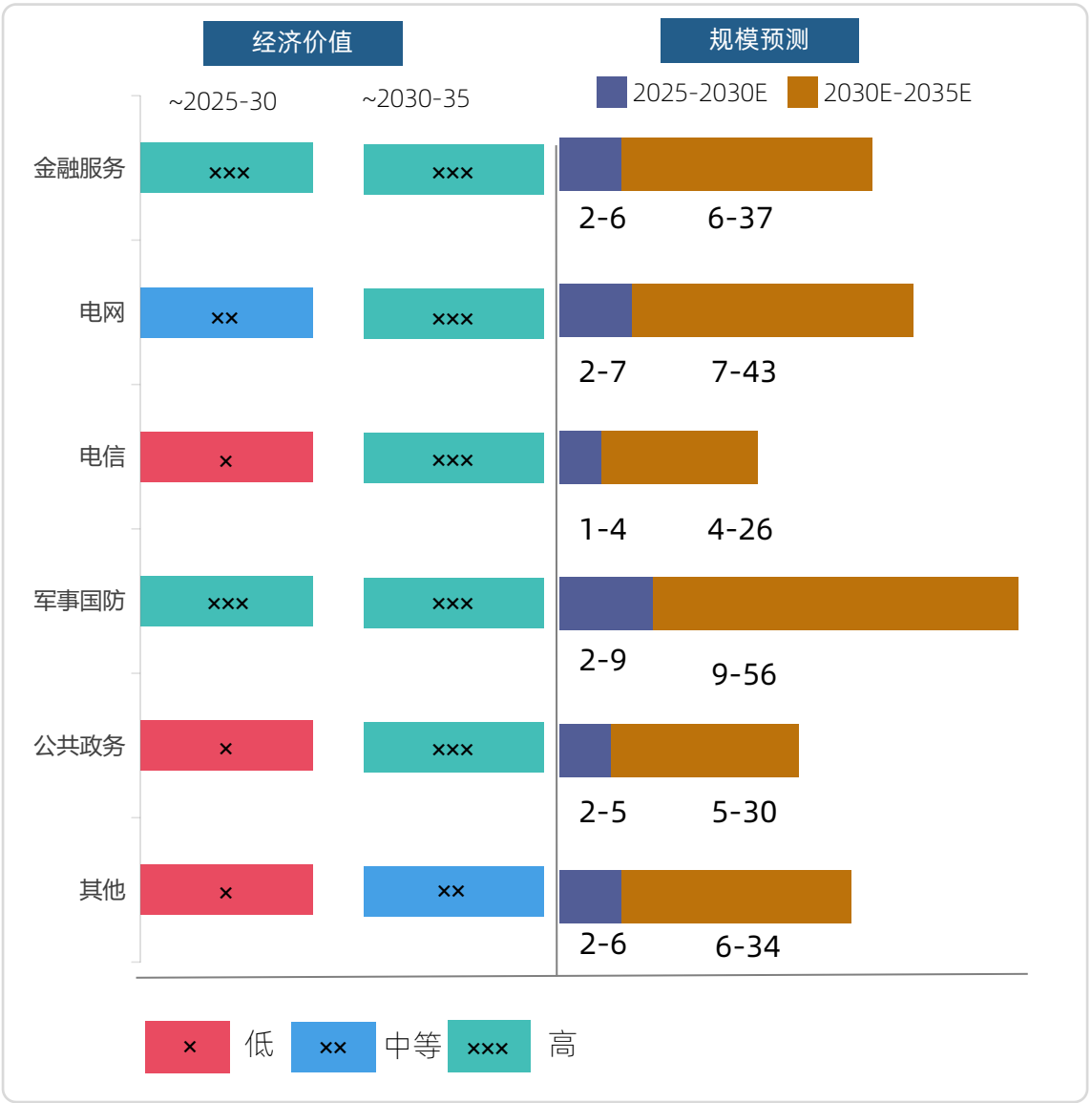
量子安全并非通过单一技术形态切入行业，而是逐步形成以抗量子密码和量子密钥分发为代表的两条互补主线：前者强调对存量系统的广覆盖和可迁移升级，后者侧重在关键链路和高敏感场景中提供更高等级的安全增强。两类技术在不同应用场景中的组合方式，正成为衡量量子安全工程可行性和产业成熟度的重要标志。

从产业规模分析

量子安全在不同行业的应用扩展呈现出明显的阶段性特征。2025—2030年期间，金融服务、电网、电信、军事国防和公共政务等领域，正处于由试点验证向可运营部署过渡的关键窗口期，整体应用规模仍以中低区间增长为主，但行业间分化已开始显现。

进入2030-2035年，随着抗量子密码迁移路径逐步清晰、量子安全服务化能力不断成熟，上述行业有望整体进入加速放量阶段，应用规模区间显著抬升。金融服务、电网和军事国防等领域，预计将率先形成数十亿美元级别的稳定应用市场；电信与公共政务则在平台化和规模复制带动下同步扩展；其余新型应用场景也将逐步形成具备可持续性的需求基础。

图表 全球量子安全应用规模区间预测（2025-2035E, 单位: 亿美元）



iCV TA&K | 2026.2



金融领域：从风险防范走向核心基础设施

金融服务是量子安全最早具备明确落地路径、同时也是应用逻辑最为清晰的行业之一。其对量子安全的需求，源于长期数据保密要求、高度严格的监管与审计制度，以及跨机构、跨地域业务对安全互联的持续依赖。进入2025年，全球金融机构在量子安全领域的关注点已明显从前期的技术验证和专项实验室建设，转向面向核心业务系统的实质性部署与迁移准备。

在这一过程中，金融行业逐步形成了以抗量子密码作为基础能力、以量子密钥分发作为高安全补充的双轨应用模式。抗量子密码被用于覆盖范围最广的系统迁移和接口改造，支撑身份认证、密钥管理和通信协议的长期安全演进；量子密钥分发则主要服务于对安全等级要求极高的跨机构通信、核心数据互联和关键业务链路，作为现有安全体系的增强层。

通过真实业务环境验证量子安全的工程可行性

- 美国银行业首次出现面向真实业务环境的量子安全商业采购案例：量子计算公司QCi获得美国前五大银行的订单，为其部署基于纠缠光子的量子通信测试平台，用于建设专用的量子安全验证与研发环境，标志着量子通信首次以明确商业订单形式进入美国银行体系。
- 新加坡金融管理局（MAS）联合多家商业银行，在实际金融通信链路上开展量子密钥分发试点，重点评估其在金融网络中的稳定性、可运维性及与现有系统的融合能力。

面向中长期的应用前景

从产业规模看，2025-2030年期间，金融领域相关应用规模预计处于2-6亿美元区间，量子安全已从试点验证进入可评估、可持续推进的实际部署阶段；进入2030-2035年，随着抗量子迁移经验积累、运营级服务能力成熟以及跨机构协同机制完善，应用规模有望进一步扩大至6-40亿美元，并逐步形成在不同金融体系间可复制、可推广的实施模式。

总体而言，金融领域的实践表明，量子安全是一项循序推进的系统工程，其核心价值在于为金融基础设施提供长期、可验证的安全支撑。

电网领域：围绕运行连续性与调度可信性的量子级加固

电网系统是量子安全在行业侧最具现实约束条件的应用场景之一。与金融侧以数据保密为核心不同，电力系统对安全的首要诉求集中在运行连续性、调度指令可信性以及关键控制链路的抗干扰能力上。随着新能源占比提升、电网结构向分布式和高度互联演进，传统基于经典密码的通信与控制体系在长期安全性和系统韧性方面逐渐暴露出不足。

2025年，电网领域对量子安全的关注重点已从技术可行性验证，转向是否具备工程可部署性、可运维性以及与既有电力通信体系的兼容能力。量子安全不再作为独立通信系统存在，而是被纳入电力调度、分布式能源管理和关键控制链路的整体安全设计中，其目标是在不改变现有系统架构的前提下，对高风险链路和核心业务节点进行分层增强。

真实业务场景中的量子安全落地实践

- 中国国家电网浙江电力在绍兴新昌首次将量子安全技术引入分布式能源聚合业务，开展真实电力业务数据的量子加密传输验证。针对分布式能源点多、链路长、调度频繁的通信特性，该项目提出了适配电力远距离通信的量子密钥生成与分发优化方案，缓解了长距离传输中光信号衰耗大、密钥生成效率下降等问题，并创新设计了“聚合—接入”双阶段量子加密架构，实现了125公里“光纤+量子”的数据加密传输，较传统方案显著拓展了可用距离。

电网领域量子安全应用呈现出几个清晰特征

- 一是优先服务于对系统稳定性影响最大的调度与控制数据，而非一般业务通信；
- 二是强调与现有电力通信体系协同运行，量子安全更多作为增强能力嵌入，而非独立系统建设；
- 三是高度重视长期运行与维护成本，工程可持续性优先于短期性能指标。

面向中长期的应用前景

从产业规模趋势看，电网领域量子安全在2025-2030年预计将形成2-7亿美元的稳定应用区间，主要集中在分布式能源调度、跨区域电力通信和关键控制系统加固等方向；2030-2035年，随着新能源系统复杂度持续提升、量子通信工程能力成熟，其应用规模有望扩大至7-45亿美元区间，并逐步向区域级乃至国家级电力安全基础设施演进。

总体来看，电网领域的实践表明，量子安全的核心价值不在于单一技术指标的提升，而在于其是否能够嵌入电力系统的运行逻辑，为高度复杂、强实时性的能源基础设施提供稳定、可验证的长期安全支撑。这一特性，也使电网成为量子安全由示范应用走向关键基础设施能力的重要落脚点。



电信领域：从网络能力验证走向可运营的量子安全服务

电信网络是量子安全最早介入、同时也是工程复杂度最高的应用领域之一。其核心特点在于网络规模大、业务类型多、对连续运行和性能稳定性要求极高，这决定了量子安全在电信领域的落地不可能以孤立链路或专用系统为主，而必须与既有光传输网络、加密协议体系和运营模式深度融合。

量子安全服务开始商用落地

Orange Business 与东芝联合推出量子安全网络服务，为巴黎地区金融机构提供融合量子密钥分发与抗量子密码的加密通信能力。

基础设施能力建设加速

中国电信在云网融合、通话安全和平台服务等多个层面推进量子安全能力建设，通过融合量子密钥分发与抗量子密码的分布式密码体系、量子加密专线和多形态密码服务组件，将量子安全作为通用能力嵌入网络与业务平台之中。

网络工程层面的融合部署持续推进

东芝、NEC与日本信息通信研究机构在NTT研发的全光网络环境中，完成了量子密钥分发信号与高速经典通信信号的同纤复用验证。

抗量子密码以低扰动方式加速落地

国际运营商Sparkle与Arqit在城域光传输网络中完成了量子韧性数据传输验证，对加密能力接入后的链路性能和业务影响进行了系统评估。

面向中长期的应用前景

从产业规模趋势看，电信领域是量子安全最具规模化潜力的应用方向之一。2025-2030年期间，量子安全在电信网络中的应用规模预计处于1-4亿美元区间，主要增长动力来自运营商侧对骨干网络、数据中心互联以及行业专线安全能力的持续投入；进入2030-2035年，随着量子安全能力进一步嵌入核心网络架构，并以服务化、平台化方式向政企客户输出，其应用规模有望扩大至4-30亿美元区间，成为量子安全产业中增长弹性较高的细分领域。

总体来看，电信领域的量子安全演进路径呈现出明显的基础设施特征：以网络级部署为载体，以现网融合和长期稳定运行为前提，通过运营商的服务能力实现规模扩散。其价值不仅体现在提升通信网络的长期安全水平，更在于为金融、政务和关键行业提供可复用的量子安全底座，成为量子安全走向广泛应用的重要支点。

军事国防领域：由前沿能力验证走向体系级安全能力嵌入

军事与国防领域是量子安全最早被纳入国家战略规划、同时也是安全等级要求最高的应用场景之一。与金融和电信侧重业务连续性和规模化不同，军事领域更加关注在复杂对抗环境下的信息可信性、抗干扰能力和体系韧性。

2025年，量子安全在军事国防领域的应用重心已不再停留在技术原理验证，而是逐步嵌入防御体系升级和作战支撑能力建设之中。

在国家层面，量子技术已被纳入核心防御系统的长期演进规划

- 在北美防空体系升级背景下，加拿大Photonic Inc.入选由国防部门主导的NORAD现代化技术竞赛，获得专项资金支持，用于推进量子中继和量子网络相关技术研发。
- 美国空军与Qunnect合作，围绕基于商用光纤的城域纠缠量子网络组件开展研发与部署测试，重点评估其在战术环境下的可实施性、稳定性以及与既有军事通信规范的适配程度。

面向中长期的应用前景

从产业规模趋势看，军事国防领域在量子安全应用中具有高安全等级、小规模起步、长期持续投入的典型特征。2025-2030年期间，相关应用规模预计处于2-9亿美元区间，主要集中在防空、指挥通信和高价值信息链路等核心场景；进入2030-2035年，随着量子通信与抗量子密码能力进一步融入防御体系建设，其应用规模有望扩大至9-60亿美元区间，成为量子安全产业中技术门槛最高、战略属性最强的应用领域之一。

总体来看，军事国防领域的实践表明，量子安全并非以快速扩张为目标，而是以体系安全和长期可信为导向，通过循序推进的工程化方式嵌入关键防御系统，其发展节奏和应用形态将持续深刻影响全球量子安全技术的演进方向。

公共政务：以城市级平台和制度约束为牵引的量子安全落地

公共政务是量子安全最早被纳入整体规划、同时推进节奏相对稳健的应用领域之一。与金融和电信侧重业务效率和市场化扩展不同，政务场景更强调数据主权、跨部门协同以及长期安全责任，其量子安全建设往往以区域平台和制度性安排为主要抓手。

2025年，量子安全在公共政务领域的应用向城市级、区域级安全底座建设演进。

在国家层面，量子技术已被纳入核心防御系统的长期演进规划

- 在中国，**城市级量子安全基础设施已开始服务于政务体系的实际运行。**中国电信在四川绵阳建成西南地区首个城市级量子城域网，构建了融合量子密钥分发与抗量子密码的统一安全架构。
- 在欧洲，**公共政务侧的量子安全推进更多通过制度与规则来实现。**欧盟《数字运营弹性法案》正式生效，要求成员国相关公共管理体系和关键行业建立面向长期风险的安全应对机制，其中包括对抗量子迁移准备工作的系统性评估。

面向中长期的应用前景

从产业规模趋势看，公共政务在量子安全应用中具备稳步扩展的特点。2025-2030年期间，相关应用规模预计处于2-5亿美元区间，主要集中在城市级政务网络、跨部门数据交换和公共服务平台安全加固；进入2030-2035年，随着制度要求持续强化和区域级量子安全底座逐步完善，其应用规模有望扩大至5-30亿美元区间，成为支撑国家和城市数字治理长期安全的重要组成部分。

总体来看，公共政务领域的实践表明，量子安全在该领域并非以单点技术应用为目标，而是作为数字政府体系中的基础性安全能力，通过平台化建设和制度化约束逐步落地，为公共治理系统提供面向未来的长期安全支撑。



其他关键新型场景：量子安全在多元系统中的前沿嵌入

除金融、电信、电网和公共政务等核心领域外，量子安全在一批新型应用场景中也开始显现出实际落地迹象。2025年，这类应用更多以能力嵌入和模式探索为主，重点验证其在复杂系统中的工程适配性和长期运行可行性，为后续规模化推广积累实践基础。

云计算与数据服务

量子安全正逐步被纳入平台级基础能力体系。2025年，美国主要云服务商开始将抗量子密码能力以托管服务的形式向用户开放。Google Cloud在其Cloud KMS中上线了抗量子数字签名能力的预览版本，使企业能够直接在云端调用符合NIST标准化路线的抗量子算法，用于代码签名与密钥管理，从而在不重构业务系统的前提下完成安全能力升级。这一模式有效降低了量子安全迁移门槛，为跨行业应用提供了可复用的云端安全底座。

物联网与设备端系统

在物联网与设备端系统中，量子安全的应用路径更加注重嵌入式和轻量化。

- 欧洲企业SEALSQ与WISeKey推出面向工业设备和机器人系统的量子安全解决方案，将抗量子密码芯片、硬件信任根与设备身份管理体系进行集成，用于保障设备在制造、部署和运维全生命周期内的可信运行。
- Patero公司将其抗量子加密技术以可插拔模块形式集成至Syllego的分布式城市安全平台，为大规模物联网设备与边缘节点提供即时量子安全防护，展示了通过平台化方式提升部署效率、降低终端改造成本的现实路径。

交通与智能系统

量子安全更多以分层方式融入现有架构。

- 韩国相关企业在自动驾驶安全探索中，将Boss Semiconductor的车载AI芯片与EYL提供的量子随机数发生器技术相结合，用于增强车端计算与通信过程中的密钥不可预测性。
- 在中国市场，小鹏汽车与阿里云围绕抗量子安全技术开展联合研发，计划将抗量子密码能力逐步扩展至车云通信、V2X基础设施以及机器人等关联场景。

空天与极端环境通信

量子安全呈现出明显的基础设施化特征。

欧洲相关企业和研究机构围绕卫星通信和远程链路安全，开始探索将抗量子密码能力引入空间通信系统。SEALSQ宣布通过卫星任务验证其量子安全密钥管理与信任根技术，重点评估其在在轨运行条件下的稳定性与长期可靠性。

面向中长期的应用前景

从产业规模趋势看，其他关键新型场景在量子安全应用中具备较大的弹性空间。2025-2030年期间，相关应用规模预计处于2-6亿美元区间，主要增长动力来自云平台安全能力下沉、设备端可信体系建设以及新型基础设施安全需求；进入2030-2035年，随着技术成熟度提升和应用模式逐步清晰，其应用规模有望扩大至6-35亿美元区间，成为量子安全产业的重要补充增长极。

总体来看，这些新型场景的实践表明，量子安全正在通过嵌入式、平台化和分层部署等方式，逐步融入更广泛的数字系统之中。其价值不在于替代既有安全体系，而在于为复杂环境和新型应用提供面向长期风险的可持续安全支撑。



08

产业分析预测

目录 08 产业分析预测

01 量子密钥分发：2035年迈入数十亿美元级

02 量子随机数发生器：区域格局稳定下的规模增长

03 抗量子密码：标准体系落地推动市场规模加速扩张

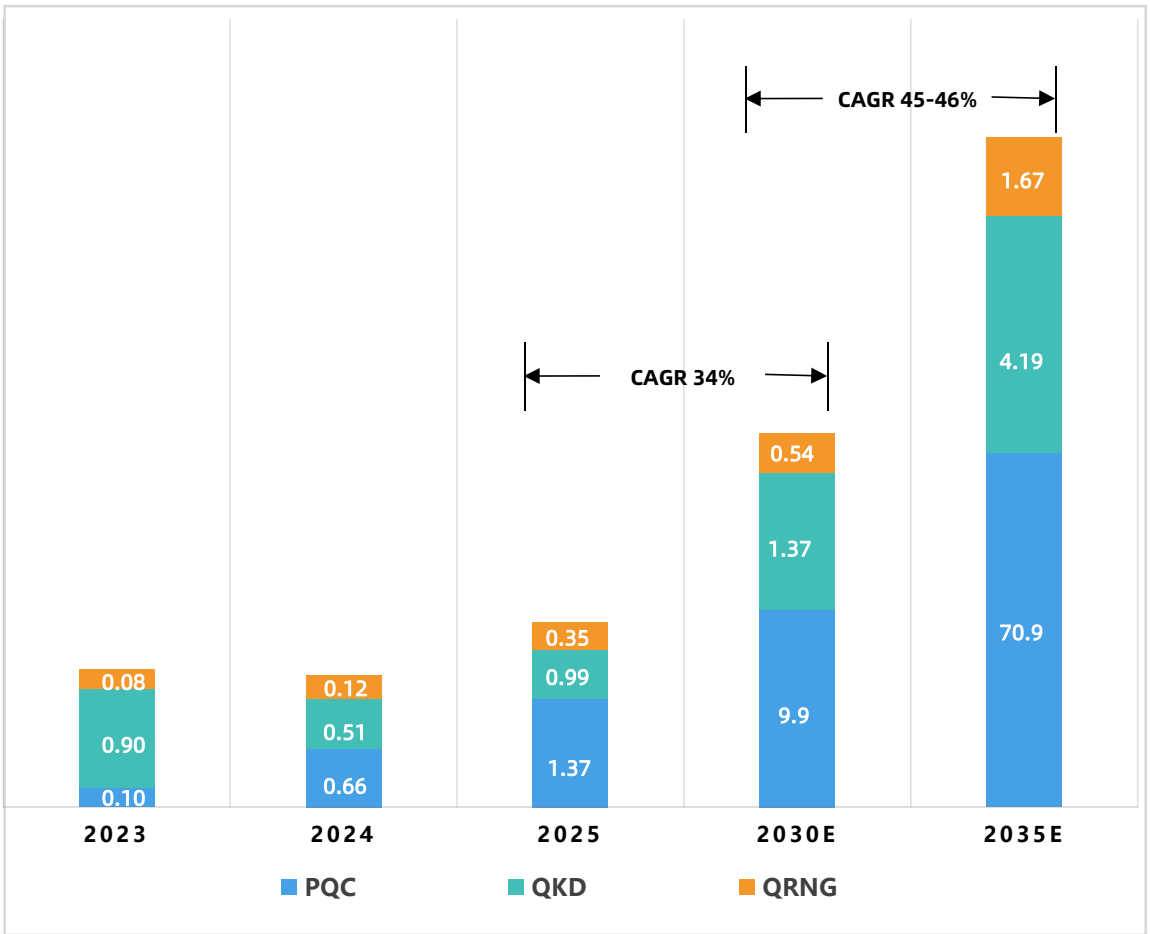
全球产业规模分析预测

2025年，全球量子安全产业在监管合规、工程化部署与关键基础设施应用的共同推动下，进入明确的规模扩张阶段。

从产业规模看，2025年全球量子安全产业规模约为27.03亿美元。预计到2030年，该规模将增长至约118.05亿美元，2025-2030年期间年复合增长率（CAGR）约为34%，显示出量子安全产业在中短期内仍将维持高速扩张态势。

从中长期看，随着抗量子密码与量子密钥分发的协同应用在关键基础设施、跨境通信和高价值数据保护等场景中逐步形成稳定部署模式，量子安全市场有望在2030年后进入新一轮加速扩展阶段。预计2035年全球量子安全产业规模将达到约767.95亿美元，2030-2035年期间年复合增长率约为45%-46%。这一阶段的高增长，反映出量子安全正从面向特定高安全需求场景的补充性技术，演进为支撑全球数字系统长期安全运行的重要基础能力，并在未来信息基础设施体系中占据更加核心的位置。

图表 全球量子安全产业规模预测（2023-2035E, 单位：十亿美元）

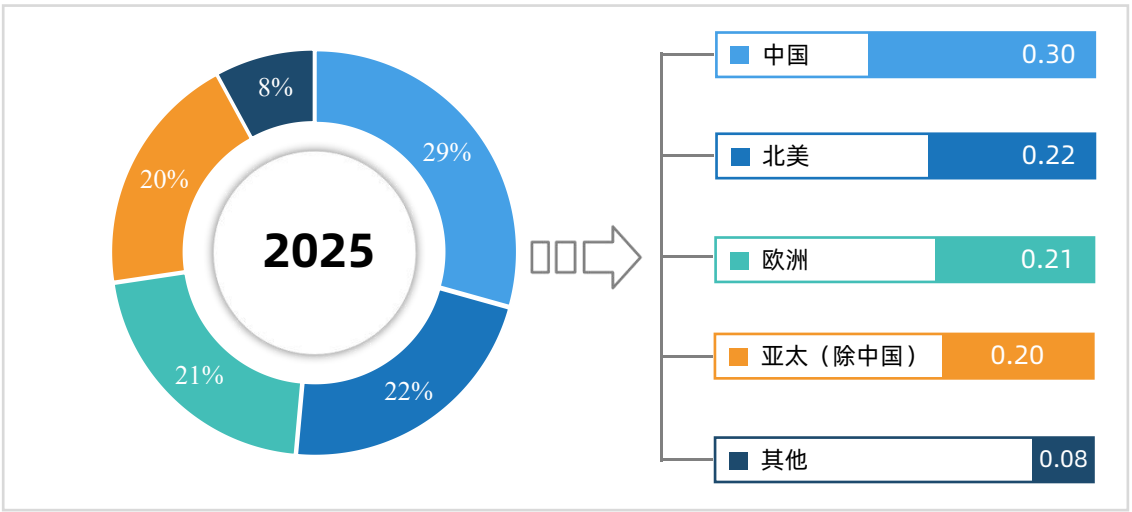


01 量子密钥分发 2035年迈入数十亿美元级

量子密钥分发作为量子安全体系中最早进入工程化部署的技术方向之一，其产业发展呈现出典型的基础设施型特征，短期受项目建设节奏影响，但中长期保持稳定扩展趋势。2025年，全球量子密钥分发产业规模约为9.92亿美元；预计到2030年将增长至约13.71亿美元，2025-2030年期间年复合增长率约为6.7%。在更长期维度上，随着量子安全网络逐步由试点建设向区域化、网络化部署推进，2035年全球量子密钥分发产业规模预计将达到约41.85亿美元，2030-2035年期间年复合增长率约为25%。总体来看，量子密钥分发市场增长节奏与通信基础设施投资周期高度相关，其长期扩张主要依赖于关键基础设施安全需求和量子—经典融合网络的持续建设。

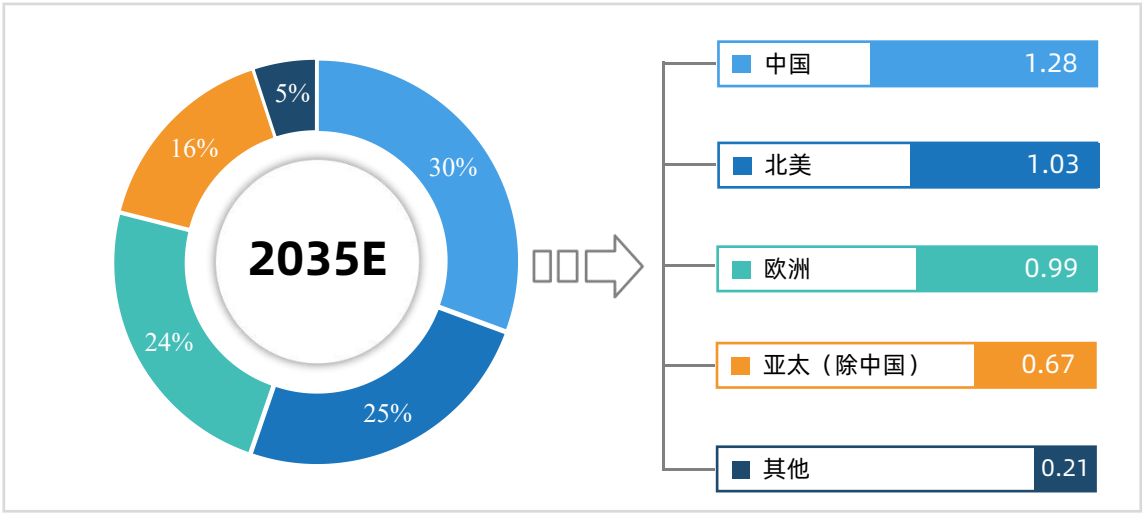
2025年，中国在全球量子密钥分发产业中继续保持领先地位，产业规模位居各地区之首，北美、欧洲及亚太地区（不含中国）处于第二梯队。展望中长期，到2035年，各主要地区量子密钥分发产业规模均呈持续增长态势，中国市场规模增长相对较快，在网络建设和应用推进方面保持较高活跃度，区域间差距总体保持可控，全球量子密钥分发产业呈现多区域并行发展的格局。

图表 2025年全球各地区量子密钥分发产业规模（单位：%，十亿美元）



iCV TA&K | 2026.2

图表 2035年全球各地区量子密钥分发产业规模预测（单位：%，十亿美元）



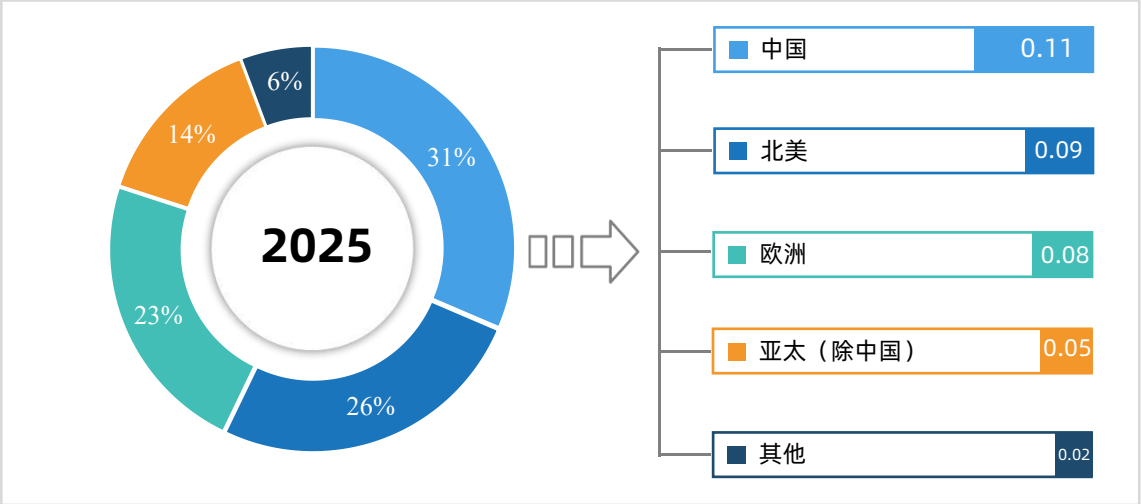
iCV TA&K | 2026.2

02 量子随机数发生器：区域格局稳定下的规模增长

2025年，量子随机数发生器在芯片集成、制造工艺与材料体系等方面持续取得进展，器件体积不断缩小、成本逐步下降，为其在密码系统、通信设备和安全终端中的规模化应用奠定了基础。

2025年，全球量子随机数发生器产业规模约为3.51亿美元，在量子安全整体产业中占比仍相对有限，但应用场景持续拓展。预计到2030年，全球量子随机数发生器市场规模将增长至约5.49亿美元，2025-2030年期间年复合增长率约为9%-10%。随着量子随机数在密码学、安全芯片及高可靠模拟等领域的应用不断深化，2035年全球量子随机数发生器产业规模预计将达到约16.74亿美元，2030-2035年期间年复合增长率约为25%。总体来看，量子随机数发生器产业呈现出前期稳步推进、后期随应用放量加速扩展的发展特征。

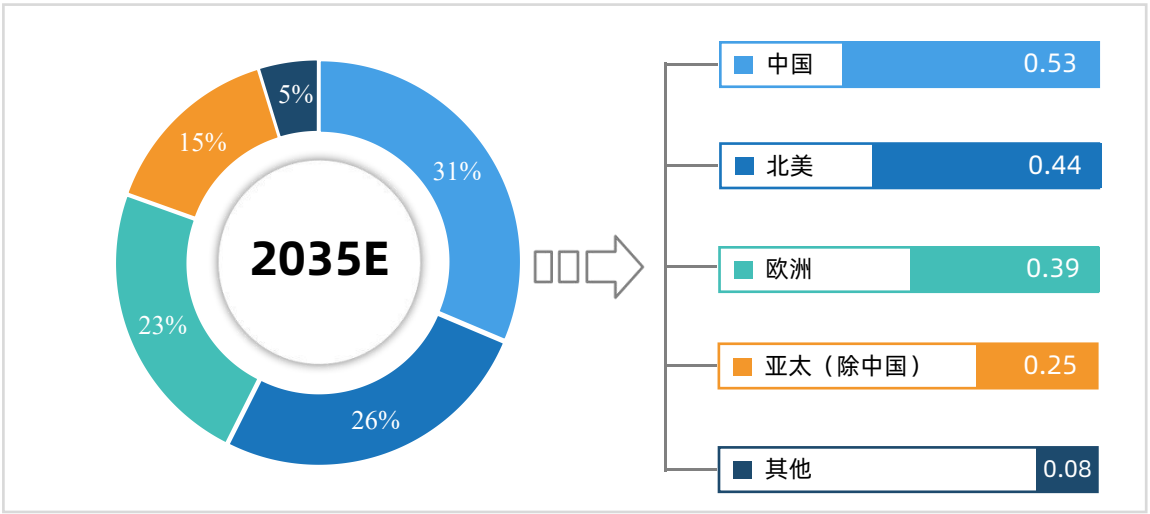
图表 2025年全球各地区量子随机数发生器产业规模（单位：%，十亿美元）



iCV TA&K | 2026.2

2025年，全球量子随机数发生器产业呈现出较为清晰的区域梯队格局，中国产业规模处于领先位置，北美和欧洲紧随其后，亚太地区（不含中国）及其他地区整体规模相对较小，但均保持稳定发展态势。各区域在技术路线和应用方向上的差异，使得产业分布呈现出一定层次性。

图表 2035年全球各地区量子随机数发生器产业规模预测（单位：%，十亿美元）



iCV TA&K | 2026.2

从中长期来看，到2035年，全球主要地区量子随机数发生器产业规模预计均将实现显著增长，区域间的位次关系整体保持稳定，中国、北美和欧洲仍构成市场主体，亚太（不含中国）及其他地区的规模同步扩大但未出现结构性跃升。这一格局表明，量子随机数发生器领域的竞争更多体现为各区域同步扩展，而非市场份额的快速重构。

从发展趋势看，未来量子随机数发生器市场增长的核心驱动力主要来自应用侧需求的持续释放。一方面，随着数据安全要求不断提高，量子随机数逐步从独立安全设备向安全芯片、通信系统和密码基础设施中的关键功能模块渗透；另一方面，与抗量子密码的协同应用不断深化，高质量真随机数在密钥生成和协议安全中的基础性作用日益凸显，推动相关解决方案在高安全场景中加快落地。

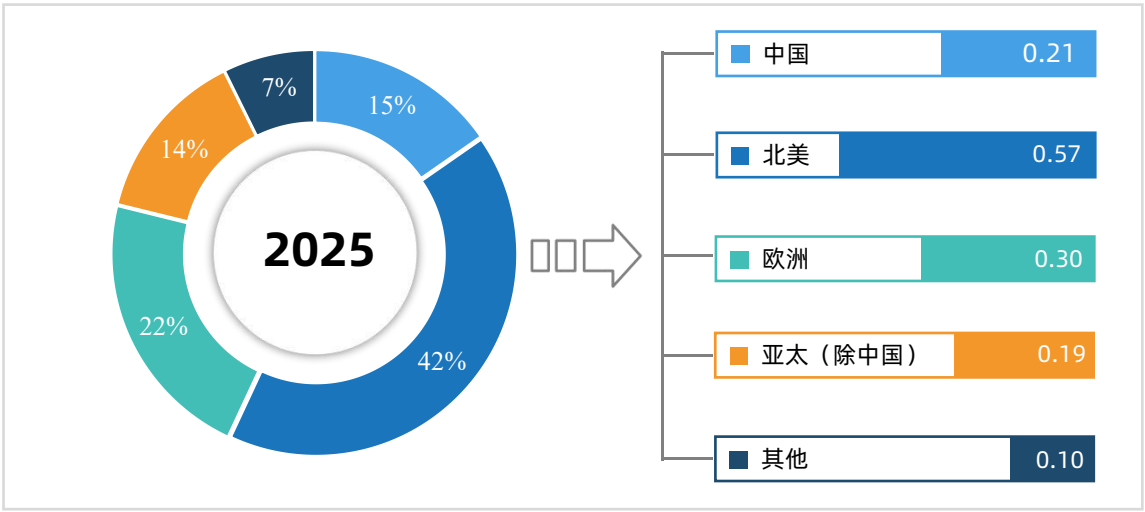
总体而言，未来几年全球量子随机数发生器产业的扩展将更多体现在应用场景的持续拓展和终端集成度的提升上，而非单一区域的快速放量。随着产业规模逐步扩大，上游芯片与器件研发、中游模块与系统集成以及下游行业应用服务等环节将同步完善，推动量子随机数发生器在全球范围内形成更加成熟、稳定的产业体系。

03 抗量子密码：标准体系落地推动市场规模加速扩张

随着美国抗量子密码标准化工作进入落地实施阶段，全球抗量子密码产业发展明显提速，2025年产业规模约为13.72亿美元，在量子安全各技术方向中已成为增长最为显著的板块。预计到2030年，全球抗量子密码产业规模将增长至约99.3亿美元，2025-2030年期间年复合增长率约为49%；进一步展望到2035年，产业规模有望达到约709.36亿美元，2030-2035年期间仍将保持接近49%的年复合增长水平。

总体来看，在标准体系逐步明确和存量信息系统密码迁移需求持续释放的共同作用下，抗量子密码正加速从前沿安全技术向通用信息安全基础能力转变。

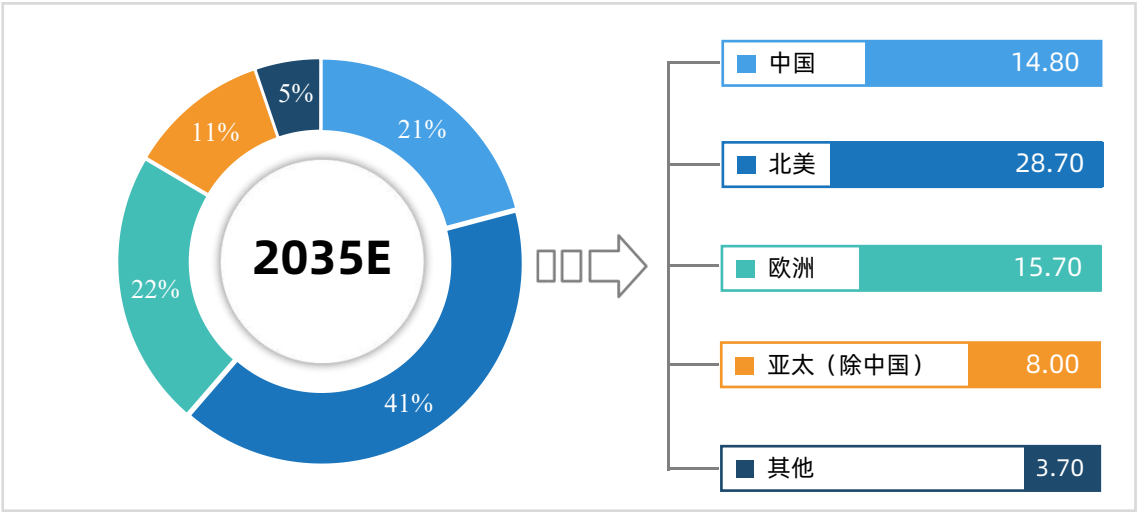
图表 2025年全球各地区抗量子密码产业规模（单位：%，十亿美元）



iCV TA&K | 2026.2

2025年全球抗量子密码产业呈现出较为明确的区域梯队：北美规模领先，欧洲位居第二，中国处于紧随其后的第三梯队，亚太（不含中国）及其他地区规模相对较小但具备一定基础。这一格局与北美在密码标准体系推进、产业生态成熟度和存量系统迁移需求集中释放等因素相匹配，也解释了其在当前阶段的领先优势。

图表 2035年全球各地区抗量子密码产业规模预测（单位：%，十亿美元）



iCV TA&K | 2026.2

到2035年，全球各地区抗量子密码产业规模预计将同步显著扩大，北美的领先地位总体延续，中国与欧洲的市场体量增长更为明显，亚太地区（不含中国）及其他地区也将形成更具规模的市场空间。整体来看，区域间的相对位次大体保持稳定，同时头部地区之间的差距逐步收敛，全球抗量子密码市场正由早期的单一领先格局，向多区域并行扩展的结构演进。

从趋势驱动看，抗量子密码产业增长主要由密码体系迁移需求所推动，而非单点技术突破本身。随着美国抗量子密码标准进入落地实施阶段，欧盟和中国加快相关标准与应用推进，全球主要经济体的密码迁移进程逐步明确，叠加关键行业对长期安全的现实需求，抗量子密码正由验证应用走向规模化部署。

总体来看，抗量子密码产业的发展将更多受到标准落地和密码体系迁移节奏的共同影响。短期内，相关应用以对现有系统的替换和兼容为主，重点在于降低迁移成本、保障业务连续性；随着迁移范围逐步扩大，抗量子密码将在安全芯片、密码基础软件以及关键基础设施安全体系中形成更加稳定的应用基础。伴随产业链配套能力的完善，抗量子密码在全球量子安全产业中的规模贡献有望持续提升。



09

产业展望

目录 09 产业展望

01 政府与制度强力介入，是量子安全发展的根本前提

02 市场进入持续增长阶段

03 抗量子迁移进入以合规要求为核心的实施阶段

04 混合加密成为网络基础设施的主流配置

05 交付能力成为核心变量，量子安全竞争重心发生转移

06 地缘政治格局固化，形成中美欧三大技术阵营

07 多量子技术融合成为长期趋势

08 “量子+”加速落地，量子安全嵌入数字基础设施

01 政府与制度强力介入，是量子安全发展的根本前提

2025年，量子安全逐步从以技术前瞻为主的议题，演变为国家层面需要长期统筹的安全治理问题。各国政府不再局限于科研资助或示范工程，而是通过制度设计、合规框架和执行机制，将量子安全纳入关键基础设施保护和长期数据安全的整体安排之中。

量子安全要求开始嵌入国家网络安全与数字治理体系

在具体实践中，多国已将抗量子密码迁移和量子安全要求，明确纳入国家网络安全和数字治理体系。

- 美国通过一系列立法和政策文件，引导联邦机构和关键行业提前规划抗量子迁移路径；
- 欧盟在DORA等法规框架下，将加密失效风险视为运营韧性评估的重要组成部分；
- 加拿大则发布联邦层面的PQC迁移路线图，对时间节奏和责任分工作出明确安排。

制度介入重塑产业运行逻辑与竞争门槛

随着制度层面的持续介入，量子安全产业的运行逻辑正在发生变化。解决方案提供方不仅需要具备技术能力，更需要能够融入既有IT和网络体系，支持分阶段部署、长期运维，并满足审计与合规要求。相较于单点技术突破，工程成熟度、体系完整性和交付可靠性的重要性显著提升，这也在客观上抬高了行业准入门槛。

长期治理需求为规模化应用提供制度支撑

从更长周期看，只要关键数据的长期保密性和核心系统运行韧性仍是国家治理的重要议题，政府对量子安全的持续介入就将成为常态。这一趋势将持续影响技术路线选择和产业结构演化，并为量子安全由示范应用走向规模化部署，提供相对稳定、可预期的制度环境。

02 市场进入持续增长阶段

尽管2025年全球量子科技整体投资热度趋于理性，但量子安全并未随之降温。在合规要求持续强化的背景下，相关投入反而进入更加稳定、可预期的增长通道。多项行业研究与企业实践显示，广义量子安全市场仍保持约30%—40%的年增长水平，需求结构也正在由分散探索走向清晰聚焦。

这一轮增长并非主要由新应用场景驱动，而是源于既有信息系统面临的系统性升级压力。随着抗量子迁移被正式纳入合规与风险管理框架，围绕身份认证、证书体系、密钥管理以及通信协议等基础安全能力，越来越多的系统进入集中调整期，推动量子安全从可选方案转变为必选项。

在金融、电信、能源等高监管行业，这一趋势表现得尤为明显。2025年，这些行业的量子安全投入不再以试点或专项验证为主，而是逐步纳入年度IT和安全预算，其决策逻辑更接近常规基础设施更新，而非前沿技术试验。量子安全开始被视为保障系统长期稳定运行和合规连续性的基础能力。

随着需求特征的变化，**市场结构也在同步调整。**用户更倾向于选择能够嵌入既有架构、支持分阶段部署、并具备长期运维与合规支撑能力的解决方案提供方，而非仅提供单点技术的厂商。量子安全市场正在呈现出与成熟网络安全行业相似的特征：需求连续、替换周期较长，服务和交付属性不断增强。

总体来看，随着合规要求逐步扩展至更多行业和业务系统，**量子安全市场仍将保持稳健增长。**但未来的增量空间，将更多向工程能力成熟、交付路径清晰、能够长期支持客户完成迁移的企业集中，而非依赖单一技术突破的参与者。

03 抗量子迁移进入以合规要求为核心的实施阶段

2025年成为抗量子迁移由规划阶段转向实际推进的重要节点，其主要触发因素来自合规要求的明确化和可执行化。对企业而言，应对量子风险已不再停留在政策表述或技术评估层面，而是需要形成清晰的迁移路径，并在合规检查和审计过程中体现出实质性进展。

在具体实施中，迁移工作的第一步往往并非算法替换，而是对现有加密资产的系统性梳理。许多机构在盘点过程中首次全面识别自身系统中使用的算法类型、证书体系、密钥管理方式以及第三方组件依赖，进而发现潜在风险并不集中于核心业务系统，而更多分布在接口层、遗留系统和外包模块中。这一发现使迁移策略趋于理性，更强调分层推进和对业务连续性的保护。

合规压力也在改变企业的技术决策方式。与其追求一次性完成替换，越来越多的组织开始优先选择具备密码敏捷性的架构，使系统能够在算法、标准或监管要求变化时保持调整空间。抗量子迁移因此逐步融入日常IT治理流程，成为一项持续演进的基础性工作，而非独立的技术改造项目。

从中长期来看，抗量子迁移将以持续实施的方式推进，其效果并不取决于单次技术选型，而取决于组织是否建立起可长期维护、可审计、可演进的密码治理能力。这一能力将成为衡量企业量子安全成熟度的重要标志。

04 混合加密成为网络基础设施的主流配置

在网络基础设施层面，2025年逐步形成了一项工程共识：**混合密钥交换是当前条件下最具可行性的实施路径。**这一共识并非源于单一标准判断，而是来自标准推进与大规模实际部署的共同验证。

从技术实现看，无论是IETF正在推进的相关标准草案，还是主流浏览器和云服务平台的落地方案，都已采用经典算法与抗量子算法并行的密钥协商机制。Cloudflare已在其全球网络中支持基于TLS 1.3的混合密钥交换，将传统椭圆曲线算法如X25519与抗量子密钥封装机制（例如ML-KEM-768）组合用于会话密钥协商。这一混合模式正逐步得到更广泛部署，帮助现有协议在保持兼容性的同时提升抗量子计算攻击的能力。

实际运行数据进一步印证了这一路径的可行性。根据Cloudflare在2025年3月公开披露的信息，在其全球网络中，约38%的HTTPS连接已经成功协商并使用包含抗量子算法的混合TLS配置。

未来，**混合加密将作为网络层的默认配置持续存在**，这种渐进式引入的方式，为抗量子迁移争取了宝贵的时间窗口，也为基础设施的长期演进提供了现实路径。

05 交付能力成为核心变量，量子安全竞争重心发生转移

随着量子安全逐步进入制度约束明确、工程路径可验证的阶段，产业竞争的核心正在发生变化。技术本身是否可用已不再是主要分水岭，取而代之的是解决方案能否被稳定交付、持续运行并长期维护。

在这一背景下，量子安全不再以单项技术或独立产品的形式被评估，而是被置于更完整的系统环境中加以审视。用户关注的重点逐步转向解决方案是否具备清晰的部署路径、是否能够与既有系统平滑衔接，以及在合规审查、运维管理和后续演进中是否具备可持续性。这一变化使量子安全从技术引入问题转变为工程与管理问题。

产业实践表明，能够获得持续采用的方案，往往并不依赖某一项技术指标的领先，而是依托对复杂系统的整体理解能力。例如，对现有加密资产的梳理能力、对业务连续性的保障能力、对监管要求的响应能力，正在成为影响方案选择的重要因素。这些能力本质上属于工程交付与长期服务范畴，而非单纯的技术研发成果。

交付方式本身也在发生变化。量子安全解决方案开始更多以平台化、服务化的形态出现，与传统网络安全产品在采购、部署和运维逻辑上逐步趋同。这种变化降低了用户采用门槛，也使量子安全更容易被纳入常规的IT和安全治理体系之中。

总体来看，量子安全产业正在从以技术路线和产品形态为核心的早期竞争，转向以工程能力、交付可靠性和长期服务能力为核心的竞争阶段。谁能够持续陪伴用户完成迁移、运行和演进，正在成为决定产业位置的关键因素。

06 地缘政治格局固化，形成中美欧三大技术阵营

量子安全的发展正越来越明显地受到地缘政治因素影响，并逐步呈现出区域分化的格局。不同国家和地区在安全诉求、产业基础和制度环境上的差异，正在塑造各自相对独立的发展路径。

从整体方向看，美国更侧重通过软件生态和技术标准推动量子安全能力的扩散，将抗量子密码融入操作系统、云平台和互联网协议体系；中国则重点投入通信基础设施建设，围绕城域网、骨干网以及空天地一体化网络，推进量子通信与量子安全的工程化落地；欧洲则主要依托监管框架和合规机制，明确量子安全的应用边界和实施节奏，引导成员国在统一规则下推进部署。

这种差异已在实际推进中逐步显现。美国主导的NIST抗量子密码标准，正在成为全球范围内抗量子密码工程实现的重要技术依据；中国持续扩大量子通信网络规模，形成以基础设施为核心的安全能力布局；欧盟则通过DORA、EuroQCI等制度安排，将量子安全纳入统一监管体系和跨国网络建设规划之中，强调规则、工程和运维的协同推进。

对跨国企业而言，这种区域差异带来了更高的现实复杂度。技术选型、合规路径和供应链安排往往需要根据不同地区分别设计，单一方案同时覆盖多个区域的可行性持续下降。相应地，区域化部署、模块化系统设计以及多版本并行运行，正在成为更具现实意义的选择。

可以预期，在可见的时间范围内，这种区域分化格局难以发生根本改变。量子安全将更加紧密地与数字主权和关键基础设施安全绑定，其技术路线和产业形态也将长期受到国际政治环境和制度差异的影响。

07 多量子技术融合成为长期趋势

随着量子技术走向工程化部署，一个日益清晰的趋势正在形成：量子安全、量子计算和量子传感正在共享越来越多的底层工程体系。这种融合并非简单的技术叠加，而是由器件共用、系统协同和运维现实需求共同推动的结果。

在底层器件与工艺层面，多数量子技术正依赖相同或高度相似的关键组件体系。

高性能单光子探测器、量子随机数源、超低噪声光学器件以及高精度时间同步系统，既是量子安全系统稳定运行的基础，也是量子计算读出和量子传感精度提升的重要支撑。随着这些核心器件逐步实现工程化成熟和规模化生产，其应用不再局限于单一技术方向，而是自然向多个量子应用场景延展，推动不同量子技术在硬件与制造层面形成交集。

在系统与网络层面，这种融合更多体现为网络化与基础设施化的发展趋势。

量子安全网络在建设过程中积累的大量工程经验——包括光纤与自由空间链路管理、网络调度机制、密钥与控制平面分离设计等——正被用于支持分布式量子计算节点的安全互联，以及远程量子传感数据的可信回传。与此同时，量子计算和量子传感对高精度控制、低时延反馈和高可靠运行的要求，也反向推动量子安全系统在稳定性、可运维性和规模扩展能力上的持续提升。

在应用模式与产业形态层面，多量子技术的融合正在重塑对量子能力的整体认知。

量子技术不再以孤立设备或单一系统的形式存在，而是逐步被视为可组合、可调用的基础能力模块。在高安全计算、国防监测、能源系统和空间应用等场景中，量子传感负责获取高精度物理信息，量子安全保障数据与链路的可信传输，量子计算则用于复杂建模与分析，三者形成分工清晰但高度耦合的技术体系。

从长期看，这种融合趋势将进一步强化量子技术的基础设施属性。

产业竞争的重心也将随之转移：不再单纯比较某一技术指标的领先程度，而是更关注谁能够构建稳定、可扩展、可跨场景复用的底层工程体系。多量子技术的协同演进，将成为量子安全乃至更广泛量子产业持续发展的内在结构，而非短期的技术组合或概念叠加。

08 “量子+”加速落地，量子安全嵌入数字基础设施

2025年以后，量子安全的落地方式正在发生根本变化。与其作为独立系统部署，不如作为能力嵌入既有数字基础设施，这已成为行业共识。

在具体实践中，抗量子密码更多承担的是大范围、低门槛的升级任务，通过软件和协议层改造，为现有系统提供面向未来的基础防护；而量子密钥分发、量子随机数等能力，则被部署在数据中心互联、运营商骨干网和关键边缘节点等安全价值密度更高的位置。两类技术以不同层级进入系统，在尽量不改变业务流程的前提下，逐步抬升整体安全水平。

来自金融、电信、云计算等行业的经验表明，量子安全是否能够持续落地，关键并不在于技术本身的复杂程度，而在于是否具备良好的集成性、可运维性和可审计性。这也直接推动了交付方式的变化：量子安全越来越多以服务化、平台化的形式出现，被纳入现有安全体系和运维框架之中，而非作为额外负担存在。

可以预见，量子安全将逐步演变为数字基础设施的内生能力，而“**量子+**”**将成为其最现实、也最可持续的落地路径。**

10

附件

目录 10 附件

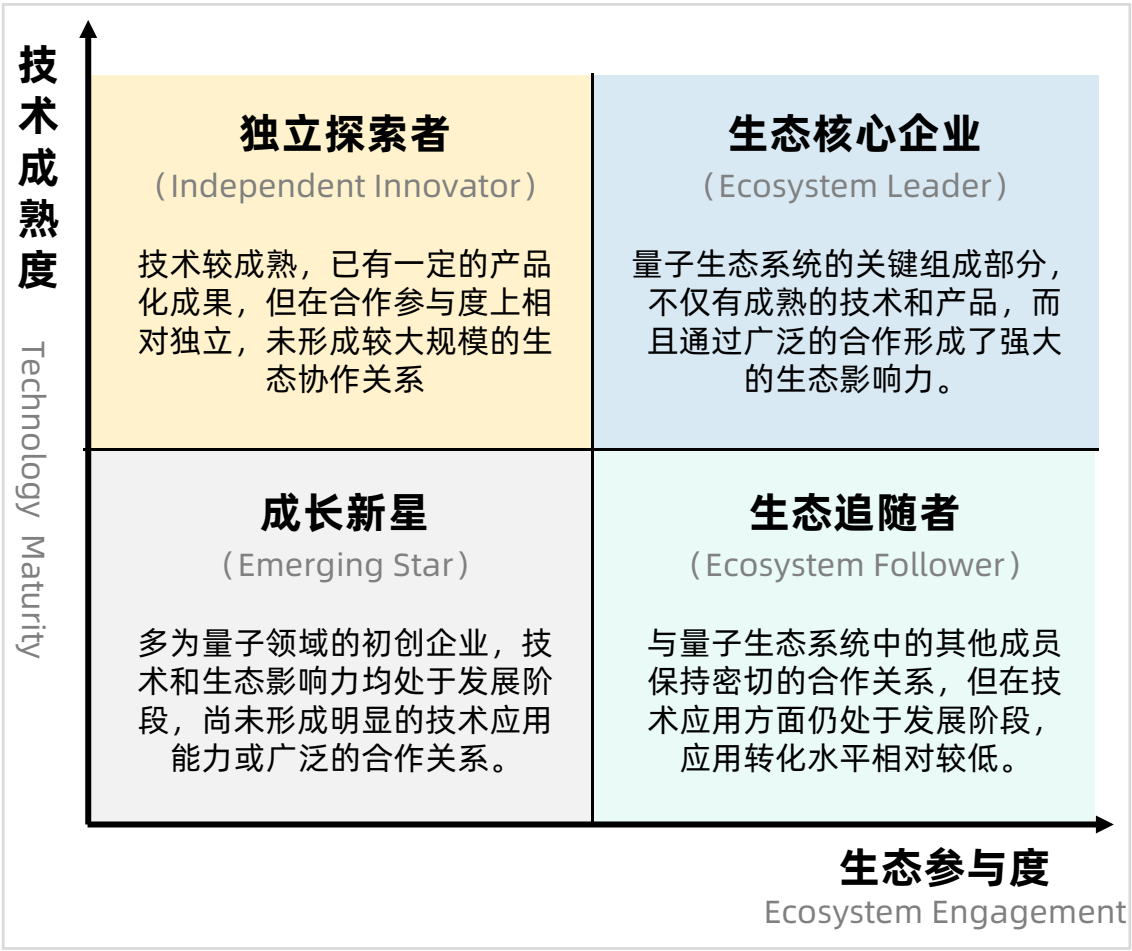
01 量子生态成熟度罗盘（Q-EMC）

02 参考链接

01 量子生态成熟度罗盘（Q-EMC）

本报告提出一个二维矩阵评价模型，该模型通过技术成熟度（纵轴）和生态参与度（横轴）两个维度，系统性评估量子计算领域参与者（企业、研究机构或技术路线）的综合竞争力，揭示其技术能力与生态整合能力的动态平衡关系。

图表 量子生态成熟度罗盘（Q-EMC）



iCV TA&K & 光子盒研究院 QUANTUMCHINA | 2026.2

模型详解

横轴：生态参与度

衡量公司在量子生态系统中的合作深度和广度。高生态参与度的公司通常与其他企业、高校、研究机构甚至政府有广泛合作，积极融入产业生态，并善于整合资源、形成协作网络。低生态参与度的公司则多倾向于独立运作，或由于处于早期发展阶段而缺乏大范围合作关系。

纵轴：技术成熟度

反映公司在量子技术方面的成熟程度，包括其核心技术的研发深度、可靠性和稳定性。这一维度评估公司在技术积累上的深厚程度，以及其量子技术是否具备标准化和可扩展性。高技术成熟度的公司通常具有经过验证的技术能力，能够提供高质量的产品或服务，并为进一步的应用转化和市场化奠定坚实基础。

模型应用

- 独立探索者：可以考虑增加生态合作，借助外部资源进一步推动技术应用；
- 生态核心企业：可通过技术突破和扩展合作网络，巩固核心地位；
- 生态追随者：可以重点提升技术及其应用能力，以增强自身市场竞争力；
- 成长新星：可以选择重点发展技术应用或增加生态合作，尽快找到合适的切入点以提升市场影响力。

在《2026全球量子安全产业发展展望》报告中。技术成熟度具体权重指标包括量子安全技术（量子密钥分发、量子随机数生成以及其他技术）、量子安全设备性能指标（密钥生成速率、误码率、安全传输距离、成码率等）、知识产权、2025年技术进展等；生态参与度具体权重指标包括2025年合作进展情况、标准制定情况、联盟情况等。

02 参考链接

https://mattermost.com/newsroom/press-releases/mattermost-and-qrypt-announce-joint-solution-for-quantum-secure-communications-in-defense-and-intelligence-applications/?utm_source
https://www.qrypt.com/resources/q1-2025-a-tipping-point-for-quantum-security/
https://www.thejakartapost.com/adv/2025/08/28/itsec-asia-qrypt-join-forces-to-bring-quantum-safe-security-to-indonesia.
https://pqsecurity.com/pqsecure-joins-nist-nccoe-pqc-consortium-as-a-technology-partner/
https://pqsecurity.com/pqsecure-achieves-nist-cavp-validation/
https://pqsecurity.com/pqsecure-collaborates-with-menta-to-advance-post-quantum-cryptographic-ip-on-efpga/
https://pqsecurity.com/pcsecure-and-fau-unveil-groundbreaking-research-on-post-quantum-cryptography-vulnerabilities/
https://pqsecurity.com/pqsecure-joins-the-pki-consortium/
https://www.qusecure.com/the-latest-news-from-qusecure-early-february-2025/
https://www.qusecure.com/category/press-releases/
https://www.sandboxaq.com/press/sandboxaq-achieves-fedramp-ready-status-powering-enterprise-readiness-across-the-defense-and-public-sector
https://www.sandboxaq.com/press/sandboxaq-and-dow-cio-partner-to-strengthen-us-defenses-against-quantum-and-ai-driven-cyber-threats
https://www.sandboxaq.com/press/sandboxaq-unveils-opencryptography-com-the-first-public-database-exposing-cryptographic-risks-in-open-source-software
https://www.prnewswire.com/news-releases/sandboxaq-and-ey-us-extend-strategic-alliance-to-accelerate-adoption-of-advanced-cryptographic-and-ai-security-solutions-302521937.html
https://www.keyfactor.com/blog/ready-for-lift-off-explore-pqc-pki-and-signing-in-our-new-test-drive-environment/
https://www.keyfactor.com/blog/ready-for-lift-off-explore-pqc-pki-and-signing-in-our-new-test-drive-environment/
https://www.keyfactor.com/press-releases/keyfactor-joins-f5-adsp-partner-program-to-streamline-certificate-management-and-strengthen-application-security/
https://www.keyfactor.com/press-releases/keyfactor-finds-nearly-half-of-enterprises-unprepared-for-quantum-cybersecurity-threats/
https://www.businesswire.com/news/home/20250811313526/en/Keyfactor-Named-to-2025-Inc.-5000-List-Amid-Rising-Demand-for-Quantum-Ready-Security-Solutions
https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-delivers-enterprise-wide-quantum-security-readiness-for-all-customers
https://www.qticompany.com/qti-atecoc2025/
https://www.qticompany.com/qti-to-lead-the-development-of-quantum-repeaters-a-new-era-for-long-distance-quantum-networks/
https://www.qticompany.com/qti-at-mobile-world-congress-2025-showcasing-quantum-solutions-for-the-telco-industry/
https://thequantuminsider.com/2025/09/25/quantum-optics-jena-secures-independent-certification-milestone-for-quantum-communications/
https://www.luxquanta.com/luxquanta-launches-second-generation-of-qkd-system-nova-lq-at-mwc-2025-n-73-en
https://www.luxquanta.com/luxquanta-demonstrates-quantum-safe-solutions-between-data-centers-and-aws-n-79-en
https://www.luxquanta.com/luxquanta-secures-8-million-in-series-funding-to-accelerate-global-deployment-of-quantum-safe-cybersecurity-solutions-n-83-en
https://www.luxquanta.com/quantum-safe-networks-in-action-at-aws-singapore-innovation-hub-n-84-en

02 参考链接

https://www.idquantique.com/integrating-solutions-idq-ionq-cisco/
https://www.idquantique.com/genevas-first-quantum-communication-network/
https://www.quantum-dice.com/news/
https://pqshield.com/pqshield-and-carahsoft-partner-to-make-powerful-post-quantum-cryptography-solutions-available-to-government-agencies/
https://pqshield.com/pqcryptolib-core-v1-0-2-achieves-cavp-certification-for-a-broad-set-of-classical-and-post-quantum-algorithms/
https://q-bird.com/press/qbird-secures-e2-5m-grant-and-e5m-equity-from-eic-accelerator-to-scale-europes-quantum-secure-networks/
https://q-bird.com/press/redefining-quantum-network-management-with-the-launch-of-qbird-quantum-domain-controller-qdc/
https://q-bird.com/press/fortifying-europes-quantum-communication-qbird-and-beqci-achieve-the-first-cross-border-mdi-qkd-link-in-benelux/
https://www.thalesgroup.com/en/news-centre/press-releases/thales-launches-its-post-quantum-mistral-encryptor-ready-secure
https://www.thalesgroup.com/en/news-centre/press-releases/thales-launches-its-post-quantum-mistral-encryptor-ready-secure
https://www.thalesgroup.com/en/news-centre/press-releases/thales-launches-its-post-quantum-mistral-encryptor-ready-secure
https://www.thalesgroup.com/en/news-centre/press-releases/thales-alenia-space-and-hispasat-start-development-worlds-first-quantum
https://xiphera.com/xipheras-2025-retrospective-by-the-ceo/
https://digitalisationworld.com/news/70026/xiphera-contributes-to-strengthening-finlands-quantum-safe-security
https://www.ssh.com/ssh-communications-security-launches-quantum-resilient-network-encryptor-release-nqx-3.1-with-breakthrough-post-quantum-encryption-capabilities
https://www.quintessencelabs.com/news
https://www.asc-csa.gc.ca/eng/news/articles/2025/2025-01-20-csa-awards-over-1-million-for-quantum-technology-demonstration.asp
https://www.asc-csa.gc.ca/eng/satellites/qeyssat.asp
https://thequantuminsider.com/2025/05/27/quantum-emotion-finalizes-qrng-hybrid-chip-design-commences-manufacturing-with-tsmc/
https://www.quantumemotion.com/press-release/20/quantum-emotion-and-jmem-technology-join-forces-to-deliver-the-first-ever-full-stack-quantum-resilie
https://quantumzeitgeist.com/quantum-emotion-engages-lightship-security-for-nist-fips-140-3/
https://crypto4a.com/resources/newsroom
https://www.quantropi.com/tag/quantum-secure/
https://www.prnewswire.com/news-releases/infosec-global-federals-agilesec-analytics-achieves-fedramp-authorization-on-the-cgc-platform-302522636.html
https://www.qnulabs.com/case-studies
https://thequantuminsider.com/2025/12/09/quantum-corridor-toshiba-demonstrate-cross-state-quantum-key-distribution-over-live-commercial-metro-fiber-network/
https://newsroom.orange.com/orange-business-and-toshiba-partner-to-launch-first-commercial-quantum-safe-network-service-in-france/
https://www.global.toshiba/ww/news/digitalsolution/2025/03/news-20250326-01.html

02 参考链接

https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline
https://www.cas.cn/cm/202504/t20250409_5061927.shtml
https://www.nature.com/articles/s41534-025-01009-w
https://opg.optica.org/oe/fulltext.cfm?uri=oe-33-10-20258&id=570887
https://journals.aps.org/prx/abstract/10.1103/PhysRevX.15.021037
https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.23.054022
https://journals.aps.org/prx/abstract/10.1103/PhysRevX.15.021066
https://biz.chosun.com/en/en-science/2025/07/30/2O3KWQZFFZH5NEUBIZKO2MC4NI/
https://www.packetlight.com/about/press-releases/packetlight-nec-demonstrate-400g-qkd
https://www.nature.com/articles/s41534-025-01052-7
https://journals.aps.org/prxquantum/abstract/10.1103/7fdd-m92n
https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption
https://www.nature.com/articles/s41586-025-08704-w
https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.23.034040
https://www.nature.com/articles/s41586-025-08739-z
https://www.gov.pl/web/obrona-narodowa/kwantowa-dystrybucja-kluczy-to-przelom-w-bezpieczenstwie-komunikacji-podmiotow-panstwa
https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
https://www.colt.net/resources/colt-completes-quantum-secured-encryption-trial-across-optical-network/
https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.23.034057
https://www.nokia.com/about-us/news/releases/2025/03/24/nokia-and-honeywell-aerospace-technologies-partner-with-numana-to-advance-quantum-safe-networks/
https://www.cohesity.com/blogs/cohesity-netbackup-11-0-protecting-data-from-the-cyber-threats-of-today-and-tomorrow/
https://www.etsi.org/newsroom/press-releases/2513-etsi-launches-new-standard-for-quantum-safe-hybrid-key-exchanges-to-secure-future-post-quantum-encryption
https://www.nature.com/articles/s41534-025-01009-w
https://www.unisys.com/news-release/unisys-launches-first-post-quantum-cryptography-service-to-block-future-security-threats/
https://journals.aps.org/prresearch/abstract/10.1103/PhysRevResearch.7.023199
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.134.210801
https://www.nature.com/articles/s41534-025-01059-0
https://journals.aps.org/prapplied/abstract/10.1103/368v-t34p
https://journals.aps.org/prl/abstract/10.1103/d53g-v8q6
https://www.nature.com/articles/s41377-025-01920-z
https://journals.aps.org/prapplied/abstract/10.1103/sx7r-1npt
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.134.220801
https://www.commvault.com/news/commvault-unveils-new-post-quantum-cryptography-capabilities-to-help-customers-protect-data-from-a-new-generation-of-security-threats
https://www.nature.com/articles/s41534-025-01052-7
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.134.230801
https://www.nature.com/articles/s41598-025-20273-6
https://journals.aps.org/prapplied/abstract/10.1103/ywz1-gqzg
https://journals.aps.org/prl/abstract/10.1103/zy2d-m3ch
https://journals.aps.org/prl/abstract/10.1103/cn3m-j743
https://journals.aps.org/prresearch/abstract/10.1103/84qz-1jz2
https://journals.aps.org/prapplied/abstract/10.1103/5c5v-cw8c
https://journals.aps.org/prapplied/abstract/10.1103/hc3f-3pbw
https://journals.aps.org/prapplied/abstract/10.1103/f92x-c3zj
https://www.nature.com/articles/s41377-025-02039-x
https://www.nature.com/articles/s41566-025-01792-0

02 参考链接

https://www.nature.com/articles/s41598-025-14226-2
https://journals.aps.org/prapplied/abstract/10.1103/njjw-ttqn
https://journals.aps.org/prxquantum/abstract/10.1103/7fdd-m92n
https://www.nature.com/articles/s42005-025-02258-z
https://www.nature.com/articles/s41598-025-13508-z
https://journals.aps.org/prapplied/abstract/10.1103/xlmc-x4xg
https://journals.aps.org/prapplied/abstract/10.1103/xq2l-r4r7
https://www.nature.com/articles/s41567-025-03022-4
https://www.science.org/doi/10.1126/sciadv.adx4180
https://investors.rigetti.com/news-releases/news-release-details/rigetti-collaboration-qphox-awarded-58m-afrl-contract-advance
https://ionq.com/news/ionq-achieves-significant-quantum-internet-milestone-demonstrates-quantum
https://www.nature.com/articles/s41598-025-17184-x
https://www.nature.com/articles/s41534-025-01100-2
https://journals.aps.org/prl/abstract/10.1103/7wrk-p6gl
https://journals.aps.org/prapplied/abstract/10.1103/q23p-l2z7
https://www.science.org/doi/10.1126/sciadv.adu8455
https://journals.aps.org/prxquantum/abstract/10.1103/j8mt-c124
https://journals.aps.org/prresearch/abstract/10.1103/v3p1-kz4h
https://www.nature.com/articles/s41598-025-91161-2
https://www.nature.com/articles/s42005-025-02317-5
https://journals.aps.org/prapplied/abstract/10.1103/zw9s-ywd6
https://www.nature.com/articles/s41598-025-20146-y
https://news.samsung.com/global/samsung-introduces-future-ready-mobile-security-for-personalized-ai-experiences
https://www.businesswire.com/news/home/20250710847121/en/Pateros-Post-Quantum-Encryption-Secures-Syllegos-DUST-Platform-to-Enhance-Smart-City-Cybersecurity
https://ionq.com/news/ionq-completes-acquisition-of-capella-space-advancing-vision-for-space-based
https://quantumcomputinginc.com/news/press-releases/quantum-computing-inc.-secures-purchase-order-from-top-5-u.s.-bank-to-advance-quantum-cybersecurity-testbed
https://www.forescout.com/blog/post-quantum-cryptography-the-real-risks-of-not-adopting-it/
https://www.sealsq.com/investors/news-releases/sealsq-commits-up-to-30-million-in-cryptocurrency-treasury-to-accelerate-post-quantum-cryptography-initiatives
https://www.btq.com/blog/introducing-leonne-topological-consensus-networks-for-scalable-blockchain-security
https://www.carahsoft.com/news/torq-and-carahsoft-partner-to-transform-public-sector-security-operations-through-hyperautomation-2025
https://www.globenewswire.com/news-release/2025/06/09/3095906/0/en/SEALSQ-and-WISeKey-Unveil-Quantum-Resilient-Security-Framework-to-Control-the-Future-of-Robotics.html
https://support.apple.com/en-us/122756
https://www.orange-business.com/en/press/orange-business-toshiba-partner-launch-first-commercial-quantum-safe-network-service-france
https://www.linkedin.com/posts/al-moammar-information-systems_mis-al-moammar-information-systems-co-activity-7341105989523304448-0Fgw
https://biz.chosun.com/en/en-it/2025/06/23/GAMG2GUE6VC5VNM7C63TZVNUYQ/
https://www.globenewswire.com/news-release/2025/06/23/3103896/0/en/WISeSat-Space-and-SEALSQ-Launch-New-Satellite-with-SpaceX-Enabling-the-First-Ever-DePIN-from-Space-and-Advancing-Quantum-Safe-Space-Communications.html

02 参考链接

https://www.binarly.io/news/binarly-partners-with-qusecure-to-accelerate-enterprise-post-quantum-readiness
https://www.nature.com/articles/s41534-025-01085-y
https://www.nature.com/articles/s41534-025-01089-8
https://www.nature.com/articles/s41534-025-01088-9
https://mp.weixin.qq.com/s/vHLURpSGUQds-Ph3Jjk1Uw
https://www.prnewswire.com/news-releases/btq-technologies-to-develop-worlds-first-quantum-secure-custody-treasury-for-bitcoin-ethereum-and-other-digital-assets-in-collaboration-with-qbits-302521695.html
https://www.businesswire.com/news/home/20250812227102/en/OPTIA-and-Patero-Launch-Industrys-First-Post-Quantum-Enabled-GPU-Compute-Platform-for-Defense-and-Edge-Applications
https://thequantuminsider.com/2025/08/13/itti-becomes-latam-distributor-of-signquantums-quantum-proof-e-signature-tech/
https://www.wdtn.com/business/press-releases/ein-presswire/839847113/interlynk-launches-post-quantum-cryptography-compliance-capabilities-to-its-sbom-platform/
https://www.paloaltonetworks.com/blog/2025/08/securing-the-quantum-age/
https://mp.weixin.qq.com/s/IkQ2BUALWdSUenQlP-DGIA
https://www.iitm.ac.in/happenings/press-releases-and-coverages/iit-madras-signs-rs-1-crore-deal-license-indias-first
https://www.microsoft.com/en-us/security/blog/2025/08/20/quantum-safe-security-progress-towards-next-generation-cryptography/
https://www.adgm.com/media/announcements/adgm-and-adgm-academy-team-up-with-tii-hub71-and-aspire-to-launch-uaes-first-quantum-secure-communications-testbed
https://www.sealsq.com/investors/news-releases/sealsq-and-ajyal-holding-launch-the-kuaentum-joint-venture-in-abu-dhabi-with-a-100-million-local-investment-target
https://photonic.com/news/photonic-dnd-ideas-announcement-august-2025/
https://gzw.sc.gov.cn/scsgzw/CU23020301/2025/8/6/42d7b1bc38c845519b3fbf7dfaf68ce4.shtml
https://www.cnenergynews.cn/dianwang/2025/09/09/detail_20250909232407.html
https://www.qunnect.inc/press-release-2025-09-09
https://www.ciena.com/about/newsroom/press-releases/redimadrid-launches-end-to-end-quantum-secure-data-transport-project-with-ciena
https://chicagoquantum.org/news/networking-infrastructure-company-belden-joins-chicago-quantum-exchange-drive-innovation
https://www.bsa.org/news-events/news/bsa-launches-quantum-policy-agenda
https://www.sealsq.com/investors/news-releases/sealsq-to-secure-space-transactions-with-post-quantum-technology-to-support-the-next-wisesat-launch-scheduled-for-november-2025
https://arqitgroup.com/resources/press-release/ncsc-post-quantum-cryptography-migration
https://aerospace.honeywell.com/us/en/about-us/press-release/2025/09/honeywell-redwire-quantum-secure-communications
https://quantumcomputingreport.com/aliro-software-supports-over-50-quantum-network-devices-advancing-scalable-quantum-internet/
https://www.xiaopeng.com/news/company_news/5505.html
https://www.superq.co/news/superq-quantum-releases-post-quantum-cryptography-pqc-ai
https://www.etsi.org/newsroom/press-releases/2594-etsi-creates-new-committee-on-quantum-technologies

ICV TA&K
Technology Advisory
& Knowledgebase

ICV TA&K（全称 (Technology Advisory & Knowledgebase)，中文常译为“智能与知识智库”或“ICV 前沿科技咨询”）已成为定义未来产业标准与评估体系的领军机构。

1. 机构定义：未来产业的“导航者”与“评估者”

ICV TA&K 是一家专门从事前沿技术（Frontier Tech）战略咨询、市场研究及产业评价的国际化智库。不同于传统的会计师事务所或通用型咨询公司，ICV 的核心基因在于“技术深度”。目前已将业务触角延伸至量子信息、具身智能、生物制造、低空经济、6G 通信以及脑科学等九大关键颠覆性领域。它被公认为全球“未来产业”布局的风向标，为各国政府制定产业政策及财富 500 强企业进行战略投资提供底层数据支持。

2. 核心竞争力：Q-EMC多维指标评价体系

ICV 公司最显著的贡献在于其自主研发的**Q-EMC**核心技术评估模型。这套模型不仅是您所使用的全球城市排名的基础，也是衡量一家企业或一个地区“未来竞争力”的国际标准。

数据驱动： ICV 整合了包括 WIPO（世界知识产权组织）、OECD、IEEE 以及全球主流高性能计算中心（HPC）的实时数据，确保每一份排名和指数（如 2025 全球未来城市排名）都具备严谨的科学依据和行业公信力。

3. 业务版图：从“前沿智库”到“战略加速器”

ICV 的业务模式分为三大板块，构成了其完整的知识生态系统：

前沿智库： 每年发布超过 50 份深度的全球行业报告，涵盖从量子芯片制程路线图到 L5 自动驾驶责任法典等关键课题。

战略咨询与评估： 协助波音、特斯拉、丰田等巨头在全球范围内进行供应链韧性评估，并为新加坡、北京、旧金山等城市的智慧城市建设提供顶层设计建议。

金融情报服务： 针对风险投资（VC）和私募股权（PE），ICV 专门设立了“量子独角兽”与“具身智能明星”追踪系统，通过分析初创企业的技术专利护城河（Filing Strength）来预测其商业潜能。

我们在最广泛的资本密集型行业和市场中汇集了最深入的情报。通过连接不同变量的数据，我们的分析师和行业专家为我们的客户提供了一个更丰富、高度整合的世界观。

光子盒研究院是一家专注于前沿科技与未来产业发展的创新型研究机构，以"探索科技边界、赋能产业升级"为使命，致力于成为全球科技创新生态系统中不可或缺的智库力量。研究院以前沿技术演进为观察坐标，以量子科技为核心研究领域，深度布局人工智能、先进计算、未来材料等战略方向，构建起"技术前瞻-产业应用-政策研究"三位一体的研究体系。

【核心定位与研究领域】

作为量子科技领域的专业研究平台，研究院聚焦量子计算、量子通信、量子传感三大技术主航道，持续跟踪全球量子科技关键技术突破。通过建立覆盖"基础研究-技术转化-产业应用"的全链条分析框架，研究院定期发布量子计算硬件发展路线图、量子安全通信应用白皮书等权威报告，为行业提供具有前瞻性的技术评估与产业化路径建议。

【智库服务与价值创造】

研究院构建了独特的"产学研政资"协同创新网络，为政府部门提供科技创新政策制定咨询，协助构建量子科技产业园区规划；为科研机构搭建技术转化评估模型，推动实验室成果与产业需求对接；为企业客户定制技术路线选择、市场竞争策略及专利布局方案；为投资机构建立科技项目价值评估体系，甄别具有突破潜力的早期技术项目。目前已形成季度产业研究报告、年度技术趋势预测、专项政策建议书等系列知识产品。

【研究特色与竞争优势】

依托跨学科研究团队（涵盖物理学、计算机科学、产业经济学等领域专家），研究院创新性采用"技术成熟度曲线+产业生态图谱"双维分析法，结合专利大数据挖掘与全球科研动态监测，确保研究成果的客观性与时效性。通过建立量子科技企业数据库（覆盖全球600+相关机构）、搭建院士专家委员会、主办国际量子产业峰会等举措，持续强化在量子科技领域的资源整合能力与行业影响力。

光子盒研究院始终秉持"以科技洞见未来"的核心理念，通过深度行业洞察、精准趋势研判和务实解决方案，助力客户把握量子革命带来的战略机遇。在科技创新加速重构全球产业格局的当下，研究院将持续输出具有决策价值的智库成果，推动前沿科技与实体经济的深度融合，为人类科技文明进步贡献智慧力量。

2026 全球量子安全产业发展展望

Q-STAR

联系我们

iCV TA&K
Technology Advisory
& Knowledgebase

Canada

5250 Fairwind Dr.
Mississauga, Ontario,
L5R 3H4,
Canada

Singapore

101 Upper Cross Street,
#04-17,
People's Park Centre,
Singapore

infer@icvtank.com

https://www.icvtank.com/

光子盒研究院
QUANTUMCHINA

扫一扫
关注光子盒

扫一扫
咨询研究员

网址：https://www.quantumchina.com/

总部：北京市海淀区信息路26号中关村创业大厦7层701

分部：上海市长宁区仙霞路317号远东国际广场B栋613

分部:成都市高新区天府软件园G区G1栋803