光子盒研究院
QUANTUMCHINA

2025

全球量子安全产业发展展望



2025/02

量子科技年度系列报告

序言

融合赋能 产业新程

随着量子科技的快速发展，量子安全成为了全球技术和产业竞赛中的关键领域。量子密钥分发（QKD）和抗量子密码学（PQC）作为量子安全的两大支柱，各自具备不同的技术优势和应用前景。但在未来，随着技术进步和产业需求的不断变化，量子安全的产业模式将发生深刻的转型。未来的量子安全生态，将可能涵盖全量子密钥分发、全抗量子密码、量子密钥分发与抗量子密码共存等几种模式，而这一切的变化都与各国不同的技术发展策略和安全需求紧密相关。

从全球产业趋势来看，量子安全的技术选择与国家的战略目标、产业基础以及技术发展阶段密切关联。中国的战略定位明确，正处于从量子密钥分发向抗量子密码过渡的关键时期，致力于逐步在量子密钥分发技术上取得领先的同时，开始在抗量子密码学领域加大研发投入，形成技术体系的双轮驱动。而美国的技术路线则更加侧重于抗量子密码学的直接部署，其基于抗量子密码的技术架构，在全球范围内已逐步商用化，为应对量子计算带来的安全威胁提供前瞻性的解决方案。欧盟则采取了一种折中的方式，主张量子密钥分发与抗量子密码并行发展，力求在量子通信的基础设施建设与抗量子密码算法的应用上同步推进，确保在全球量子安全格局中的竞争力。

因此，未来全球量子安全的格局，极有可能呈现一种多元化发展趋势。在这一过程中，各国将根据其技术积累、产业基础、国家安全需求和国际竞争格局，选择适合的技术路径。在这一过程中，量子密钥分发和抗量子密码可能并非完全对立，而是呈现出相互补充、相辅相成的局面。比如，在量子通信网络中，量子密钥分发可以提供核心的量子安全保障，而抗量子密码则可在传统的互联网和现有网络架构中提供量子计算安全防护，形成协同防护效应。

本报告旨在全面分析当前量子安全领域的发展动态，探索量子密钥分发和抗量子密码学技术的结合前景，深入剖析各国在量子安全领域的技术路线选择与产业布局，展望未来全球量子安全的格局演变，并提出相应的产业发展建议。

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2024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2024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2024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（2025全球量子安全产业发展展望[R].光子盒研究院.2025.02）。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，使用本报告内容时，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，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，需在允许范围内。违规使用本报告者，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，不够成投资建议，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应用，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发布。

感谢包括但不限于以下公司给予技术和素材的支持：

IDQ
ARQIT
QMill
中电信量子集团 CHINA TELECOM QUANTUM GROUP
国盾量子 QuantumCTek
Q*bird quantum connectivity
SEALSQ semiconductors + quantum
QuSecure
QUANTUMXCHANGE
SK telecom
硅臻 SILICON EXTREME
问天量子
QUDOOR 启科量子
SPEQTRAL
BT
Qrypt
quantum emotion
PQSHIELD
TOSHIBA
循态量子 XT Quantech
QUANTUM DICE

目录

1. 2024产业发展概览 7

2. 量子保密通信 17

3. 抗量子密码 63

4. 全球主要国家现状与分析 90

5. 投融资分析 104

6. 供应商评价 112

7. 产业分析预测 144

8. 产业展望 153

9. 附件 166

研究对象

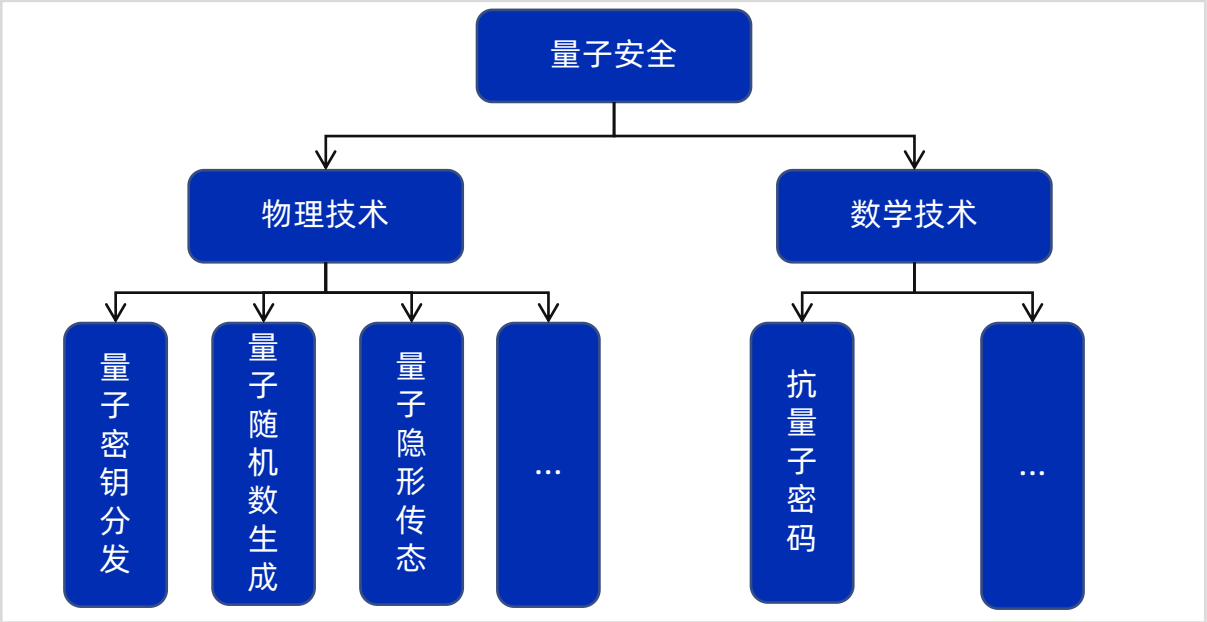
本研究报告的研究对象是量子安全产业，量子安全产业（Quantum-Safe Industry）是指为应对量子计算机对传统密码体系构成的威胁，围绕量子通信技术（如量子密钥分发，QKD）和抗量子密码技术（Post-Quantum Cryptography,PQC）的研发、应用及商业化而形成的技术密集型产业。其核心目标是构建基于量子力学原理或数学复杂性理论的下一代安全体系，确保信息在量子计算时代的安全性、完整性与隐私性。

量子安全是指为应对量子计算威胁所采取的措施，包括物理与数学两种技术手段，其中物理技术即指量子保密通信，包括量子密钥分发（QKD）、量子随机数发生器（QRNG）、量子隐形传态（QT）等；数学技术是以抗量子密码学（PQC）为核心构建的密码安全算法，以及量子数字签名、量子计算机在安全领域的应用等多个方面。量子安全旨在提供一种理论上无法被破解的通信方式，即使面对未来强大的量子计算机的攻击也能保持信息的机密性和完整性。

量子保密通信是指利用量子力学的基本原理，特别是量子不可克隆性、量子纠缠原理以及测不准原理，通过保密通信协议和工程技术，如量子密钥分发、量子随机数发生器和量子隐形传态等，实现信息传输的安全性。

抗量子密码是指抵抗量子计算攻击的密码学算法，这些算法被设计用来确保即使在量子计算机成为现实的情况下，其计算复杂度仍为指数级，从而保障信息安全。一切可以抵抗量子计算攻击的新算法均可成为抗量子密码。

图表 量子安全产业研究对象架构





01

2024产业发展概览

目录

01
2024产业发展概览

01 深耕研发，技术多线突破

02 产业链纽带增强，推动多元化合作发展

03 抗量子密码企业集聚成势，赋能产业优化升级

04 政策引领产业方向，融资激发创新活力

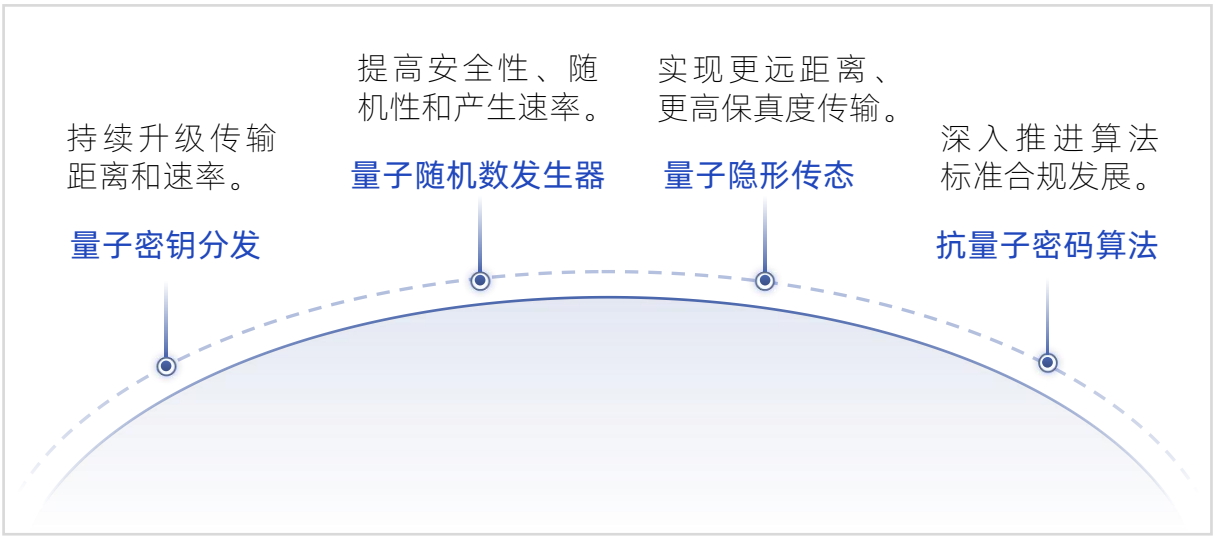
05 产业规模爆发增长，细分领域协同发力

06 产业发展周期逐步向融合阶段迈进

01 深耕研发，量子安全技术多线突破

2024年，量子密钥分发、量子随机数发生器、量子隐形传态及抗量子密码算法等关键技术均取得显著突破，成果丰硕。

图表 2024年量子安全关键技术发展情况



光子盒研究院QUANTUMCHINA | 2025.2

量子密钥分发技术持续升级，不仅在传输距离和速率方面取得了重要突破，而且使得量子安全通信的覆盖范围更广、信息传输效率更高。丹麦技术大学团队利用连续变量量子密钥分发（CV QKD），在100公里距离成功分发量子安全密钥，刷新连续变量量子密钥分发传输距离记录，为长距离量子通信网络构建提供技术支撑。

量子随机数发生器在安全性和随机性方面有了很大提高。同时产生速率也得到了提升，以满足各应用场景对于实时性的要求。韩国SK电讯与KCS公司共同开发的量子密码芯片QKEV7，此芯片集量子随机数发生器与加密通信功能于一体，有物理不可克隆等技术，且轻量、低功耗。

量子隐形传态实现了更远距离和更高保真度传输。美国西北大学工程师利用现有互联网光缆演示量子隐形传态，在30公里长的光缆上与高速互联网信号同时传输量子信息，证明量子通信和经典通信可共存，为构建更复杂、高效的量子信息系统提供了技术支持，也为长距离量子连接的实现开辟了新路径。

抗量子密码算法继续深入推进。美国国家标准与技术研究所（NIST）的加密算法验证程序，严格评估筛选各类抗量子密码算法，促使全球科研力量积极优化改进算法，有力推动了抗量子密码技术合规性与实用性的发展，并于8月正式发布了全球首批抗量子密码标准。

02 产业链纽带增强，推动多元化合作发展

2024年，量子安全产业迎来了技术突破与商业应用并进的发展高峰。在这一过程中，产业链中协同创新与多元化合作成为行业发展的核心驱动力。通过各环节的深度联动，形成了持续推动产业繁荣的闭环体系。

量子保密通信是产业链的关键构成，核心在于保障信息传输安全。量子密钥分发作为量子保密通信的核心技术，吸引了诸多企业和机构积极参与。这些参与者在密钥分发技术研发和设备制造方面持续发力，不断推动量子密钥分发系统性能的显著提升。与此同时，量子网络建设也在稳步推进，众多企业携手共同探索构建广域量子通信网络，力求实现更大范围的安全通信，为信息安全传输筑牢坚实基础。

抗量子密码技术旨在抵御量子计算对传统密码的威胁。一方面，有专门的抗量子密码算法研究机构和企业，积极投入算法研发，美国国家标准与技术研究所（NIST）的加密算法验证程序也推动着算法的合规性发展。另一方面，“抗量子密码+”体现在与其他技术融合，如与传统加密技术结合，开发新的加密模块和芯片，企业研发的具备抗量子能力的密码芯片，为设备提供更安全的加密功能，提升整体安全性。

行业应用领域广泛且深入。金融行业是积极探索应用的典型，众多银行利用量子保密通信和抗量子密码技术，保障金融交易数据的保密性、完整性和不可抵赖性，防范潜在的量子计算攻击风险。国防领域，机构运用量子安全技术，增强军事通信和信息系统的安全性，确保国防信息安全。通信电网行业同样积极应用，量子安全技术保障通信网络稳定和电力系统数据安全，各行业的应用需求也反向推动着量子安全技术的持续创新和发展，促使产业链不断完善。

未来，随着全球对数据安全需求的不断提升，量子安全产业的合作模式将更加开放多元。通过构建更加紧密的合作网络，量子安全产业链有望形成以需求为导向、创新为驱动的全球化发展格局，进一步巩固技术与商业应用的双重优势。

图表 2024全球量子安全产业生态图谱



光子盒研究院 QUANTUMCHINA | 2025.2

03 抗量子密码企业集聚成势，赋能产业优化升级

当前，全球抗量子密码企业正加速集聚，在科技资源富集区域形成产业高地。这一集聚现象推动资本、人才、技术等要素深度交融，极大提升了创新效率，加快技术迭代与应用拓展。

图表 全球抗量子密码研究企业分布



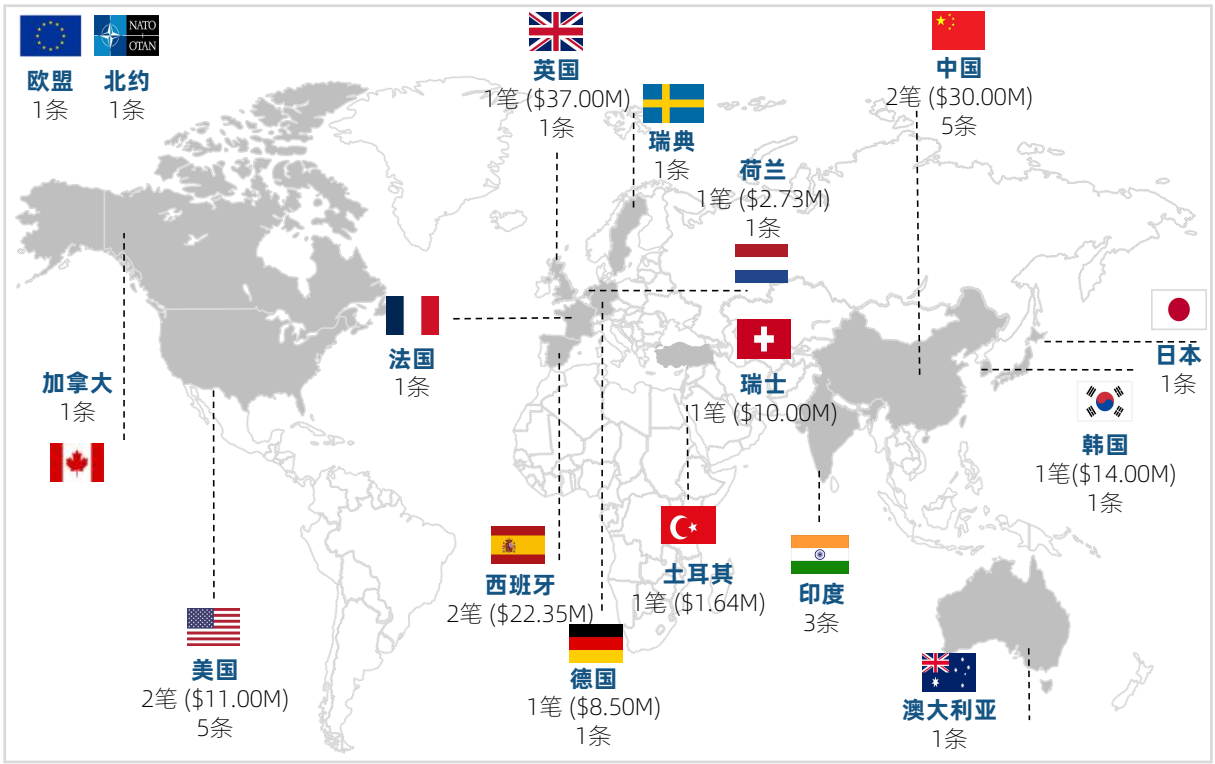
光子盒研究院 QUANTUMCHINA | 2025.2

从地域分布来看，美国、中国、欧盟吸引众多抗量子密码公司扎根，美国凭借其标准化主导权和产业生态优势，引领抗量子密码技术发展；欧盟通过政策协调推动技术整合；中国则在量子通信产业化基础上加速布局抗量子密码研发，但产业成熟度和国际话语权仍需提升。加拿大、英国、日本、韩国、印度等国家，虽然其公司数量相对较少，但也凭借自身优势在抗量子密码领域崭露头角。未来，随着对抗量子密码领域的资金投入不断增加、相关企业创新持续活跃，各区域有望形成量子安全产业集群。

04 政策引领产业方向，融资激发创新活力

2024年，全球各国家与地区量子安全政策频出，涵盖战略规划与行业规范等多个方面；融资端同步上扬，政府与社会资本合力为量子安全产业注入活力。

图表 2024年全球量子安全企业融资情况及发布的国家级政策条数



ICV TA&K & 光子盒研究院 QUANTUMCHINA | 2025.2

政策方面，全球各国对量子安全重视程度与日俱增，纷纷出台相关政策，支持产业发展。美国从战略层面引导资源流向，强化自身在量子安全领域的技术优势和产业布局；中国积极推进量子通信基础设施建设，致力于构建量子通信网络；印度、澳大利亚等也不甘落后，纷纷出台涵盖法案与国家量子发展战略等政策文件。

融资方面，与政策的活跃程度一致。政府对量子安全领域重视程度的提升，即政府融资的占比不断增加。政府通过直接投资、设立专项基金等方式，为量子安全企业提供了稳定的资金来源，降低了企业的融资成本和风险。同时，政策的利好也吸引了更多社会资本的关注，风险投资、私募股权投资等纷纷涌入，为企业的技术创新、产品研发和应用拓展注入了强大动力。

总体来看，政策与资本的双轮驱动，正加速全球量子安全产业的成熟与落地。政策制定战略、规范标准，引导融资流向关键方向；融资为科研项目和企业发展供能，保障政策落地。二者合力增强国际合作与竞争优势，促进产业发展。

05 产业规模爆发增长，细分领域协同发力

2024年，量子安全领域产业规模持续增长。在技术进步、需求增长以及政策支持等多重因素推动下，量子密钥分发、量子随机数发生器、抗量子密码等细分领域，展现出巨大发展潜力和广阔应用前景。从全球范围看，2024年全球量子安全产业规模约12.9亿美元，较2023年增长2.1亿美元，增长率达19.4%。预计2030年，这一规模有望达到172.7亿美元，2024-2030年期间年复合增长率为55.9%。若继续保持这一良好发展趋势，预计到2035年，全球量子安全产业规模将达到966.6亿美元。

从各领域逐步推进应用的时间线来看，2027年前，经典密码仍相对安全，产业处于缓冲期。预计到2035年，经典密码将面临严峻挑战，各行业对量子安全需求的激增，推动量子密钥分发、抗量子密码等领域快速发展。届时量子安全产业规模有望迎来爆发式增长。从量子安全行业应用发展态势看，到2035年：

军事领域

- 产业规模将达到70.34亿美元，位居榜首。军事活动是国家安全的基石，对信息保密性、完整性和抗攻击性要求近乎苛刻，因此在量子安全技术上投入不遗余力，造就了最大的应用产业规模。

电网领域

- 以53.95亿美元紧随其后，凸显了在数字化浪潮下，能源基础设施对量子安全的高度依赖。稳定的电力供应是社会运转的动力源泉，其信息系统的安全性至关重要，而量子安全技术则是抵御潜在网络威胁的关键防线。

金融领域

- 以46.61亿美元位列第三。在金融交易日益数字化、全球化的背景下，保障客户资金和敏感信息安全是行业发展的生命线，而量子安全技术可为其提供前所未有的安全保障。

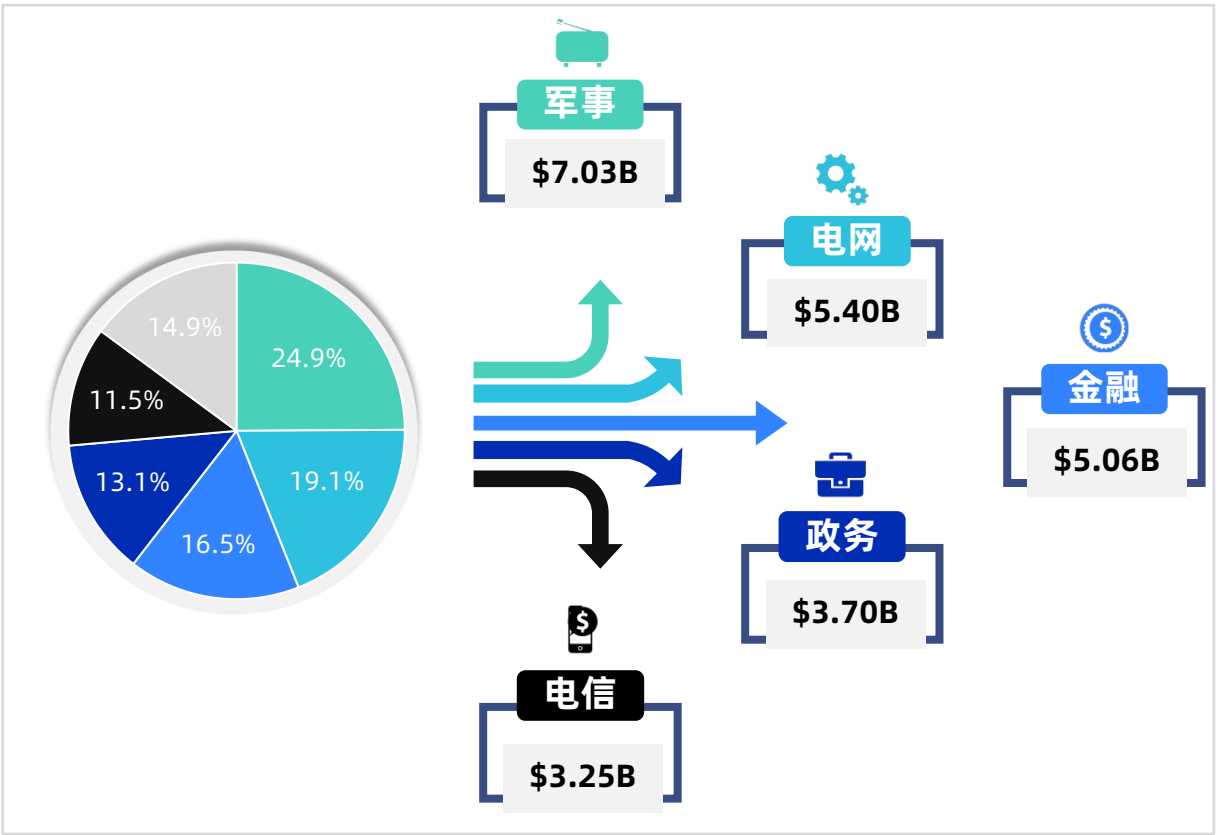
政务领域

- 产业规模达37.00亿美元。电子政务广泛应用，使政府数据面临诸多安全挑战，而引入量子安全技术将有效提升政务系统的安全性和可靠性。

电信领域

- 产业规模为32.48亿美元。电信行业作为信息传输的关键通道，应用量子安全技术将为其构建更稳固的通信网络，确保信息传递安全畅通。

图表 2035年量子安全应用产业规模概览

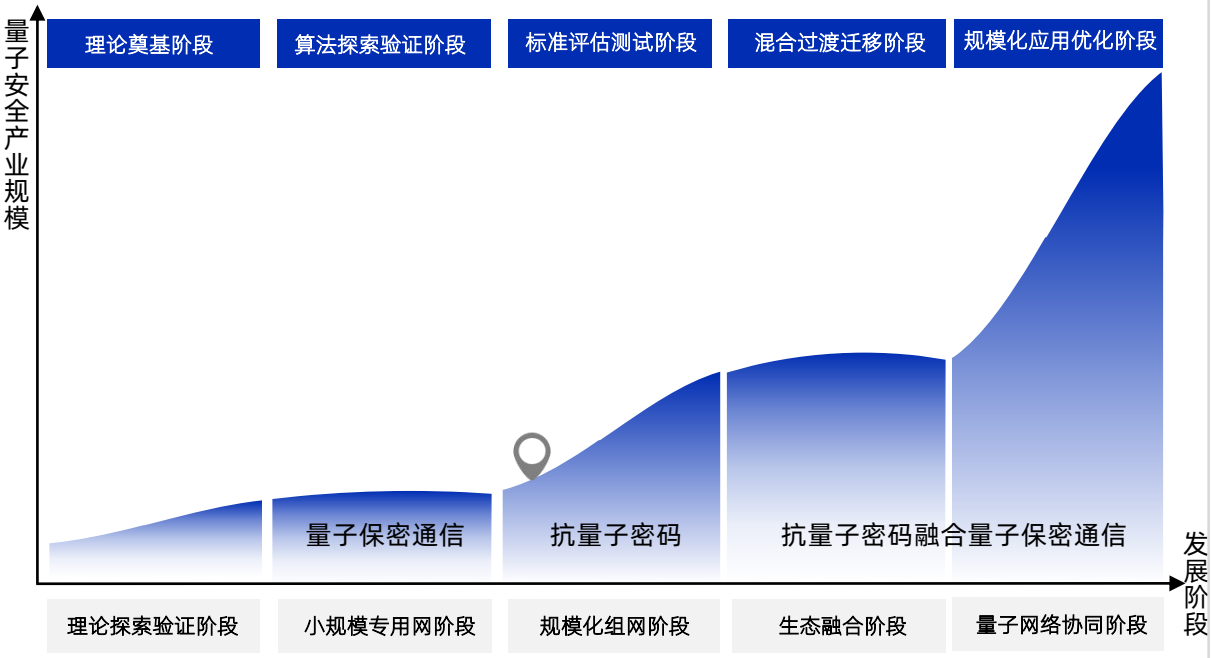


ICV TA&K & 光子盒研究院 QUANTUMCHINA | 2025.2

06 产业发展周期逐步向融合阶段迈进

量子安全产业发展周期具有震荡上升的趋势。产业发展初期，主要聚焦于量子保密通信，进展相对缓慢。近年来，抗量子密码受关注度迅速增加，其与量子保密通信逐渐呈现出并驾齐驱的发展趋势，产业发展步伐加快，利润也随之稳步提升。直至规模化应用化阶段，抗量子密码持续得到广泛应用，并在之后的量子网络协同阶段大幅增长。

图表 量子安全产业发展周期示意图



	理论探索验证阶段	小规模专用网阶段	规模化组网阶段	生态融合阶段	量子网络协同阶段
量子保密通信	• 原理性实验验证，以证明量子通信的可行性，稳定地演示量子通信的一些关键功能。	• 开始在一些特定场景或区域进行小规模的试点应用，如在一些对信息安全要求较高的机构。	• 实现较大规模的量子通信网络建设，如覆盖城市、城市群甚至更大范围的广域量子通信网络。	• 建成量子互联网，与传统互联网深度融合，实现安全通信和实时量子协作网络。	• 成为多功能网络的一部分，同时具备量子计算、传感和控制等功能，网络系统高度智能化。
抗量子密码	• 主要集中在对各种数学难题的研究，如格问题等，以寻找适合构建抗量子密码算法的数学基础。	• 初步的筛选工作，在安全性、性能和实现成本方面展开广泛讨论，但技术仍主要停留在实验验证阶段。	• 标准化成为核心任务，全球范围内对候选算法展开算法的性能、兼容性和安全性评估。	• 关键领域开始逐步替换或升级加密系统。同时，硬件和软件开发商研发支持抗量子，密码的产品和技术。	• 抗量子密码算法成为通用技术被广泛使用。密码算法持续优化，形成动态升级机制。

光子盒研究院 QUANTUMCHINA | 2025.2

目前，量子保密通信正处在从小规模专用网阶段到规模化组网阶段。未来发展的重点在于通过对量子密钥分发等技术的持续研究，提高应用系统的安全性与效率。抗量子密码尚在由算法探索验证过渡到标准评估测试阶段。受益于标准化推进和政策支持，相关机构正积极将现有加密算法迁移至抗量子密码体系，推动密码学领域向更安全、更高效的方向升级。随着量子计算技术的快速发展，抗量子密码与量子密钥分发的融合趋势将日益显著，未来或许会“后来居上”，成为替代单一方案、保障未来信息安全的关键力量。



02
量子保密通信

目录

02
量子保密通信

01 保密通信协议

02 工程技术

03 综合通信网络

04 应用场景分析

05 标准化工作进展

01 保密通信协议

量子密钥分发：寻求更远距离、更高速度、更强安全性的突破

量子密钥分发技术作为量子保密通信领域的核心，展现出高安全性和低误码率等优势。其发展着重于提升安全性和效率，旨在提高密钥生成速率、降低误码率，进而确保量子保密通信具有更高效率和更强安全性。

同时，量子密钥分发在高效率与远距离传输方面不断取得突破，当前研究大多聚焦于突破现有距离限制，实现更远距离的传输，推动跨区域、跨城市乃至跨国界的量子保密通信网络的建设。

增加传输距离与提升传输速率为发展关键

量子密钥分发技术的核心挑战之一在于提升密钥分发的传输距离和速率，这对于实现长距离量子保密通信具有决定性意义。在量子保密通信领域，传输距离直接关联到量子密钥分发网络的覆盖范围和实用性，而传输速率则影响着密钥生成的效率和通信的实时性。为了克服这些挑战，全球的研究人员和工程师在2024年探索了多种创新技术和方法。

首先，提高传输距离意味着量子密钥分发系统必须能够在更长的光纤链路或者自由空间信道中保持量子态的完整性，同时抵抗环境噪声和信号衰减的影响。

01

连续变量量子密钥分发为长距离量子通信网络构建提供支撑

Danmarks Tekniske Universitet DTU

利用连续变量量子密钥分发（CV QKD），在100公里距离成功分发量子安全密钥，刷新CV QKD传输距离记录，为长距离量子通信网络构建提供技术支撑。

其次，传输速率的提升是实现高效率量子密钥分发的关键。在长距离传输中，信号衰减会导致密钥生成速率降低，从而影响通信的实时性和效率。

02

采用QCKD协议，在1707公里的光纤电缆上演示量子密钥分发

通过采用量子保护控制密钥分发（QCKD）协议，在1707公里的光纤电缆上演示了量子密钥分发，尽管传输速率降至0.9比特每秒，这一成就仍然是量子密钥分发技术在不使用量子中继器的情况下实现的最长距离之一。

但是，目前仍然存在一定的问题：

一是量子通信距离依旧较近。由于量子态随距离增加衰减急剧增加，严重制约量子通信距离的增加。目前光纤传输最远可达1707km，水下通信可达到几百米范围，与实际应用对传输距离的要求还有一定差距。未来随着量子通信中继、量子存储等技术的发展，量子通信距离将得到大幅提升。

二是通信速率依旧较低。由于目前量子态产生、传输和检测速率低，使得量子通信速率一直无法有效提升，无法完全满足大规模应用对系统　高带宽的使用需求。未来，有望通过优化量子通信网络架构和采用多路复用技术等方法，不断提高量子通信速率。

未来随着量子通信中继、量子存储等技术的发展，量子通信距离将得到大幅提升。

重视协议升级，持续增加量子密钥分发的抗干扰能力

量子密钥分发技术之所以受到广泛关注，很大程度上归功于它基于量子力学原理提供的无条件安全性。然而，理论的完美性并不直接等同于实际应用的无懈可击。在现实世界的量子密钥分发部署中，实际的量子密钥分发系统可能会因为设备不完美、环境噪声、操作失误等因素而出现漏洞，这些漏洞可能被敌手利用来窃取密钥信息。例如，量子信道中的光子可能受到损失或退相干的影响，导致信号质量下降，从而影响密钥的安全性。为了应对这些挑战，研究人员正在开发更加鲁棒的量子密钥分发协议，以提高系统的安全性和抗干扰能力。

01

中国科学院 CHINESE ACADEMY OF SCIENCES

更精确相位误码率提高系统安全性

对双场量子密钥分发（TF-QKD）的相位误码率采用了更精确的估计方法，有效降低了误码率，从而提高了系统的安全性。

02

JIQT

清華大學

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

利用强光产生的非线性噪声进行量子安全隐蔽通信

验证了在进行经典通信的光纤中，可以利用强光产生的非线性噪声作为背景，进行量子安全隐蔽通信，这种技术能够在一定程度上抵御窃听和干扰。

除了改进协议和提升系统性能，量子密钥分发系统的安全性还依赖于对潜在攻击的持续监测和防御，包括实时监控量子信道的状态，及时发现异常行为，并采取相应的对策等。例如，通过机器学习等先进技术，研究者可以更有效地识别和预测可能的攻击模式，从而提前采取措施防范。

聚焦创新协议与优化算法

为适配多样化应用场景并提升量子密钥分发效率，研究者持续创新，不断提出和优化各类新型协议与算法。不同应用场景对量子密钥分发系统的要求各异。

- 金融高频交易、5G核心网及海底电缆通信等场景，因数据量庞大，对密钥生成速率要求极高；
- 政务公文传输、军事战场通信等，鉴于对信息实时性和保密性的严格要求，则更看重系统的稳定性与抗干扰能力。

研究者开发出多种量子密钥分发协议，涵盖基于不同量子比特编码的协议、适应不同信道条件的协议，以及能在特定攻击模型下增强安全性的协议。

在效率提升方面，新的量子密钥分发协议通过优化量子信道利用、减少量子资源需求、提高密钥生成速率及降低错误率，来增强系统整体性能。

01

优化模式匹配量子密钥分发方案

使模式匹配量子密钥分发方案适用于至长度、衰减不对称信道，显著降低非对称信道对性能的影响。

02

融合多节点量子密钥分发技术与多种密码手段

为提高长文档签名效率，提出一种抗抵赖、抗伪造的电子商务解决方案，强化了安全性。

在算法优化上，研究者借助数学工具和计算技术，剖析和改进量子密钥分发协议性能。有助于预测并适应信道变化，动态调整参数以实现密钥生成速率最大化，同时提升安全性。

与现有通信技术的高度兼容集成

量子密钥分发技术的兼容性和集成性是实现其产品通用化和大规模部署的关键所在。在量子通信迅猛发展的当下，量子密钥分发技术既要与现有的通信基础设施实现无缝对接，又要维持其独有的量子安全性。这种兼容性和集成性所面临的挑战，不仅体现在技术层面，还涉及成本效益、用户接受度以及市场推广等多个维度。

从技术角度而言，量子密钥分发系统的兼容性表现为能与现有的光纤网络、数据中心及各类通信设备协同运作，无需对基础设施进行大规模改造。

01

Danmarks Tekniske Universitet DTU

实现连续变量量子密钥分发技术与现有互联网基础设施兼容

成功实现连续变量量子密钥分发技术与现有互联网基础设施兼容，为量子密钥分发的广泛应用筑牢了重要的技术根基。

从集成性角度来说，量子密钥分发技术与其他通信技术的高度整合涵盖经典通信协议和网络管理系统。这就要求量子密钥分发系统除了提供量子密钥分发功能外，还需适配现有的网络架构和操作流程。

02

NOKIA LUXQUANTA

验证量子密钥分发技术与空芯光纤技术的兼容性

在数据中心生产网络环境中对量子加密系统开展概念验证，验证了量子密钥分发技术与空芯光纤技术的兼容性，为数据中心安全通信提供了新方案。

01

中电信量子集团
CHINA TELECOM QUANTUM GROUP

发布商用量子密钥分发光传输终端

实现了60km以上10Tbps经典量子共纤传输，集成了量子密钥分发共纤融合、集中式密钥中继、国密OTN加密、网络统一管控等功能。

随着量子技术的持续进步，量子密钥分发需在保障量子安全性的前提下，实现与现有通信技术的无缝对接和深度整合。这不仅能降低部署成本、加速技术推广，还能为用户提供更灵活、更可靠的通信解决方案。

多方加强国际合作与技术共享

在全球化的科技发展浪潮中，量子安全领域的复杂性和多样性使得各国科研机构、企业以及政府之间的协作变得至关重要，只有携手共进，才能有效应对共同面临的技术挑战和安全威胁。

量子通信技术专业性强、技术门槛高，依靠单一国家的力量很难全方位推动其发展。量子密钥分发技术作为量子通信的关键部分，涉及量子物理、光学工程、信息技术等多学科交叉，研究人员在这些领域的深入合作与交流尤为必要。

01

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
esa
European Space Agency

验证了量子密钥分发技术的有效性和安全性

联合27个欧盟成员国和欧洲航天局开展的量子通信实验，通过扩大实验规模和丰富实验场景，在不同环境与条件下验证了量子密钥分发技术的有效性和安全性。

技术创新合作，共同探索如何借助量子力学特性增强通信安全性，抵御潜在的量子攻击。

02

HERIOT WATT UNIVERSITY

SAPIENZA UNIVERSITÀ DI ROMA

LUND UNIVERSITY

利用逆设计把多模光纤转变为通用的多结果测量设备

利用逆设计技术，将光学回路嵌入到多模光纤等模式混合器的高维空间中，成功把多模光纤转变为通用的多结果测量设备，实现了传输和验证纠缠态的功能。

03

Danmarks Tekniske Universitet DTU

UNIVERSITY OF COPENHAGEN

将优化稳定性后的量子点单光子源频率转换到通信波段

在哥本哈根城区的现网光纤上开展诱骗态BB84协议试验，在信道衰减9.6dB的情况下，成码率保持在2kbps以上。

国际间在量子密钥分发技术上的合作研究，这种合作不应局限于学术界，政府、产业界和安全机构的参与同样不可或缺，各方应共同构建一个协作生态系统，共同应对未来安全挑战。

04

SDT SPACE & DEFENCE TECHNOLOGIES

부산대학교 PUSAN NATIONAL UNIVERSITY

量子纠缠光子对光源技术

致力于开发一种紧凑的、可机架安装的量子纠缠光子对光源技术，旨在实现该技术的产业化应用。

目前，量子密钥分发技术正快速走向成熟，在安全性、效率、兼容性和创新协议开发等方面成果显著。然而，要实现该技术的广泛应用，仍需克服成本较高、设备复杂以及用户接受度有待提升等问题。

量子隐形传态：实现多维度、远距离及多端兼容的探索

量子隐形传态是量子安全领域的关键技术，近年来取得了一系列进展。研究人员通过发展多维度量子隐形传态来增强信息处理能力，突破远距离传输助推全球通信链路构建，还在实验里达成了与经典网络的兼容。然而，该技术仍处于探索阶段，面临成本高昂和设备复杂等挑战。

发展多维度量子隐形传态，提高系统安全性

多维度隐形传态指的是在更高维度的量子系统中实现信息传输，涉及更复杂的量子态和更高级的量子操作。其发展不仅扩展了量子通信的维度，还极大地增强了量子信息处理能力。

多维度量子隐形传态能够提供更丰富的量子信息编码方式。在多维度系统中，每个量子比特可以表示更多状态，使信息的编码和传输更为高效，同时也提高了系统的安全性。

01

为高维量子网络中的资源设计和分配提供新方法

提出了一种实现最佳d-维度量子隐形传态保真度的方法，能在更广泛范围内精确确定最佳量子隐形传态保真度，提高了对通道资源有效性的识别能力。

在高维量子系统中，量子信息可以在更多自由度中分布，使系统能够更好地抵抗外部噪声和干扰，有效保持长距离条件下量子通信的稳定性和可靠性。

创新量子隐形传态接口，构建长距离传输信道

远距离量子隐形传态的发展突破了地理限制，使全球范围内的量子通信成为可能。在不同国家和地区之间建立安全的通信链路，实现长距离的量子态传输，对国际合作、科学研究以及全球数据安全意义重大。

通过构建超远距离的量子信道，不同国家和地区之间能建立起高度安全、难以被窃听与破解的通信传输网络。

01

创新的量子接口实现了远高于经典边界的隐形传态保真度

Danmarks Tekniske Universitet DTU

提出一种创新的量子接口，该接口能够将金刚石NV色心量子网络节点与光子时间仓量子比特进行连接，实现了远高于经典边界的隐形传态保真度。

电信光纤上实验量子隐形传态，验证在经典网络运行的可行性

量子隐形传态的部署需要多节点稳定运行，同时具备高度系统兼容性与优化网络协议，以实现量子网络跨区域连接更多用户和系统，进而达成广泛的信息共享与处理。

01

证明在统一光纤基础设施中同时运行先进量子和经典网络应用的可行性

展示了在承载传统电信流量的光纤上实现量子隐形传态，实验在30.2公里的光纤上进行，该光纤同时承载400-Gbps的C波段经典流量。

量子隐形传态技术的这一突破，不仅在一定程度上解决了技术在多节点稳定运行的问题，还展示了其在现有网络基础设施上的兼容性，为未来的量子网络发展提供了新的方向和可能。

目前，量子隐形传态技术大多还处于科研实验阶段，要实现量子隐形传态的广泛应用，还需要解决成本、设备复杂性等问题。量子隐形传态技术的成本因实验设备和技术要求而异，通常需要高精度的量子控制设备、低温超导技术以及可靠的量子态监测系统，以支持量子隐形传态实验的开展，尽管设备初期投资较高，但随着技术进步和规模化生产，成本有望降低。

量子密钥共享：加快量子纠缠的高效传输和多体纠缠的快速生成

量子密钥共享作为量子保密通信的基石，依赖于量子纠缠特性，借助纠缠态粒子间无视距离的“心灵感应”式相互作用，能在两个或多个实体间构建牢不可破的安全通信链路，确保信息传输的绝对安全与保密。

优化量子密钥共享的传输性能，拓展实现途径

量子密钥共享的高保真度意味着纠缠态在传输中受干扰和噪声小，从而降低了被窃听者窃取密钥信息的风险。

提升传输性能要持续追求更低噪声、更高不可区分度、更远距离传输和更高保真度。这些指标是实现量子保密通信广泛应用的技术基础。

01

研制将金刚石Si空穴单光子转换到通信波段的系统

实现了低噪声和89%的高不可区分度转换能力，还演示了将光子通过50km现场光纤传输，并与金刚石量子存储器建立纠缠，保真度达87%。

其他实现途径还有量子密钥共享研发新型编码算法，提升密钥信息密度，降低传输冗余。利用拓扑材料构建量子信道，减少信号损耗，进一步扩大量子密钥共享技术的适用范围。

构建多体纠缠快生机制，降本增效

在量子密钥分发协议中，纠缠生成速度决定密钥生成速率，多体纠缠的快速生成能有效提高量子密钥分发速率。

快速生成多体纠缠意味着能在更短时间内产生更多密钥，从而提高通信效率和吞吐量。

01

揭示量子纠缠快速生成的新机制

解释了在哈密顿系统中如何通过量子离域过程在关联景观上快速生成高度纠缠的多体量子态。该研究框架为量子纠缠快速生成提供了理论基础，对实现高效量子密钥共享意义重大。

此外，快速生成多体纠缠还可降低量子通信系统的复杂性与成本，使量子保密通信技术更易部署和维护，推动其广泛应用。

02 工程技术

量子随机数发生器：逐步从实验室走向大规模商业化

量子随机数发生器虽已有一定成熟度，但距离大规模商业化仍有差距。

01

TOSHIBA

可用于批量组装的全芯片量子随机数发生器

计划投入规模化生产，这是从实验室走向大规模商业化部署的重要一步，能为计算机模拟、彩票等多种应用提供更安全的随机数解决方案。

在高安全认证方面，量子随机数发生器的密码芯片成果显著。

02

硅臻 SILICON EXTREME

突破毫米级尺寸的量子随机数发生器芯片

研发的量子随机数发生器芯片'QRNG-10'，2024年向信息安全终端企业完成首批10K级出货，该芯片尺寸仅4×4mm，采用QFN封装形式。

03

问天量子

发布WT-QRNG300量子随机数芯片

芯片采用基于量子隧穿效应的量子熵源，能生成不可预测的真随机数，裸片尺寸1.3×1.7毫米，封装后5.8×5毫米，体积小、功耗低、性能强，应用前景广泛。

量子光源：高保真度纠缠和多光子纠缠技术日趋成熟

单光子源技术已从理论研究走向实际应用阶段。科研机构不仅在利用卫星单光子源开展相关实验，还在城网光纤等实际场景中进行了大量实践。

01

Abbe Center of Photonics JENA Friedrich-Schiller-Universität

利用卫星单光子源远距离传输

利用卫星单光子源作为远距离安全传输信息的手段。

02

Leibniz Universität Hannover

Technische Universität Braunschweig

确定性单光子源进行的首次城际量子密钥分发实验

利用德国汉诺威和布伦瑞克之间79公里长的链路，损耗为25.49dB（相当于直接连接光纤的130公里），实现了创纪录的每脉冲4.8×10^{-5}密钥比特，平均量子比特错误率约为0.65%。发现最大可容忍损耗为28.11dB，相当于144公里长标准电信光纤。

03

UNIVERSITY OF COPENHAGEN

RUHR UNIVERSITÄT BOCHUM RUB

量子点实现高保真度多光子纠缠

展示三量子比特纠缠的确定性光子源，该电子自旋被囚禁在嵌入平面纳米光子波导中的量子点中，令核自旋变窄，从而使高保真度的相干光学自旋旋转成为可能，并实现了一个自旋回波脉冲序列，用于顺序生成自旋-光子和自旋-光子-光子纠缠。

从技术实现角度看，将电子自旋囚禁在嵌入平面纳米光子波导中的量子点是重要基础。然而，量子点材料制备存在批次间性能差异大、稳定性与一致性难保障的问题，平面纳米光子波导制备工艺复杂，微小误差就会影响光子传输，再加上量子系统易受环境干扰，检测和调控手段不够成熟，这些都给多光子纠缠的实现带来挑战。

单光子探测器：性能提升，解决限制，增强远距离探测与稳定性

单光子探测器在量子通信中起着至关重要的作用，保障信息安全传输和量子态的精确测量。不同类型的单光子探测器在量子通信中相互补充，根据具体应用场景和性能需求，可选择不同的探测器技术，常见的有以下几种：

图表 单光子探测器分类及简介

类别	简介
光电倍增管（PMT）	适用于紫外、可见和近红外区，具有响应快速、成本低、阴极面积大等优点。
半导体雪崩光电二极管（APD）	利用半导体的内光电效应实现单光子探测，具有体积小、集成度高的优势。
超导纳米线单光子探测器（SNSPD）	基于超导材料的纳米线结构，具有高探测效率、低暗计数、低时间抖动等优点，是目前量子通信中最先进的探测技术之一。目前正通过扩大制冷机以容纳更多探测通道数量，从而降低单通道成本。

光子盒研究院QUANTUMCHINA | 2025.2

2024年，单光子探测器的研究取得了一系列的进展。一方面，针对单光子探测器固有的“死区时间”（dead time）问题。

01

LG Electronics

针对单光子探测器固有的“死区时间”问题

由于量子通信传输速率一直受限于“死区时间”（dead time），公布了一项新协议，有望提高传输速率并增强传输安全性。

另一方面，探索单光子雪崩探测器性能影响要素，以保持其使用的长期稳定性。

02



探索单光子雪崩探测器性能影响要素

研究了γ辐照对InGaAsP/InP单光子雪崩探测器（SPADs）性能的影响。研究结果显示，辐照导致暗电流和暗计数率轻微下降，但探测效率和后脉冲概率保持稳定。

未来单光子探测器的发展方向：

一是要进一步提高探测效率，趋近100%理想水平，减少光子丢失和误码率；

二是降低暗计数率，提高信号的信噪比，减少噪声干扰；

三是提升响应速度至GHz及以上频率，以契合高速量子通信的需求；

四是在增加可探测光子数量的同时，实现探测器的小型化和高度集成，便于应用在便携式设备和大规模量子网络中。

数字信号处理芯片：加密性能大幅增强，集成多种算法

在量子随机数密钥生成方面，现场可编程门阵列（FPGA）作为一种数字信号处理芯片，利用量子的不确定性，使密钥生成具有更高的随机性和不可预测性，极大提升数据传输的安全性，有效抵御潜在的量子计算攻击。

FPGA芯片可以支持多种安全算法，例如国际通用的DES、AES、RSA等算法，能满足不同应用场景和用户对安全算法的多样化需求，增强了芯片在全球市场的通用性和适应性。

01

研发量子安全芯片CCP907TQ

C*Core Technology Co.,Ltd.

芯片采用多芯片封装技术，集成了云安全芯片CCP907T、光信号处理芯片AGC001和光量子噪声源芯片，内嵌自主研发的C*CoreC9000 CPU，支持高达20Gbps的数据加密性能，支持多种国际加密算法，还支持SR-IOV技术，能在虚拟化环境中增强硬件密码算法的执行效率。

03 综合通信网络

量子通信链路：实现远距离、高效率和安全性提升

量子通信链路构建研究主要是基于量子密钥分发、量子秘密共享、量子隐形传态等协议进行。

量子中继是加长链路的重要手段

当前，量子通信中继主要有三种类型：

一是基于无源光器件的量子密钥分发，可以实现多用户间的时分复用，但是距离有限，一般不超过100km，且不具备可扩展性；

二是基于可信中继的量子密钥分发，距离远，但中继必须可信，实际应用受限；

三是基于量子纠缠的量子中继，通过在量子通信链路中间设置若干量子中继器进行纠缠交换，可将衰减从指数级降低为多项式级，从而延长量子通信距离；

第三种方式有效解决了通信距离问题，实用性较强，当前关于量子通信链路中继的研究主要以其为基础展开。

量子中继器在量子网络的物理层中发挥着关键作用，特别是能够实现高效纠缠分布的量子中继器。基于单光子干涉的量子中继器方案因其潜在的效率而很有前途。然而，涉及对远距离节点光子源的一阶干涉的方案要求组件具有严格的相位稳定性，这对长距离实现提出了挑战。

01

量子中继器方案实现了更高的终端节点之间的纠缠分布率

提出了一种量子中继器方案，该方案利用单光子干涉并降低了实现相位稳定的难度。在特定条件下，与现有方案相比，该研究方案实现了更高的终端节点之间的纠缠分布率。

提出兼具高效性和鲁棒性的异步量子中继协议，加强实用化量子网络的建设。

01

纠缠产生效率高、相位稳定要求低的异步量子中继协议

提出了一种异步量子中继协议，该协议具有纠缠产生效率高、相位稳定要求低的优势，对于发展实用化量子通信网络的建设具有重要意义。

实现多节点中继和超距量子关联，构建量子通信网络。

02

实现在12公里光纤上预报原子-光子量子关联的多路复用增强生成

连续产生280对原子-光子量子关联，产生一连串光子时间仓脉冲，填充长纤维，并在成功预报后以固定或可变的存储时间按需读出激发的记忆模式。通过多路复用增强，原子-光子关联的预报率可以达到1.95 kHz，对于12 km的光纤长度，量子关联生成速率与内存退相干率的比值可以提高到0.46。

03

量子关联突破物理过程的局部速度限制

通过导引打破局部量子速度限制，展示了量子关联如何允许仅使用局部测量和共享纠缠态的两方之间的经典通信来突破物理过程的局部速度限制。为研究量子相关性如何影响状态和可观测量的动力学性质开辟了途径。

链路安全性不断增强，有望部署城市光纤链路

增强量子通信链路安全性，可从多方面着手。

在量子密钥分发环节，利用单光子不可分割、测量即改变状态的特性，能检测窃听。通过优化量子态编码方式，提高密钥生成与传输的可靠性，降低误码率。

在硬件设备上，选用高质量的单光子源与探测器，减少噪声干扰，确保信号准确收发。

在网络层面，构建量子中继站，可延长通信距离，同时监控传输过程，保障链路安全。还可采用量子加密与经典加密相结合的混合加密模式，双保险提升信息保密程度。

暗光纤链路环境复杂，信号传输易受多种因素干扰，而量子态隐形传态对环境稳定性要求极高。

01

突破复杂环境下量子态精准控制难题
验证了城市量子通信的可行性

MenloSystems

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

UNIVERSITÄT DES SAARLANDES

在14.4公里的城市暗光纤链路上实施了分布和量子态隐形传态实验，实现了主动偏振稳定。这项技术的成功演示，突破复杂环境下量子态精准控制难题，验证了城市量子通信的可行性。

此外，定期对通信链路进行安全检测与漏洞扫描，及时发现并修复潜在安全隐患，全方位守护量子通信链路安全。

02

实施地面量子密钥分发链路成功

esa European Space Agency

在位于比利时的欧洲太空安全教育中心与卢森堡的一个数据中心之间实施了一个地面量子密钥分发链路。基于这一实验的成功，计划拓展至太空，建立天基量子密钥分发链路，这将进一步增强量子通信的安全性。

高效低能耗量子存储技术助力传输距离进一步扩展

实现高效低能耗量子存储技术，是量子领域研究的重要突破方向，可从材料选择、结构设计和策略优化等方面推进这一目标达成。

01

量子存储器将有助于扩展量子网络使信息实现更远的传输距离

制造出了美国宇航局有史以来第一个量子存储器。这项技术是NASA创建大规模量子网络的第一步，它可能会带来更安全的空间通信，并最终带来新的科学发现。

02

利用新形式的存储策略实现高效低能耗量子存储技术

在材料上着手，实验演示了一种新形式的量子存储实现方案，通过将铷原子限制在空心的光子晶体光纤中（空心直径约40微米），可以实现相当于自由空间方式的存储效率（约30%），并且操控所需的能量可以降低为原来的1/100。

03

高效的光子存储策略优化存储和检索过程的效率

从策略优化角度出发，提出了一种高效的光子存储策略，用于腔辅助量子存储器。该策略能够在非绝热条件下，即脉冲持续时间远短于存储器带宽的情况下，优化存储和检索过程的效率。

量子通信网络：推动安全性、集约化和规模化发展

点对点的量子通信链路构建研究只能解决两个节点之间的安全保密通信问题。若要进行多用户之间的密钥交换和信息的安全保密传输，则需研究量子通信网络架构，设计量子通信路由协议，构建量子通信网络。

此外，多芯光纤技术和量子网络的结合将进一步推动量子保密通信的发展，其能显著提高量子通信系统的容量和效率，支持多个量子信号的同步传输，推动量子通信网络的互联互通。

全球多地推进量子通信网络建设

随着全球对量子计算机的投资加速，当前加密技术面临更大风险，量子计算机有可能破解当前用于保护网络的大部分密码学基础，各国需要增强量子计算时代的网络韧性。

目前，全球量子通信网络的建设正在加速推进，多个国家和地区已经建成或正在建设量子通信网络，主要集中在中国、欧洲、美国、日本等。截止到2024年底，全球已建成近30个量子通信网络，并且有10个以上量子通信网络正在建设中。

中国积极推进量子通信网络建设并正在构建覆盖全国的量子通信骨干网。中国中电信量子项目建设取得成效，一是，量子城域网以量子密钥分发为基础，融合经典光通信网络，构建天地一体量子通信基础设施，面向政务、国防、金融、企业、驻外机构的需求，提供敏感信息加密传输、关键数据加密存储等服务。二是，以中国电信OTN精品光网为基础，融合自主可控的量子安全+国密技术，打造超高安全的政企OTN专线增值服务和新型量子城域网解决方案，构建安全可信的抗量子计算新型信息基础设施。



美国：
通过多方合作、技术攻坚和资金支持，全方位推进量子网络发展

- **分布式量子网络测试平台局域网络与广域量子网络结合。**美国能源部布鲁克海文国家实验室和美国空军研究实验室（AFRL）签署了一份谅解备忘录。通过将AFRL位于罗马的分布式量子网络测试平台局域网络与布鲁克海文实验室在纽约地区的广域量子网络的合作研究工作联系起来，以加强量子通信和网络合作。

- **构建远距离量子网络，创光纤量子纠缠距离记录。**美国哈佛大学团队展示了一个由硅空位（SiV）中心构成的多量子比特寄存器搭建的两节点量子网络。该网络通过集成电信光纤网络的纳米光子钻石腔体，部署在大约22英里的环路上，实现了远程纠缠。

- **真空光束引导器突破量子通信距离，大幅提升信道容量。**美国斯坦福大学应用物理系、金兹顿实验室与芝加哥大学普利兹克分子工程学院发现，真空光束引导器（VBG）为长距离量子通信提供了全新解决方案，克服了现有光纤和卫星技术的局限。

- **资助学校量子系统研究，推进量子网络纠缠技术提升。**美国罗切斯特理工学院已获得NORDTECH 397万美元的拨款，这是一项为期四年奖励的一部分，随着研究的进展，学校可能会获得近1000万美元的资助，重点将是通过将量子系统纠缠在光子网络中来扩展量子系统的能力。



中国：
深入挖掘量子网络潜能，不断拓展量子网络技术边界

- **实现远距离量子纠缠网络，提升量子通信至新量级。**中国科学技术大学潘建伟院士带领的研究团队首次完整实现了基于单光子干涉的远距离双节点纠缠，并以此为基础构建了城域三节点量子纠缠网络。该工作使得现实量子纠缠网络的距离由以往的几十米延长至几十公里，整整提升了3个数量级，为后续开展量子网络应用奠定了科学与技术基础。
- **研究量子网络的远程状态制备能力，发挥量子优势。**中国台湾省国立成功大学通过实验研究了一种被称为远程状态制备（RSP）能力的量子资源。这种资源验证了实现真正量子网络所需的所有静态和动态元素，在这种网络中，RSP的实现可以超越任何无纠缠和无量子比特单元策略的经典模拟。



阿联酋：
积极融入全球量子密钥分发网络，铸牢自身通信安全边界

- **阿联酋凭借其前瞻性的战略眼光，在量子通信领域迈出了坚实步伐。**中东和北非地区最大的量子光学地面站——阿布扎比量子光学地面站ADQOGS正式启用。该设施将致力于发展安全的自由空间光通信，可以将阿布扎比和阿联酋集成到全球量子密钥分发网络中，有效解决传统光纤无法满足的远距离量子保密通信需求的问题。这是对全球量子通信网络建设的积极融入，也是在拓展自身通信安全边界，提升国际通信安全保障能力，为未来在金融、电信等领域的安全通信应用筑牢基础。



欧洲：
通过产学研多方协作，推动其从理论研究迈向实际应用

- **开启对量子安全网络的访问，推出量子安全连接服务。**英国BT Group、Toshiba和Equinix之间的合作开启了对数据中心之间量子安全网络的访问。这是英国首次在数据中心之间提供专用的量子安全连接服务，支持多用户访问，为各类组织试用“量子密钥即服务”提供了理想场所，标志着量子安全通信向更广泛可访问性迈出了重要一步。

- **发展量子通信网络，推进跨境安全连接保护关键数据。**欧盟在“连接欧洲设施”下的提案中，鼓励联盟成员提出包括地面和卫星在内的量子通信网络解决方案，其核心目标是利用量子密钥分发技术实现安全的跨境连接，以保护关键公共基础设施和敏感数据的跨境传输。据悉，欧盟正在推进欧洲量子通信基础设施计划，以建立一个跨越整个欧盟及其成员国的超安全通信网络。

- **实现量子网络节点间预报纠缠，为城域量子网络提供通用平台。**荷兰代尔夫特理工大学报告了两个相距10公里的独立运行量子网络节点之间的预报纠缠。承载金刚石自旋量子比特的两个节点通过已部署的25公里光纤与中点站连接。通过将量子比特原生光子的量子频率转换为电信L波段，并将链路嵌入到可扩展的稳相架构中，从而最大限度地减少了光纤光子损耗的影响，能够使用抗损耗的单击纠缠协议。该架构为探索城域尺度量子网络建立了一个通用平台。

- **提出量子网络相关性证明方法，增强多方量子协议安全性。**英国赫瑞瓦特大学、瑞士日内瓦大学、西班牙数学科学院等的研究提出了一种通用方法，旨在证明在特定量子网络中无法产生某些特定的相关性。采用量子膨胀技术，对量子群加密实验中收集的数据进行处理，从而确保在光学元件较少的网络中，观察到的结果不可能通过任何局部的物理过程产生。

- **利用MQPG实现频率编码量子网络，提升可扩展性和资源效率。**德国帕德博恩大学提出了一种基于多输出量子脉冲门（MQPG）的线性光量子网络实现方法。该方法通过频率转换实现基于频箱的、完全可编程的干涉仪，节省资源并提高可扩展性。网络的量子输入态由0型参数下变频（PDC）源提供，具有强频率纠缠。
- **在生产设施中无缝集成新型量子密钥分发网络。**西班牙马德里理工大学提出马德里量子通信基础设施（MadQCI）——一个在生产设施中部署的异构且可扩展的SDN-量子密钥分发网络，它通过解耦组件和现代范式设计，提高了网络的灵活性、可扩展性和成本效益，同时促进了量子密钥分发在安全和电信网络中的集成。

量子通信网络：聚焦安全性、集约化和规模化发展

图表 2024全球各国家地区量子通信系统分布情况



光子盒研究院 QUANTUMCHINA | 2025.2

合作推进小型化和集成化建设

在小型化层面，量子通信系统主要设备体积的持续减小，可大幅降低发射成本，使更多机构与国家有能力参与量子通信项目，加速全球组网进程。同时，小型设备便于灵活部署，能快速响应多样化通信需求，在特定区域或应急场景中发挥关键作用。

例如，重约3.53公斤的德国小型立方体卫星“Qube”成功发射升空并进入预定轨道，即将通过光链路进行量子密钥生成和分发的测试。

集成化趋势下，将量子有效载荷与各类软件、平台深度融合，能打造高度协同的系统。这不仅能提升通信系统的设备性能与可靠性，还能简化操作流程，降低技术应用门槛。

01

为政府和商业运营商创建、交付和部署量子安全密钥分发卫星

合作关系将涉及将SpeQtral的量子有效载荷与Antaris SatOSTM太空飞行器软件和合作伙伴总线平台集成。

向构建天地一体的量子通信网迈进

当前，构建天地一体的量子通信网已成全球科研与产业领域的重要趋势。各国纷纷加大投入，积极开展卫星发射与地面网络建设工作。

01

小型卫星的紧凑型设计已在实验室环境中完成了验证

从设备端来看，计划在2026年发射一颗名为Q4S的小型卫星，以展示其在轨量子纠缠交换能力，探索量子通信新应用。

02

为近地轨道任务开发量子密钥演示器

已获得西班牙CDTI（技术发展和创新中心）授予的第二阶段合同，为500-700公里高度的近地轨道（LEO）任务开发量子密钥演示器，用于搭载近地轨道卫星及其相关的地面段，包括光学地面站。

地面上，中国电信大力部署量子城域网，未来将与骨干网、“墨子号”卫星打通。这种天地协同发展，不仅能扩大量子通信覆盖范围，提升信息传输安全性，还将助力构建更加安全可靠的全球通信体系。

04 应用场景分析

2024年量子保密通信在下游应用进一步推进，在金融、政务和电信等高安全需求领域已取得一定应用成果。随着技术进步和应用场景的拓展，量子保密通信技术预计将进一步扩展至物联网、自动驾驶、无人机通信等新兴领域，为这些领域提供高安全性的量子安全保障。全球多地也正积极推进量子密钥分发网络的建设，聚焦于提升网络的安全性、集约化和规模化发展。

然而，目前量子保密通信的应用也存在一定的制约。

- 量子保密通信涉及量子态的制备、传输和探测等复杂技术，为达到高纯度量子态，需不断探索和使用新型材料与先进工艺，这都增加了研发成本。为此，应持续增加对量子通信技术的研发投入，鼓励高校和科研机构开展基础研究和应用技术创新。
- 目前量子保密通信市场处于发展初期，主要集中于国家级项目等特定领域，普通商业和大众市场尚未大规模开启，导致设备产量低，无法通过大规模生产来降低单位成本。通过扩大市场规模，增加设备采购量和使用量，积极培育大众市场需求，开拓量子通信在除金融等已有应用领域之外的更多高价值商业领域的应用，有助于实现规模经济，从而降低单位成本。
- 量子保密通信基础设施建设投入大，且难以与现有的通信基础设施完全兼容，而有限的应用场景难以支撑这些成本的分摊。因此，推动量子通信基础设施与现有通信基础设施的融合发展至关重要，可鼓励不同企业和机构之间开展合作，从而实现基础设施的共建共享，提高资源利用效率，降低建设成本。

国防军事：解决传统加密技术的安全隐患

量子保密通信提供了理论上无法破解的加密保障。基于量子不可克隆原理和测不准原理，任何窃听行为都会导致量子态的改变，从而被通信双方察觉。这一特性使其成为军事通信的理想选择。传统加密通信无法察觉是否被窃听，而量子通信可以实时检测通信链路的安全性，一旦发现异常立即终止通信或更换密钥，确保军事机密的安全性。

在战略指挥通信领域，量子保密通信技术为最高军事指挥机构提供了绝对安全的通信保障。通过量子密钥分发网络，战略核武器指挥控制系统可以实现高度安全的指令传输，确保二次核打击能力的安全性和可靠性。在战术通信层面，量子保密通信技术已开始应用于野战部队的战术指挥系统，为战场实时通信提供安全保障。

军事侦察数据传输对安全性要求极高。量子保密通信技术为侦察卫星、预警机、无人机等侦察平台的数据传输提供了有效的解决方案。通过量子加密，侦察获得的高价值情报可以安全传输至指挥中心，极大降低了情报被截获和破译的风险。

全球军事强国正在加速量子通信技术的军事化应用。美国、中国、欧盟等都在积极推进量子通信网络的军事部署，量子卫星、量子雷达等新型装备不断涌现。特别是，量子通信技术与传统军事系统的融合正在深化。从指挥控制系统到武器装备平台，推动军事通信体系向更安全、更智能的方向发展。

量子保密通信技术不仅解决了当前军事通信的安全隐患，更为应对未来战争形态演变提供了技术支撑。随着量子通信技术的不断成熟和军事应用的深入推进，它将成为维护国家安全的核心技术之一，在国防军事领域发挥越来越重要的作用。

政务：从传统防御到全新安全架构的升级

随着数字政府建设的深入推进，政务数据泄露、网络攻击等风险日益加剧，量子保密通信凭借其物理原理级的安全性，为政务系统提供了防窃听、防篡改的终极解决方案，成为全球主要国家政务安全体系升级的关键技术方向。

电子政务数据安全传输。量子保密通信在政府跨部门数据共享中发挥关键作用。



中国
京沪干线

已实现中央部委与省级政府的量子加密公文传输，日均处理机密文件超5000份。

Bundesministerium für Bildung und Forschung

德国
联邦政府

欧盟“量子通信基础设施”（QCI）计划中，德国联邦政府率先将财政数据、人口普查信息通过量子信道传输，密钥分发速率达10Mbps，较传统方式提升3个数量级。

公民隐私保护升级。在个人敏感数据处理场景，量子技术构建新型防护体系。

MIC
Ministry of Internal Affairs and Communications

日本
总务省

于2023年启用量子加密的居民信息系统，采用“量子随机数+一次一密”方案，保护1.2亿公民的户籍、医疗数据。

Canada
canada revenue agency

加拿大
税务局

引入量子密钥分发技术，实现纳税人信息在75个地方分局间的安全流转，抵御了3次大规模网络攻击。

量子通信的实时监测特性重构政务安全架构。



建设的量子政务网通过量子态连续检测技术，在仁川智慧城市项目中成功识别并阻断147次中间人攻击，较传统IPS系统响应速度提升200毫秒。

量子安全认证技术解决政务系统身份伪造难题。



开发量子数字身份系统，利用量子纠缠态生成不可复制的数字证书，在莫斯科电子政务平台实现2000万用户的零信任认证，伪造攻击率下降至0.0003%。

量子保密通信正在重塑政务安全范式。从数据安全到系统可信，从技术防御到制度创新，量子技术为数字政府建设提供了物理定律级的安全保障。随着量子网络与5G、区块链等技术的深度融合，未来政务系统将实现从被动防御到主动免疫的跨越式发展。这场量子革命不仅关乎技术升级，更是国家治理能力现代化的战略支点，将在维护政府公信力、保障公民数字权利方面发挥不可替代的作用。

电信：从实验室走向实际应用

量子技术与电信等传统行业正加速融合。

电信行业对通信安全需求极高，量子随机数发生器在加密应用中的探索，有助于发现技术在实际应用中的问题并加以改进。

英国 Quantum Dice　英国 BT Group

一起探索将其量子随机数发生器用于电信领域的加密应用。BT集团的研发部门将使用Quantum Dice的VERTEX QD-1100设备来评估其长期性能和可靠性、硬件集成，并探索利用PCIe卡的自我认证能力作为安全应用的可信熵源。

技术平台推动量子密钥分发互操作，行业协同应对加密危机。

美国 IBM　英国 汇丰银行

澳大利亚 AP+　美国 PayPal

亚洲新兴支付协会（EPAA）宣布，在东盟范围内正式成立“量子安全密码学工作组”（WG-QSC），IBM、汇丰银行、AP+及PayPal已作为创始成员加入。该工作组将聚焦政策研究、监管建设和运营商业务流程，以推动量子安全加密技术的应用，从而强化支付系统的防护能力。

瑞士 IDQ　以色列 HEQA Security

巴塞罗那 LuxQuanta　德国 Quantum Optics Jena

意大利 ThinkQuantum

推出Clarion KX平台，实现多厂商量子密钥分发互操作，新增HEQA Security、LuxQuanta、Quantum Optics Jena和ThinkQuantum为生态合作伙伴。面对加密破解危机，平台支持混合量子密钥分发技术，助力企业、政府高效过渡到量子安全网络。

在实现远距离信息传输的征程中，传统电信基础设施与新兴量子加密技术的结合是关键突破点。



达成合作以加速加拿大下一代量子通信技术的发展。作为合作的一部分，Telus将为Photonic提供不列颠哥伦比亚省30公里长的专用光纤网络，用于测试日益复杂的量子网络，推进量子网络和量子密钥分发的关键能力，利用量子加密技术实现超安全、不可篡改的远距离信息传输。

在实现远距离信息传输的征程中，传统电信基础设施与新兴量子加密技术的结合是关键突破点。



合作将通过Telsy的量子密钥管理平台，在两个数据中心之间的大容量链路上进行量子安全视频会议，展示了在现有运营商网络上提供量子密钥分发安全连接服务的能力。

各国深耕基础设施建设，加固量子安全技术。

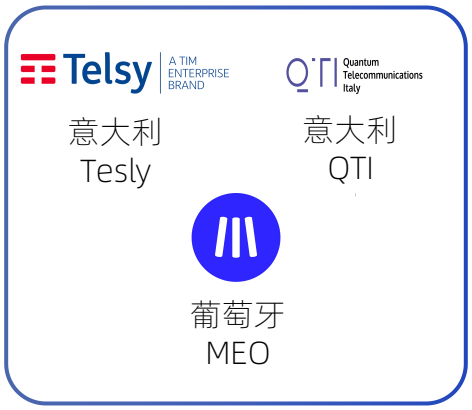


在量子安全新型基础设施领域，加速建设量子安全技术设施，例如，量子密钥分发网、量子密钥资源池、量子安全管理平台等，为各行各业的用户提供高效、安全的通信服务。试点测试量子技术，优化移动塔布局和网络安全，并为6G网络开发做准备。



合作试点测试量子技术。项目重点包括利用量子计算机优化移动塔位置，以提高网络效率，以及增强网络安全，特别是针对量子计算威胁的量子安全措施。

量子技术与传统通信网络的融合实践，使量子安全通信具备实际应用可行性，为电信网络安全升级提供方案，也为大规模商业应用奠定基础。



在里斯本实施了量子级安全通信链路，该项目旨在将先进的量子密钥分发解决方案深度集成到现有的电信网络之中。通过这种创新性的集成，能够从根本上增强电信网络中通信的安全性，为用户提供更加可靠、难以被破解的通信环境，从而在未来的通信领域中占据技术领先地位，推动整个行业的安全升级。

未来，电信运营商应用场景将多维度变革。在技术融合上，与量子技术深度整合趋势更明显；业务拓展方面，将以量子安全为核心开发增值服务；行业合作上，运营商会加强与各方协同，推动技术标准制定与基础设施建设，加速量子安全技术普及。

金融：多个协议技术领域同步推进

在金融市场预测与风险评估方面，量子计算结合量子通信可更高效处理数据、优化模型。

英国 Arqit　英国 Mastercard

达成协议，为金融机构提供数字资产安全和合规产品。Arqit的对称密钥协议平台有助于保护网络设备之间的通信链路，防止攻击，特别是来自量子计算机的攻击。Arqit WalletSecure（Arqit量子安全对称密钥协议技术的应用产品）有助于降低与私钥盗窃相关的风险，并阻止高风险交易的完成。

美国 Quantinuum　日本 Mitsui

日本 NEC

在东京成功通过10公里光纤网络传输量子令牌，这是全球首次使用商业量子密钥分发硬件实现量子令牌的传输，标志着在金融领域使用量子技术提升安全性的重要一步，有助于推动量子令牌在资产安全和高速交易等用例中的部署。

在密钥管理方面，量子密钥分发协议基于量子不可克隆、测不准原理，为金融数据传输加密，构建起理论上不可窃听破解的密钥通道，如在跨境转账指令传输加密中，确保交易指令准确、安全。

美国 摩根大通

实施了高速量子安全加密敏捷网络（Q-CAN），在已部署的光纤连接两个数据中心的基础上，建立了第三个量子节点，目前作为测试适用于银行和金融的下一代量子技术的研究平台。



签署了一份谅解备忘录，旨在全力开展量子安全合作。此次合作聚焦于深入研究量子密钥分发在金融服务领域的创新应用，力求通过量子密钥分发技术，为金融数据传输和存储构建起更为坚固的安全壁垒，抵御未来可能出现的量子计算破解风险，助力金融行业在数字时代实现更安全、更稳健的发展，为整个金融服务生态带来全新的安全变革。

身份认证方面，量子随机数发生器生成的真随机数，结合零知识证明等密码协议，为金融用户身份认证提供了更高级别的安全保障，有效降低账户被盗用风险。



在计划中的商业概念验证（PoC）中探索量子随机数发生器在金融蒙特卡罗模拟方面的优势。Quantum Dice的量子随机数发生器利用其独特的专利量子架构，以更好地再现蒙特卡罗模拟的基础分布，以更优化的方式对概率空间进行采样。

此外，量子保密通信技术与区块链协议的融合，为金融分布式账本带来优化，确保交易数据不可篡改，进一步增强金融体系信任机制，推动金融业务朝着更安全、高效的方向发展。



形成战略联盟，以利用量子技术革新区块链安全。该联盟结合了Krown在区块链和金融科技的专业知识与QeM的量子随机数发生器技术，旨在为数字资产领域提供更安全、可扩展的解决方案。

能源：共同探索商业化路径

能源行业作为国家经济命脉和民生保障的关键领域，其IT基础设施面临量子计算的潜在威胁。为应对这一挑战，部署量子安全网络成为保护水电与核电公司等关键能源基础设施IT系统的重要举措。

通过合作增强对演变的网络威胁的响应能力，确保关键能源基础设施的安全。

芬兰 诺基亚　　韩国 SK宽带

合作为韩国水电与核电公司部署了量子安全网络，以增强数据安全性。该网络利用量子安全的MACsec技术保护KHNP的IP MPLS租用线路网络，抵御现有和新兴的网络威胁，包括基于量子计算的网络攻击。

建立新合作组织，提升电网弹性与安全性，有利于加速量子技术商业化。

美国 epb　　美国 橡树岭国家实验室

在能源相关联合研究基础上，新的联合研究工作将侧重于利用查塔努加高度先进和综合的能源和通信基础设施来开发技术和最佳实践，提高国家电网的弹性和安全性，同时加速量子技术的商业化。

将量子技术与传统燃气表深度融合，为数据传输、指令交互提供不可破译的加密保障，吸引更多企业参与，完善产业链，促进量子安全技术在能源的创新应用。

中国 国盾量子　　中国 合燃华润燃气

中国 国网信通　　中国 南方电网

国盾量子携手国网信通、南方电网、合燃华润燃气等，打造出多个能源领域应用示范场景。公司2024年实现了量子通信技术在电力负荷管理系统、国家最高电压等级换流站等场景的首次应用；近千块量子安全物联网燃气表在合肥市成功挂表。

医疗：面向全生命周期数据深度加密

量子安全技术在医疗领域的应用，正从基础的网络安全防护，朝着医疗数据全生命周期的深度加密方向不断演进。

在数据传输环节，量子安全技术使得医疗数据在医疗机构内部流转、远程医疗开展以及不同医疗机构之间交互时，其保密性与完整性得以切实保障，为远程会诊、医疗影像传输等业务提供了坚实可靠的安全支撑。

此外，在数据存储领域，量子安全技术与存储系统的深度融合至关重要。它能够确保患者病历、基因数据等重要医疗信息在长期存储过程中的安全性，有效防止数据泄露与篡改，最大程度地维护患者隐私。

quantum emotion

加拿大
Quantum eMotion

达成基于云的Sentry-Q平台商业化的转折点，平台旨在解决现代远程医疗和数字医疗保健中未满足的关键网络安全挑战。该平台与相关技术共同为安全的数字医疗保健解决方案，设定了新标准，确保不同医疗保健系统的安全性、可靠性和可扩展性。

未来，随着医疗行业数字化转型的加速，对医疗数据安全的要求将愈发严苛，量子安全技术的应用将会促使医疗行业重新审视并完善安全标准与规范，推动整个行业在安全防护层面实现全面革新，从而为医疗行业的高质量发展奠定坚实的安全基础。

ICT：技术领先标准，发展错位

目前，产业界和学术界在量子保密通信与ICT（Information and Communication Technology）技术融合方面已取得多项实践成果。

在云平台技术融合方面，量子保密通信为云上数据安全提供了新解决方案。

中国
国科量子

与合作伙伴在OpenStack架构中集成了量子通信网络的加密系统，通过量子密钥分发和安全密钥管理策略，为云平台组件提供安全资源池。

日本
情报通信研究机构

日本
东京大学

提出了信息理论安全（ITS）的量子安全云系统，并通过互联网搭建该系统，为用户提供加密传输和量子安全分布式存储服务。

在物联网技术融合方面，量子通信在密钥协商过程中释放了原本用于密钥生成和身份认证的算力，增强了数据采集和传输的安全性。中国电信、中国联通等公司在多个物联网应用场景中，如智慧燃气、智慧城市、工业物联网等，提供了量子加密安全支持。欧美则更加注重量子保密通信对能效的影响.

英国
布里斯托大学

研究发现，引入量子保密通信后，相比传统本地生成密钥的方式，物联网设备的能耗显著降低，使用寿命延长了18%。

目前，在量子保密通信与ICT技术融合领域，虽已取得诸多实践成果，但技术与标准发展的错位问题突出。相关标准发展明显滞后，标准数量不足，难以全面规范各类融合技术应用。这种技术与标准的不平衡发展，制约了量子保密通信与ICT技术融合的进一步推广与深化，亟待加快标准制定，以匹配领先的技术发展步伐。

其他：创新性与个性化解决方案频出

在量子安全技术领域，还展现出了一系列创新性的发展方向以及个性化的解决方案。

在市场拓展方面，企业越来越注重多元渠道的开拓。通过与拥有广泛销售网络以及政府采购资源的伙伴合作，不断提升产品市场覆盖率和影响力，加速产品在不同行业的渗透。

ARQIT 英国 Arqit　carahsoft 英国 Carahsoft

按照协议，Carahsoft将借助其经销商合作伙伴，推广Arqit独特的对称密钥协议平台，助力其进入更多应用场景，满足不同行业的安全需求。

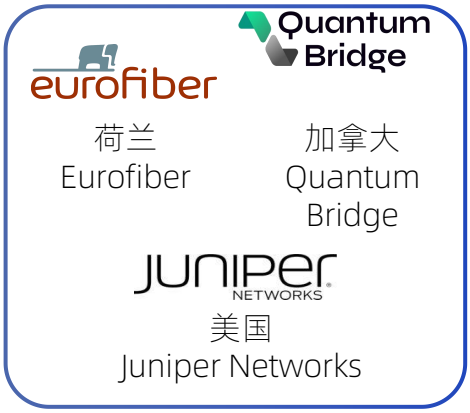
技术应用边界持续向外拓展，企业积极探索新兴领域的应用。以太空领域为例，量子安全技术与特殊场景需求深度融合，为行业安全防护提供了全新的解决方案。这不仅推动了量子安全技术在不同领域的深度融合与创新应用，也能更好地应对各行业日益增长的安全需求。

ARQIT 英国 Arqit

宣布Satellite Applications Catapult成功试部署Arqit的网络安全产品。该产品专为太空领域打造，旨在充分利用卫星技术提升安全防护能力。

aliro 英国 Aliro

为解决量子网络部署与管理复杂的难题，推出AliroNet® Quickstart Network——一套集量子网络硬件与综合软件为一体的解决方案，通过提供编排、控制和数据平面操作的一体化工具，大幅简化量子网络的部署与管理流程。



在安全解决方案创新上，建立战略合作关系，共同强化量子安全基础设施解决方案。此次合作将Quantum Bridge的分布式对称密钥建立（DSKE）技术与Juniper Networks的SRX防火墙相结合，为Eurofiber网络中的组织提供不依赖传统易受量子攻击的非对称加密的安全方案，从而提供更高效的量子安全通信解决方案和扩展的安全数据传输能力。

05 标准化工作进展

目前，由于缺乏统一的行业标准，不同企业的研发方向和技术路线存在差异，难以形成规模效应和协同创新，导致重复研发，浪费资源，推高了整体研发成本。未来，政府、行业协会等应牵头制定量子通信行业标准和规范，统一技术指标和接口要求，引导企业聚焦关键技术和共性问题，避免重复研发，促进产业协同发展，提高研发效率，降低整体成本。



政府推动量子通信标准化，支持量子技术标准试点网络

全球各主要国家政府认为，目前对量子技术制定法规为时尚早，但需采取持续行动以增强监管能力，确保监管促进量子技术的发展，同时保护国家安全和公众利益。

英国政府回应了监管地平线委员会关于量子技术监管的建议，强调了在量子技术发展初期实施适时监管的必要性。英国政府回应表示，支持RHC的建议，包括建立量子技术监管论坛、提供监管预见性方法、为政策制定者和监管者提供量子技术培训等。

此外，部分国家政府还将支持建设量子技术标准试点网络，推动量子通信标准化，并与量子通信专家合作，确保在量子密钥分发研究和开发方面的领先地位。

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

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》

2024.03

中国计量科学研究院、中国科学技术大学、国盾量子等产学研各方参与

中国国家市场监督管理总局、国家标准化管理委员会

- 批准发布7项量子信息领域国家标准
- 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》

2024.07

中国通信标准化协会牵头

国科量子牵头，联合国盾量子、新加坡国立大学共同制定

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》

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

2024.09

美国国家标准与技术研究所

- 西班牙Quside的量子熵源已获得SP800-90B认证

2024.11

中国工业和信息化部

- 发布公告，其中6项涉及量子密钥分发领域

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》



03

抗量子密码

目录 03 抗量子密码

01 抗量子密码算法

02 关键技术与抗量子密码芯片

03 抗量子密码迁移计划

04 应用场景分析

05 标准化工作进展

01 抗量子密码算法

抗量子密码学算法主要分为四大类，每类在安全性、效率和资源消耗方面各有优缺点。未来的研究方向包括提高安全性、优化性能、实现标准化和互操作性，同时开发备份方案。

图表 抗量子密码算法分类及简介

类别	算法简介
基于格的算法	• 算法原理方面，CRYSTALS-Kyber是一种具有较高安全性的密码算法，其核心基于模块化格（Module Lattice）和基于学习带噪声（LWE）问题。 • 数字签名方面，FALCON算法基于结构性同余系统（SIS）问题及其相关的陷门函数，提供更紧密的安全性证明，但其效率较低，因此不适用于计算资源有限的设备。
基于编码的算法	• BIKE算法通过FO变换实现了IND-CCA安全性，每次密钥交换时生成新的公私钥对，确保公私钥的独特性。 • Classic McEliece算法基于Niederreiter框架，具有较高的安全性，但由于其公钥较大，生成速度较慢，因此存在一定的实用性挑战。 • HQC算法在公钥和密文的长度上优于BIKE，并且具有较快的密钥对生成和解密速度，进一步实现了IND-CPA和IND-CCA2安全性。
基于多变量的算法	• MQ（Multivariate Quadratic）问题算法：以多变量二次方程组求解困难为基础。如HFE（Hidden Field Equation）算法，通过在有限域上构建隐藏结构的多变量多项式方程组，增加破解难度。 • 签名算法：如Rainbow签名算法，它基于HFE改进，引入多层结构，提升签名效率和安全性，签名长度短、验证速度快。 • 密钥交换算法：像UOV（Unbalanced Oil and Vinegar）算法，利用油变量和醋变量的不平衡性设计密钥交换机制，在抗量子攻击方面有独特优势。
基于哈希函数的算法	• 一次性签名方案（One Time Signature，OTS）通过将消息分割成多个段，并为每个段生成签名来减少密钥对的大小，确保安全性。 • 几次签名方案（Few Times Signature，FTS）允许每对密钥签名固定次数的消息。 • 多次签名方案（Many-time Signature，MTS）则允许签署多次消息，但每次签名后需要更新状态以确保安全性。尽管多次签名方案提供更大的灵活性，但也增加了实现的复杂度。

2024年8月，美国国家标准与技术研究院（NIST）正式发布三项抗量子密码算法标准，包括基于格密码的ML-KEM（FIPS 203，原Kyber）、ML-DSA（FIPS 204，原Dilithium）以及基于哈希签名的SLH-DSA（FIPS 205，原SPHINCS+）。这些算法覆盖了密钥封装、数字签名等核心功能，为全球抗量子密码迁移提供了技术基准。

欧盟、韩国、日本等国家加速跟进，例如，韩国在2024年采纳抗量子密码应用规范，计划在开放量子测试平台实施；德国则评估FrodoKEM和Classic McEliece等其他算法。中国虽未发布国家标准，但清华大学、中科院信工所等机构积极参与国际标准化工作，并推动自主算法（如基于NTRU和SM3的算法）研究。

02 关键技术与抗量子密码芯片

高效硬件实现技术：平衡硬件性能

抗量子密码算法主要涉及模运算、系数生成等核心算子，核心计算操作有多项式、矩阵和向量间的模加、模减及模乘运算。核心算子硬件实现效果对整个抗量子密码系统的资源消耗和运算性能影响显著。

在信息安全领域，鉴于应用场景多样、开发需通用且安全级别需求多元，硬件实现抗量子密码方案核心算子时，要全面权衡功耗、性能与面积。既要优化硬件资源消耗，确保一定运算性能，避免追求高性能时的资源浪费，又要在电路设计中引入低功耗技术，实现特定场景下硬件实现效率最大化。

动态可重构技术：匹配运算差异

研究不同抗量子密码算法方案核心运算的计算方式与特点，针对算法加解密中的关键运算特征，如基本数据位宽、向量基元长度、迭代运算次数以及计算属性等，设计可配置数据位宽、计算规模与计算方式的可重构抗量子密码的核心计算单元。

在芯片架构层面，探索支持多种算法协议的可重构架构，深入研究哈希、采样、多项式、数论变换及模乘等运算关键步骤，尤其针对差异化的高效多项式乘法器和高速可配置哈希硬件，进行实现技术探究与方案创新，提升抗量子密码安全芯片的灵活性与适配性，以应对复杂应用场景需求。

侧信道攻击防御技术：优化抗击能力

抗量子密码算法通过芯片、程序等实现后，采样、模运算等核心算子运行时会经计算时间、功耗和电磁等侧信道泄漏敏感信息，算法漏洞攻击也具极大破坏力。

为解决上述问题，可以从以下两方面着手。算法层面，改进优化易受侧信道攻击的核心算子以降低信息泄露风险。硬件实现方面，深入分析各功能模块工作原理和可能面临的侧信道攻击类型，重点关注密钥参与计算的解密模块，设计抗侧信道攻击的电路结构，提升系统抵御能力。

安全SoC集成技术：实现标准合规

具有多种功能的片上系统（System on Chip,SoC）需更全面安全防护。聚焦融合多种技术的抗量子密码安全IP，将其与SoC内其他电路及功能模块有机整合，平衡芯片性能、功耗、稳定性与安全性，找准高集成度设计与低功耗方案的最优均衡点。

在此基础上，探索SoC参与安全认证及实际应用流程，实现抗量子密码算法在各类认证协议中的替代与兼容，通过安全身份认证应用示范，推动其对传统安全芯片的替代进程。美国QuSecureD的QuProtect软件解决方案已达到SOC 1和SOC 2 Type 2合规性，验证了其行业抗量子密码解决方案对其内部安全控制和实践的严格、独立评估。QuProtect软件提供全面的量子安全即服务架构，结合零信任和下一代量子弹性技术，保护网络、云系统、边缘设备和卫星通信免受当前和未来的网络攻击及量子威胁，同时对现有系统的干扰最小。

多种困难问题密码算法：探索新的方向

基于不同困难问题的密码算法在当前研究和评估中被认为安全，但并非绝对。

抗量子密码芯片设计依据多样化应用场景，朝着差异化性能方向深度发展

信息化时代，信息在端点或中继加密后汇聚至云服务器和高算力数据中心，经解密处理后再次加密传输至设备。不同应用场景对抗量子密码芯片设计需求各异，面向资源受限环境的低功耗芯片和面向云服务器与数据中心的高性能芯片是两大代表性方向。

低功耗抗量子密码芯片聚焦抗量子密码系统，适配更多资源受限的终端设备

基于格的抗量子密码是轻量化优选，其系统中的采样与多项式运算是高能耗核心计算，常从这两部分进行低功耗与低资源开销优化。采样的低功耗设计需提高效率，采用耦合紧凑硬件结构；多项式运算优化则多通过算法改进和提高存储利用率。

高性能抗量子密码芯片发展多任务调度技术，提升运行频率与吞吐率

网络服务器中用户数据加密、数字签名与验证大量高速重复，要求芯片高性能、高频运行和高吞吐率。应用中，攻击者手段多样，对芯片防御强度挑战增大，多元侧信道攻击防御机制研究成为重要领域。面向关键信息基础设施的高性能计算需求，开展算法、架构到电路的多层次高性能实现和侧信道防护是未来芯片设计重要方向，具有动态监测和安全感知的抗侧信道攻击防护技术也将是研究重点。

此外，针对资源敏感场景，低功耗抗量子密码SoC研究在物联网领域有应用价值，研究设计更多基于不同困难问题的密码算法很有必要，如基于椭圆曲线同源或量子随机漫步的算法。中国清华大学陈一镭提出破解格密码的量子算法引发关注，尽管该算法的有效性仍需密码学界进行深入评估与验证，然而，其对抗量子密码算法安全性构成的潜在挑战，已经促使各方重新审视和加强抗量子密码体系的安全性研究。

03 抗量子密码迁移计划

随着量子计算的发展，传统密码面临着被破解的风险，数据安全受到严重威胁。其时间紧迫性极高，一旦量子计算能力达到能够破解传统密码的水平，未迁移的系统将面临巨大的安全风险。

由于金融、政府、军事等领域数据涉及重大利益与国家安全，所以应优先迁移。迁移方式主要有逐步替换，即分阶段将传统密码算法替换为抗量子密码算法；也可采用双栈并行，在一段时间内同时运行传统与抗量子密码体系，实现平稳过渡；还可采用混合加密方式，将抗量子密码算法与传统密码算法结合使用，增强安全性。

抗量子密码的迁移技术需要具备灵活性设计，实现抽象化、模块化、配置化。在系统架构中引入抽象层，并将加密功能设计为独立的模块，通过配置文件或参数来指定使用的具体密码算法。同时，还需要考虑抗量子密码算法与现有系统的兼容性以及性能开销等问题。

开展抗量子密码升级迁移这一复杂系统工程，大致可分为三个主要阶段：

- 迁移需求分析：精准明确信息系统标准、软硬件模块、密钥管理软件和代码等方面的抗量子密码升级需求，梳理迁移清单。针对清单深入分析算法性能、带宽、存储等技术需求，研究算法替换与补偿方案。
- 升级方案制定：依据需求清单，剖析不同信息系统安全生命周期和迁移优先级，为不同系统制定详尽迁移实施方案。设立示范应用项目，为信息系统使用方提供技术产品支持与迁移指导。
- 示范应用推广：根据抗量子密码在重点行业领域升级迁移的示范应用成效与问题，稳步推动其他相关行业领域的信息安全系统迁移，实现各行业抗量子密码整体升级。

尽管2024年抗量子密码技术领域的迁移取得一定进展，但仍面临诸多挑战。随着量子计算的快速发展，传统加密方法面临越来越多的漏洞，各国认识到迫切需要量子抗性解决方案来保护敏感数据和关键系统，都纷纷开始开展抗量子密码的迁移计划。



美国：
在标准的指导下稳步推进，但整体迁移工作仍有滞后

美国网络安全和基础设施安全局（CISA）、国家安全局（NSA）与美国NIST等机构陆续发布《量子计算网络安全方案法案》、《量子准备：向抗量子密码学迁移》指南、《向抗量子密码学迁移》项目情况说明书等配套文件。这些文件从技术选型、实施步骤、风险评估等多方面，为各组织着手开展抗量子密码迁移工作提供了详细指导，要求2035年前完成联邦系统的抗量子密码迁移，也为企业提供分阶段迁移策略。

在企业实践方面，美国苹果公司宣布对其iMessage通讯平台进行升级，此次升级采用PQ3加密技术，PQ3协议预计将在2024年内完全替代现有的对话协议。美国超威半导体公司推出支持抗量子密码算法的FPGA SoC产品“SpartanUltraScale+”。在抗量子密码升级迁移和应用的初期阶段，加密应用供应商普遍采用传统公钥加密算法和抗量子密码算法并用的“两把锁、双保险”混合加密模式进行迁移，未来逐步过渡到仅使用抗量子密码算法加密模式。

在资金规划上，美国白宫发布了一份《抗量子密码学报告》。报告概述了美联邦政府为应对未来可能遭受的与密码分析相关的量子计算机（CRQC）攻击所采取的策略，并估计到2035年联邦机构向抗量子密码学过渡将花费71亿美元以上的资金。

为深入了解迁移情况，美国Entrust网络安全研究所与Ponemon研究所发布《2024年PKI和抗量子趋势研究》，针对九个国家和地区的IT安全从业者对公钥基础设施（PKI）实践和抗量子准备情况进行了调查。结果显示，这些组织管理着多种不同应用的PKI，如电子邮件和网络认证。多数受访者表示组织正在为量子威胁做准备，并计划在未来五年内迁移到抗量子密码学，但总体而言准备工作较为滞后。



英国：
发布指南，为迁移做好准备

在全球积极探索抗量子密码学的大背景下，英国在推动抗量子密码迁移方面迈出了坚实且具有引领性的步伐。

英国依据抗量子密码指南，指导组织迁移。英国国家网络安全中心（NCSC）发布了《为抗量子密码学做准备的后续步骤》指南的2.0版本。该指南针对不同领域的组织需求进行了深入剖析与规划，可帮助商业企业、公共部门组织和关键国家基础设施中的系统和风险所有者思考如何为向抗量子密码学迁移做好最佳准备。

英国国家网络安全中心通过发布这一指南，为各类组织提供了清晰且实用的行动路线图，助力其在信息安全领域积极应对抗量子时代的挑战。这种前瞻性的举措不仅体现了英国在网络安全领域的领先意识，也为全球其他国家和地区在推动抗量子密码迁移方面提供了宝贵的参考范例。



瑞士：
成立实验室，为迁移提供支持

瑞士成立实验室，并加强与高校院所合作，利用学术优势加速抗量子密码技术的进步。瑞士SEALSQ扩展其研发部门，成立SEALQUANTUM.com实验室，以开拓量子安全加密和抗量子研究。实验室不仅提供教育平台，还是研发量子安全密码学的有力支撑，为企业提供专业知识、实时洞察和指导。SEALSQ的抗量子技术产品包括抗量子密码算法和抗量子芯片，与Mines Saint-Étienne等机构合作开发，确保行业能够有准备地过渡到抗量子时代。

瑞士还与相关组织合作创建量子安全金融论坛，汇聚多方力量，推动金融向抗量子密码过渡。欧洲刑警组织的欧洲网络犯罪中心与EC3金融服务咨询小组密切合作，创建了量子安全金融论坛（QSFF）。QSFF是一项多方利益相关者的努力，旨在解决整个金融部门向抗量子密码的过渡问题，特别关注欧洲，其成员由来自欧盟、英国和美国几家主要商业和中央银行、其他金融服务提供商、协会和专家的专家组成。



中国：多方入局，迁移一触即发

2024年，中国在抗量子密码迁移计划方面呈现出全方位积极推进的态势。

在技术研发上，高校和科研机构成为主力军，数学算法和硬件融合两条技术路线并行发展，不断探索新型抗量子密码算法，加强与硬件的适配性，迈出技术应用重要一步。

标准制定进程加速，通过举办各类研讨会，围绕前沿技术、研究动态及发展趋势进行探讨，推动抗量子密码标准的设立与应用实施。此外，中国积极参与国际标准制定，力求在全球抗量子密码标准体系中占据一席之地。

产业生态逐渐成型，企业开始布局抗量子密码相关业务，产业链上下游合作不断加强，有望在未来几年形成涵盖技术研发、产品生产、系统集成和服务支持的完整产业生态。如复旦大学与格尔软件合作成立“后量子密码技术校企联合研究中心”，聚焦算法设计与硬件实现；中国科学技术大学、国盾量子等团队完成“量子密钥分发+抗量子密码”融合方案的现网验证，为量子通信与经典密码结合提供范例。

尽管在国家层面，中国尚未出台明确法案支持抗量子密码迁移，但随着行业关注度提升，相关政策有望逐步落地，为迁移计划提供政策保障和引导。

总体来说，抗量子密码升级迁移是一项长期系统性工程，从算法标准走向产品应用，需开展大量产品级和系统级的研究开发、测试验证与更新适配工作，明确密钥、密文和签名参数设置，以及计算处理和故障处理等能力要求，完成与目标系统架构和环境的适配与升级。

04 应用场景分析

虽然抗量子密码研究，在2024年算法评估和标准化进程中取得初步进展，但由于量子计算硬件性能突破和潜在破解算法的研究仍存在诸多不确定性，业界对于现有抗量子密码算法在未来成熟量子计算机攻击下的安全性仍存顾虑。

美国NIST在标准化过程中广泛选取多种算法方案并持续征集评估，既满足了不同应用场景在计算资源、安全级别上的灵活性需求，也分散了风险，提升整体安全性，避免单一算法被破解导致整个密码体系失效。

从实际应用场景来看，这种谨慎和全面的标准化策略意义重大。运营商为保障通信网络安全，已抢先接入抗量子密码安全服务，防止通信数据被窃取或篡改。金融行业因其业务对安全性和稳定性要求极高，提前部署抗量子密码技术，预防量子计算可能带来的潜在风险，保障客户资金和交易信息安全。

抗量子密码与量子密钥分发的结合，实现了优势互补，极大增强了量子安全防护能力，可应用于对保密要求极高的军事通信、政府机密传输等场景。抗量子密码搭配量子随机数发生器，开创了抗量子算法新模式，为数据加密、身份认证等领域提供更可靠的安全保障，在物联网设备安全、区块链加密等场景中展现出巨大应用潜力。

由此可见，对抗量子密码算法安全性的评估和验证工作，将贯穿抗量子密码迁移与应用的全生命周期，成为一项长期且至关重要的任务。随着各行业对量子安全重视程度不断提高，抗量子密码技术在不同场景下的应用将持续拓展和深化，为数字世界筑牢安全基石。

电信：抢先接入抗量子密码安全服务

电信运营商推出量子安全产品，提供抗量子密码的按需服务。

日本
东芝

韩国
KT公司

在韩国的量子安全通信领域展示了如何通过引入量子密钥分发和抗量子加密，来保护银行和金融网络免受量子计算机的网络攻击，这种混合量子安全通信的方式已经应用于韩国领先银行之一的新韩银行。

意大利
Sparkle

预售量子安全产品，这是该公司网络即服务套件中的第一款产品。该产品已经通过了测试，能够为企业提供符合MEF标准的、采用抗量子加密技术的按需接入服务。目前，法国、希腊和英国的企业已经可以订购并开始测试这项量子安全连接服务。

中国
中国电信

在量子通信领域持续发力，推动行业发展。不仅搭建融合量子密钥分发的分布式密码系统架构，打破传统密码体系的局限，实现了密码技术的升级换代。同时，构建起量子密钥分发、抗量子密码与经典密码深度融合的新型密码体系，将不同密码技术的优势有机结合，极大增强了通信的安全性与可靠性。

金融：提前部署预防潜在风险

金融等核心数据资产机构将加快抗量子密码评估和相关部署。金融机构由于业务涉及大量资金流转、客户敏感信息存储以及众多复杂金融交易，面临的网络安全挑战极为严峻，一旦遭受攻击，损失巨大。

因此，相较于其他行业，金融、政务等机构更可能更早采取措施为新的加密系统过渡做准备。这些机构需要全面评估量子计算机带来的未来风险和潜在追溯风险，清点自身使用的加密算法（尤其是公钥），建立加密敏捷性，从而提高整体网络安全弹性，确保核心数据资产安全。

为推动金融机构构建应对量子威胁的密码灵活性策略，相关机构积极行动。

新加坡
金融管理局

发布了一份关于抗量子密码迁移的指导建议，旨在敦促该国的金融机构为迎接量子计算时代的网络安全威胁做好充分准备，确保整个金融体系在技术升级的过程中保持高度的安全性和韧性。全球金融服务信息共享分析中心FS-ISAC发布白皮书《Building Cryptographic Agility in the Financial Sector（构建金融领域的密码灵活性）》，该白皮书旨在构建密码灵活性以应对量子计算带来的威胁。

在保障数字资产和金融通信安全实践中，各机构积极试验量子安全技术。

英国
汇丰银行

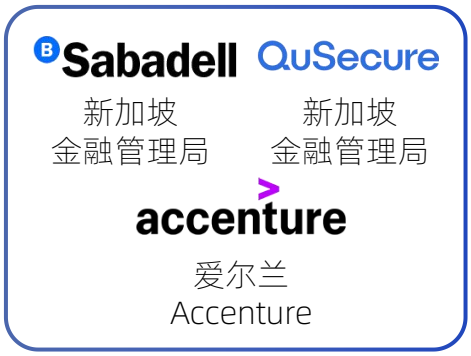
成功试验了量子安全技术应用，用于购买和销售代币化实物黄金。此次试点项目中，汇丰银行还测试了使用抗量子密码的黄金代币的互操作性，通过安全网络在分布式账本间安全转移数字资产。



新加坡
金融管理局

法国
法兰西银行

试用抗量子密码学来保护金融通信。这次联合实验利用抗量子密码算法以及当前的算法来签署和加密电子邮件。



新加坡
金融管理局

新加坡
金融管理局

爱尔兰
Accenture

通过将QuSecure先进的抗量子密码技术融入Banco Sabadell现有的系统架构，借助Accenture专业的技术整合与实施能力，探索抗量子密码技术在该银行基础设施中的采用，以增强其量子安全基础设施。

在算法优化与拓展方面，抗量子密码算法虽具备抵抗量子攻击的安全性优势，但在实用性上存在短板，如密钥尺度大，导致存储和传输成本增加，加解密签名效率低，影响业务处理速度。



美国
KeySight

首创抗量子密码测试功能，提供算法安全验证。Keysight将提供必要的测试工具和认证服务，以支持抗量子密码算法的标准化和应用。通过集成抗量子算法扩展生态系统，提升数据安全技术水平。



瑞士
Terra Quantum

推出开源的抗量子密码学库TQ42 Cryptography，通过抗量子算法扩展其量子即服务生态系统，以实现数据安全。该库支持多种应用，如智能家居系统、Wi-Fi和区块链安全，以及实现信息共享的完美前向保密性。

抗量子密码+量子密钥分发：增强量子安全防护

面对全面纠错量子计算机的潜在威胁，传统密码体系在抵御量子计算攻击时存在明显的脆弱性。而量子密钥分发和抗量子密码作为量子安全技术的关键组成部分，为数据安全提供了强大的防护能力。

量子密钥分发因其能够提供理论上绝对安全的密钥传输，因此适合保护高价值资产，如骨干网络；而抗量子密码则适用于广泛的信息基础设施，可在常规计算资源下实现对大量数据的加密保护。由于不同应用场景对安全防护的需求各有差异，要实现向量子安全体系的平稳过渡，需要融合抗量子密码技术与量子密钥分发技术，而单一技术或将难以满足未来所有场景。

欧洲E2EQSS项目旨在纳入抗量子密码，以促进为未来卫星群明确定制的量子密钥分发。项目通过无缝集成空间和地面组件，应对量子计算威胁。

瑞士
ID Quantique

引入量子随机数发生器芯片技术，这是加密和保护数据传输的关键组件。IDQ的芯片符合ECSS-Q-ST-60-13标准，服务于需要在空间中使用辐射硬化或辐射耐受设备的整个任务配置文件。

新加坡
SpeQtral

西班牙
Arquimea

通过谅解备忘录合作，合作领域包括探索与BeetleSat星座兼容的潜在量子安全解决方案，以及探索欧洲和亚太地区的联合商机，调查洲际量子密钥分发服务。利用其协同效应，两家公司将探索SpeQtral的天基量子密钥分发解决方案和Arquimea的抗量子密码技术的集成，以加强BeetleSat的点对点通信与量子安全。

新加坡
金融管理局

宣布将在金融部门技术与创新补助计划下投入1亿新元（约7449万美元）以提高该国金融机构开发量子和人工智能技术的能力，并推动这两项技术的相关创新和在金融服务领域的采用。其中有高达30%的资金将用于支持与量子安全技术相关的试点项目和开发工作。

美国
量子经济发展联盟

发布研究报告，探讨量子技术在金融信息传递中的应用，强调量子计算对现有加密的威胁。报告提出抗量子密码学和量子密钥分发作为解决方案，并推荐金融业试用量子密钥分发技术、实施抗量子密码标准、探索量子密钥分发与抗量子密码的结合方法等，以增强金融通信的安全性。

日本
东芝数字解决方案公司

新加坡
SpeQtral

新加坡
ST Engineering

签署了谅解备忘录，正式建立战略联盟，加强在新加坡和东南亚市场的量子安全通信解决方案推广。根据备忘录协议，三方将在各种战略举措上进行合作，以推进混合了量子密钥分发和抗量子密码学技术的量子安全通信、量子安全数据存储等解决方案在这些市场的应用。

韩国
KT公司

完成混合量子安全虚拟专用网络（VPN）服务演示。此次量子安全演示网络将VPN技术与传输网络相结合。VPN技术结合了抗量子密码学，即使是量子计算机也无法解密。KT使用量子加密保护传输网络，并通过量子安全VPN保护两个省之间交换的空间信息数据。

未来，有机结合量子密钥分发和抗量子密码的优势，从密钥生成、传输到数据加密全过程构建多层次的安全防护体系，长期来看，可能是实现量子安全的最有效策略。

抗量子密码+量子随机数发生器：抗量子算法新模式

2024年，全球多家企业如韩国SKT的X-Quantum联盟以及加拿大BTQ Technologies和瑞士ID Quantique合作，推出集成抗量子加密和量子随机数发生器的量子密码芯片，标志着量子安全技术在加密领域的生态扩展。

韩国
X-Quantum

组成的量子联盟“X-Quantum”推出了商业产品“Q-HSM”量子密码芯片。芯片集成了抗量子加密技术和量子随机数发生器，是全球首款同时搭载这两种技术的量子芯片。Q-HSM利用量子特性生成不可预测的随机数以制造强加密密钥，并防护现有加密体系面临的量子计算威胁。SKT计划将其应用于无人机、CCTV、家庭网络和IoT设备等，进一步扩展量子技术生态。

加拿大
BTQ
Technologies

瑞士
ID Quantique

签署了一份谅解备忘录，共同开发一种结合了量子随机数发生器和抗量子密码学的创新身份验证系统。

西班牙
Quside

英国
PQShield

将Quside的量子随机数发生器与PQShield的抗量子密码加密解决方案集成，为各行各业创建量子安全解决方案。该集成解决方案将Quside的随机性与OpenSSL3.2+环境中的PQShield加密原语相结合，可以在减少应用程序更改的基础上支持客户更便捷地采用量子安全加密技术。

全球量子安全技术领域呈现出抗量子密码与量子随机数发生器融合发展的态势。量子安全技术将在加密领域生态将不断拓展，技术集成注重减少应用程序更改，让量子安全加密技术更易被用户采用，加速在各行业普及，同时不断完善创新抗量子密码技术，寻求新模式的融合。

05 标准化工作进展

全球抗量子密码标准化工作正稳步且全力推进，其关键目标是保障不同厂商抗量子密码方案之间具备良好的互操作性，同时确保安全性达到高标准，以此大力推动抗量子密码技术的商业化应用以及广泛普及。

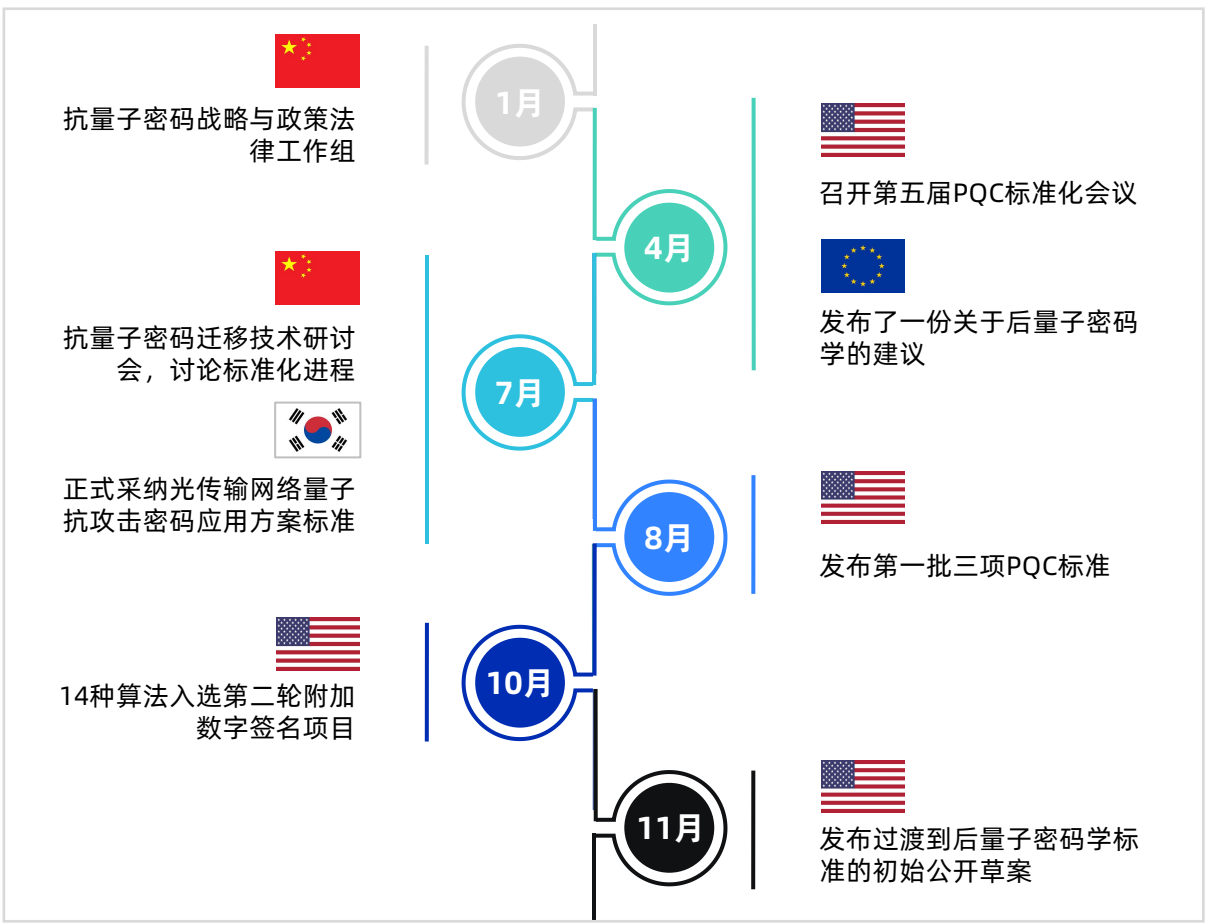
美国NIST发布了全球首批三个抗量子加密标准。

英国通过国家网络安全中心（NCSC）等机构，组织国内科研力量参与抗量子密码算法研究与标准制定讨论，推动相关技术在本土的合规应用。

韩国则大力支持高校和科研机构开展抗量子密码技术研究，在哈希函数类抗量子密码算法研究方面取得一定成果，并积极与国际接轨，参与国际标准的研讨与制定。

中国同样在积极行动，一方面组织本国专家深入研究抗量子密码算法，在格密码、基于编码的密码等方向取得多项理论突破；另一方面，通过举办国际学术会议、参与国际标准组织活动等方式，积极参与抗量子密码国际标准制定，同时推动本国相关技术标准的设立，为抗量子密码技术的落地应用奠定基础。

图表 2024全球抗量子密码标准化工作进展





美国：技术规范与时间表逐步明晰

自2016年启动抗量子密码标准化项目以来，历经多轮严格的算法征集和评审。2024年，美国NIST发布了全球首批三个抗量子加密标准，分别为ML-KEM（一种密钥封装机制，为通信双方提供安全的密钥协商方式）、ML-DSA（基于特定数学原理的数字签名算法，用于确保数据来源的真实性和完整性）和SLH-DSA（具备独特优势的数字签名算法，在签名验证效率和安全性上有良好表现），不仅为全球抗量子密码技术应用提供了规范依据，更标志着抗量子密码技术从探索起步阶段迈向快速发展的成长期。

8月，美国国家标准与技术研究院发布了三种抗量子加密算法的联邦信息处理标准（FIPS）出版物。NIST已经发布了全球首批抗量子密码标准，分别是ML-KEM（基于CRYSTALS-Kyber）、ML-DSA（基于CRYSTALS-Dilithium）和SLH-DSA（基于SPHINCS+），以加强量子时代的现代公钥加密基础设施。

10月，美国NIST宣布，在经过一年多的评估后，有14种算法入选抗量子密码学标准化流程的第二轮附加数字签名项目。这些算法分别为：CROSS、FAEST、HAWK、LESS、MAYO、Mirath（MIRA/MiRitH合并）、MQOM、PERK、QR-UOV、RYDE、SDitH、SNOVA、SQIsign和UOV。NIST内部报告IR 8528详细描述了评估标准和选择过程，第二轮候选人将有机会提交更新的规范并进行调整，评估和审查预计将持续12至18个月。

11月，美国NIST发布了过渡到抗量子密码学标准的初始公开草案（《Transition to Post-Quantum Cryptography Standards》），包含迁移的路线与时间表。NIST希望到2035年将政府机构的加密系统转变为抗量子加密。根据草案，NIST将在2030年前弃用112位及以下安全强度的加密算法，并于2035年前禁用这些算法。这份路线图标志着NIST迈向管理和指导向抗量子密码学过渡的更广泛战略的第一步。

图表 美国NIST主导的抗量子密码项目时间线概览

2016	2016.02	2016.04	2016.12	
	NIST在PQCrypto2016上发表演讲：NIST征集公告和大纲	NIST发布PQC报告	NIST发布PQC正式征集提案	
2017	2017.11	2017.12		
	NIST在PQCrypto2016上发表演讲：NIST征集公告和大纲	第一轮PQC算法征集结果公布，共69份算法		
2018	2018.04			
	第一届PQC标准化会议召开			
2019	2019.01	2019.03	2019.08	
	第二轮候选人公布，共26份算法	第二轮更新提交包截止	第二届PQC标准化会议召开	
2020	2020.07	2020.10		
	第三轮候选人公布，7名“入围者”，8名“候选者”	第三轮更新提交包截止		
2021	2021.06			
	第三届PQC标准化会议召开			
2022	2022.07	2022.10	2022.11	
	标准化候选人及第四轮候选人公布	第四轮更新提交包截止	第四届PQC标准化会议召开	
2023	2023.08			
	发布三份FISP草案以征求公众意见			
2024	2024.04	2024.08	2024.10	2024.11
	召开第五届PQC标准化会议	发布第一批三项PQC标准	14种算法入选第二轮附加数字签名项目	发布过渡到抗量子密码学标准的初始公开草案
Further	2025			

光子盒研究院 QUANTUMCHINA | 2025.2



欧盟：
推动成员国共建抗量子密码标准

欧盟正积极推动成员国共建抗量子密码标准，以保障数字基础设施和服务的安全，维护欧盟的数字主权和竞争力。4月，欧盟委员会发布了一份关于抗量子密码学的建议，旨在推动成员国制定和实施协调一致的路线图，以使欧盟在向抗量子密码学过渡时能保障数字基础设施和服务的安全。此外，欧盟还鼓励成员国加强国际合作，参与国际标准制定，并加大对抗量子密码研发的投入，支持学术界和产业界合作，推动创新解决方案的开发和应用。



韩国：
首次发布通信设备团体标准

韩国的标准制定预计将激活量子密码通信产业生态系统。这也是韩国通信行业首次制定的量子抗攻击密码应用标准，同时也是韩国首次针对量子抗攻击密码应用的通信设备的团体标准。7月，韩国运营商LG U+与韩国智能信息社会振兴院（NIA）共同提出的光传输网络量子抗攻击密码应用方案的标准草案，已于7月1日首次被韩国信息通信技术协会（TTA）正式采纳为标准。该标准名称为《光传输网络中量子抗攻击密码应用方案与框架》（Application Method and Framework for Post-Quantum Cryptography in Optical Transport Network）。该标准提出了光传输网络框架、引入量子抗攻击密码光传输网络设备的考虑事项、支持抗量子密码的通信网络设备的主要应用案例等内容。



中国：多方通过会议交流协同制定标准

中国目前开展抗量子密码研究的单位有两大类，一类是偏数学算法方面的，例如清华大学、复旦大学、上海交通大学等；另一类是偏硬件融合方面的，例如中国科学技术大学、国盾量子等。

此外，中国积极推动抗量子密码标准化工作，多次举办抗量子密码相关会议，强调抗量子密码产业发展的重要性，促进产业链上下游协同合作。虽然在国家层面尚未出台明确的法案或行动计划来支持抗量子密码的迁移工作，但标准化进程一直在有序推进。目前已完成多项基础研究工作，为后续标准制定奠定理论基础，同时积极参与国际抗量子密码标准的研讨与制定，在国际交流中提升话语权。

中国抗量子密码战略与政策法律工作组于2024年1月成立，该工作组致力于对抗量子密码技术、产业、业务的现状以及国内外相关政策、法律法规展开深入研究，并计划以公开或定向方式发表抗量子密码相关蓝皮书、要报、专题研究报告等成果，为中国制定相关政策和标准提供有力支撑。

7月，抗量子密码迁移技术研讨会在北京召开，会议围绕抗量子密码迁移的国内外标准化进程、技术路线、实施策略、抗量子密码迁移的优先级、技术与产业链的发展方向、实施推进等议题展开深度交流。会议达成多项重要共识，明确了以保障关键信息基础设施安全为首要目标，优先推进金融、政务等领域的抗量子密码迁移工作，为中国抗量子密码迁移和标准化工作指明了方向。

其他：
科技企业积极响应，助力国际标准成型

多家科技企业宣布采用美国NIST最新抗量子密码标准



美国微软参与了FrodoKEM、SIKE、Picnic、qTESLA这四个用于签名和密钥交互的抗量子密码项目的研究，抗量子密码库的开发和安全协议集成也是其重点投入的工作。

微软还发布了基于格密码库（LatticeCrypto）和项目抗量子密码rypto-VPN，并在OpenVPN中实现了抗量子密码算法，可在VPN中测试抗量子密码算法的功能和性能。

微软研究院与许多科技公司、大学以及研究机构进行抗量子密码学合作，共同开发了Supersingular Isogeny Key Encapsulation（SIKE）密钥交换协议的抗量子密钥封装机制。此外，共同开发了qTESLA抗量子数字签名方案，其安全性基于带错误的决策环学习（R-LWE）问题的硬度。

2024年9月，微软宣布已开始在其开源核心加密库SymCrypt中部署抗量子加密算法，其中包括ML-KEM和XMSS算法。



美国谷歌于2016年宣布涉足抗量子密码，在Chrome浏览器的Canary测试版本中使用名为New Hope的抗量子密钥交换算法进行实验，开展抗量子密码技术的测试活动，开始应用基于环上带误差学习问题密钥交换协议“新希望”。

2019年1月，谷歌宣布将部署一种新的TLS密钥交换方法，称为CECPQ2（组合椭圆曲线和抗量子密钥交换）。

2019年6月，谷歌和Cloudflare合作探索抗量子密码如何在实践中击败HTTPS连接。

2023年8月，谷歌开始在Chrome 116中采用新的抗量子加密技术X25519 Kyber768。

2024年9月，谷歌宣布更新其Chrome网络浏览器中的抗量子加密技术，用完全标准化的基于模块晶格密钥封装机制（ML-KEM，NIST首批抗量子密码标准之一）取代实验性的Kyber，以提升对量子计算潜在攻击的防御能力。

此外，谷歌母公司Alphabet剥离出来的量子技术开发部门成立了初创公司SandboxAQ，其主要研究目标之一是创建抗量子密码系统和相关的隐私增强技术。



美国IBM于2019年联合一些大学开发了新的量子安全算法，作为CRYSTALS格密码学套件的一部分，该算法已开源，并提交给NIST进行标准化。

同年，IBM已在IBM TS1160磁带驱动器原型上成功测试了CRYSTALS，该原型使用Kyber和Dilithium并结合对称AES-256加密，以实现世界上第一个量子计算安全磁带驱动器。

2022年4月，IBM发布量子安全系统——IBMz16，该系统基于格密码理论来研发并优化加密算法和数字签名技术。

2023年5月，IBM在年度Think大会上推出了量子安全路线图，以帮助政府和企业完成量子安全加密工作以及抗量子密码迁移。IBM量子安全路线图概述了抗量子密码过渡步骤并提供了三个独立产品帮助美国联邦机构及企业向量子安全过渡。

2024年8月，IBM宣布，在NIST发布的三项标准中，ML-KEM和ML-DSA两项标准是由位于苏黎世的IBM研究中心的密码学研究人员与合作伙伴共同开发的成果，而SLH-DSA标准则由现已加入IBM研究中心的科学家参与开发。



美国PQShield设计并构建了首个符合美国NIST发布的抗量子密码标准的硅芯片，标志着抗量子密码从准备阶段转向合规阶段。这款全功能硅测试芯片集成了PQShield的PQPlatform IP，专为系统级芯片（SoC）半导体供应商提供平台安全和实现安全。该芯片能够详细评估抗量子密码操作、合规性和侧信道攻击（SCA）对策效率，具有硬件/软件协同设计IP和完全可编程固件，可更新以支持未来标准或增强安全性。

符合NIST的抗量子密码学标准的处理器与安全模块陆续推出

英国PQShield与美国SiFive合作，推进RISC-V架构中的抗量子密码学应用。PQShield的PQPlatform-CoPro安全协处理器将与SiFive的Essential Core系列CPU集成，简化RISC-V计算应用的抗量子密码学集成。合作还将移植PQShield的加密库到SiFive的Vector-enabled Performance P470 CPU，加速高性能计算中抗量子密码的采用。

加拿大Crypto4A Technologies成为Cryptographic National Security Algorithm Suite （CNSA）2.0的一部分。Crypto4A与Atsec Information Security合作，针对NIST算法实现进行了测试，获得了ML-KEM、ML-DSA和SLH-DSA算法的认证。其硬件安全模块（HSM）内置硬件信任根和原生量子安全算法支持，确保组织能够保护关键信息。

抗量子密码算法的国际标准化工作仍将持续

目前，抗量子密码算法的国际标准化工作仍在持续推进。国际标准化组织/国际电工委员会第一联合技术委员会（ISO/IEC JTC1）信息安全工作组（SC27）早在2020年5月就发布了抗量子密码研究报告SD8，对多种抗量子密码算法方案进行了全面综述，为后续的标准制定工作奠定了理论基础。

当下，ISO/IEC JTC1正开展两项关键的抗量子密码国际标准制定工作。其中一项由德国在2022年4月提出，计划采用Frodo、ClassicMcEliece、Kyber等抗量子密码算法，对现有公钥加密国际标准ISO/IEC 18033-2:2006/WD Amd2进行增补，目前该项目处于工作草案阶段。另一项由日本于2023年10月发起，采用基于NTRU格的加密算法，当前处于预研项目阶段。

这些参与国际标准制定的算法各有特点。Frodo算法运用无结构格加密技术，在安全性上表现出色，能够为需要长期保密的高安全场景提供可靠保障，不过其公私钥尺寸较大，计算性能欠佳。Classic McEliece算法基于纠错编码方案构建密钥封装，在安全性方面具备一定优势，但存在公钥过大、密钥生成速度较慢的问题，在无需频繁传输公钥的应用场景中或许能发挥其长处。

此外，德国、荷兰和日本等国积极推动的Frodo、Classic McEliece和NTRU等抗量子密码算法，尽管由于性能、实现难度等因素未能入选美国NIST的抗量子密码算法标准，但出于维护抗量子密码技术的独立性以及保障应用安全性等多方面的考量，各国依然不遗余力地推动它们成为国际标准，这也体现了国际标准化工作的多元化和复杂性。

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：多管齐下，资金注入、标准制定，引领量子安全领域发展

02 中国：政策引导，攻克技术创新产业落地难题，构建量子安全坚实壁垒

03 欧盟：依托量子通信基础设施，借政策协调之力，强化量子安全布局

04 澳大利亚：聚焦生态建设，国际合作搭桥，完善量子安全产业链

05 日本：加速追赶，技术合作与政府规划并行，在量子安全领域奋力突围

06 韩国：标准先行，技术紧随其后，推动量子安全技术在多领域应用

01 美国：多管齐下，资金注入、标准制定引领量子安全领域发展

自2020年量子计算技术取得重大突破后，其潜在威胁给全球信息安全体系带来严峻挑战，而量子安全领域的重要性已愈发凸显。美国作为科技强国，在量子安全领域的布局举足轻重，引领着全球量子安全技术发展方向。

在经济增长缓慢、产业亟待升级与科技创新的背景下，量子安全领域发展依旧迅猛。和同样重视量子技术研发的中国、欧盟相比，美国凭借深厚科研底蕴和完善科研体系，在量子安全技术基础研究与应用转化方面进展更快；相较于新兴科技国家，美国量子安全产业成熟度更高，产业生态也更完整。

从美国当前科技战略布局和国际量子安全技术研讨会成果来看，美国量子安全领域强劲发展主要有三大支撑：

- **一是持续的科研创新和人才储备。**得益于美国长期对科研教育的高投入以及对全球顶尖人才的吸引，美国高校和科研机构的量子安全技术在全球处于领先地位，承担大量基础研究和关键技术攻关工作。例如，美国麻省理工学院（MIT）和加州理工学院（Caltech）等顶尖学府在量子算法和量子加密技术方面取得了显著进展。此外，美国的科技创新不仅体现在技术突破，还体现在构建新的量子安全应用场景。
- **二是政府企业重视投入，市场量子安全需求增长。**随着量子计算技术逐步成熟，美国各政府部门和企业意识到量子安全防护的紧迫性，纷纷加大投入。美国国防部高级研究计划局（DARPA）启动“量子安全网络”项目，旨在开发抗量子攻击的通信协议。同时，国际市场对量子安全产品和服务的需求，为美国相关企业提供了广阔发展空间。
- **三是完备的产业生态和丰富的资金来源。**美国不仅有先进的量子安全技术研发企业及其上下游配套企业，还有一系列产业促进机制，如国际量子安全技术研讨会，为技术交流、成果展示和商业合作提供了平台，助力美国整合全球量子安全领域资源。此外，美国企业在量子安全领域融资渠道多样，风险投资、政府专项基金等为企业发展提供充足资金支持。

作为信息技术产业的重要组成部分，美国量子安全领域的蓬勃发展也带动了相关产业的协同进步。

- 美国Quantum Xchange在2024年推出了商用量子密钥分发网络，覆盖美国主要城市。
- 美国信息技术产业协会公布的数据表明，2024年美国信息技术产业中与量子安全相关的业务连续第18个月保持增长，且增长速度逐月加快。

此外，美国军方也高度重视量子安全，通过出台《国防部拨款法案》、《国防量子加速法案》等，投入大量资金，从制定标准、建立卓越中心到开展军事应用项目招标等多方面布局，还积极与盟友及北约合作，引领量子安全发展。美国空军研究实验室（AFRL）启动了“量子优势计划”，旨在增强军事作战能力。

未来，随着量子安全技术不断突破和应用推广，美国信息技术产业安全防护能力有望进一步提升，推动产业稳健发展，量子安全产业也将成为美国在新一轮科技革命中保持领先地位的关键驱动力。

02 中国：政策引导，攻克技术创新与产业落地难题，构建量子安全坚实壁垒

2024年，中国在量子安全领域稳步前行，政策引导、技术创新、产业落地三管齐下，初步构建完善的产业生态，在全球量子安全赛道上占据先发优势。

政策引导是中国量子安全发展的先驱力量。中国对量子安全重视程度日益加深，顶层设计引领量子安全发展，一系列政策相继出台。

- 2021年，《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》明确提出，要加快量子通信等前沿技术的研发和应用。
- 此外，国家发改委、科技部等部门相继出台了一系列支持量子科技发展的政策文件，为量子安全技术的研发和产业化提供了强有力的政策保障。
- 2021年，中国发布了《量子信息科学“十四五”发展规划》，明确了量子通信的重点任务和发展目标。
- 2022年，国家发改委批复了多个量子科技重大专项，总投资超过100亿元，用于支持量子通信网络的建设和技术研发。

技术创新是中国量子安全发展的核心动力。科研团队在量子密钥分发、量子加密算法、量子通信设备等关键技术方向持续突破。

- 在量子密钥分发技术上，中国科学家实现了超过500公里的光纤量子密钥分发，创下世界纪录；同时，星地量子密钥分发实验突破1200公里，为构建全球量子通信网络奠定了坚实基础。
- 在量子保密通信设备研发制造方面，中国成功研制出量子密钥分发专用芯片，打破了国外技术垄断，实现了核心器件的国产化替代。
- 此外，中国科研团队开发的量子随机数发生器已达到每秒产生超过100G比特的随机数，为量子加密提供了强大的基础支撑。

产业落地是中国量子安全发展的必然趋势。中国积极推动量子安全技术在多领域的产业化落地。2024年政务领域的量子保密通信网络建设持续推进，已在安徽、山东、江苏等地投入使用，为政府部门的敏感信息传输提供了绝对安全保障，覆盖范围进一步扩大，新增多个城市将政务系统接入量子通信网络，更有力地保障政务信息传输与存储安全。

未来，随着全球量子技术竞争的加剧，中国将进一步深化政策引导，持续加大技术研发投入，推动量子安全技术与更多行业深度融合，为维护国家信息安全、推动全球量子安全技术发展贡献中国智慧与力量。

03 欧盟：依托量子通信基础设施，借政策协调之力，强化量子安全布局

在量子安全领域，欧盟虽已凭借欧洲量子通信基础设施计划（EuroQCI）等在量子安全领域有所布局，但相较美国，整体战略方向仍不够明晰，欧盟当前关注重点较多集中于量子密钥分发领域。

2019年启动的欧洲**量子通信基础设施**计划（EuroQCI）在2024年取得显著进展。该计划旨在构建一个覆盖整个欧盟及其海外领土的安全量子通信网络，由地面和空间两部分构成。

- 地面部分依托光纤通信网络连接战略地点，并在欧盟委员会“数字欧洲”计划的支持下，于2023年1月进入首个实施阶段。一系列工业项目的开展推动了关键技术模块的成熟，促进了欧洲量子通信生态系统和产业的发展。各成员国积极设计并建设国家量子通信网络，测试不同技术与协议以满足自身需求。2024年中期，相关测试和评估基础设施投入使用，为量子密钥分发服务的技术和服务提供评估与验证，确保用户通信的安全性。
- 空间部分则通过与欧洲航天局（ESA）的合作，基于第一颗原型卫星Eagle-1，制定了欧洲量子通信基础设施计划的服务卫星星座规格。该卫星计划于2025年底或2026年初发射，将进一步完善欧盟的量子通信网络，为全球范围内的量子安全通信提供支持。
- 此外，2024年，欧盟通过《欧洲量子网络安全议程》，提出制定欧盟量子转型协调行动计划等建议，旨在强化在该领域的应对能力，促进各国间合作。

政策协调方面，欧盟积极推进，进一步加强量子安全。

- 2024年4月发布《向抗量子密码迁移的协同实施路线图建议》，鼓励成员国制定统一战略，实现向抗量子密码的协调同步迁移。建议成立抗量子密码分组，制定“向抗量子密码迁移的协同实施路线图”，预计两年后发布，成员国依此制定调整迁移计划。
- 强化欧盟委员会监督评估职能，成员国需提交相关信息，委员会据此监督路线图起草进展、验证措施有效性，必要时可提出具有约束力的联盟法律，以此促进国家间数字系统互操作性，保障欧盟数字基础设施和服务在未来数字时代的安全。

整体来看，2024年欧盟量子安全布局成效初显。量子通信基础设施的完善为量子安全技术应用提供物理支撑，使量子密钥分发等安全通信服务得以广泛实现，保障了关键领域信息安全。同时，政策协调为抗量子密码迁移提供统一战略框架，加速技术升级和应用推广。然而，欧盟也面临量子技术创新突破、国际合作协调等挑战，需持续努力探索解决方案，以保持竞争力。

04 澳大利亚：聚焦生态建设，国际合作搭桥，完善量子安全产业链

在全球量子技术蓬勃发展的背景下，澳大利亚积极布局量子安全领域，以生态建设为切入点，结合国际合作，推动量子安全产业稳步前行。

澳大利亚深刻认识到**生态建设**对于量子安全产业发展的关键意义。

- 在企业层面，澳大利亚政府积极搭建交流合作平台，推动量子中心的创建以及澳大利亚量子联盟的组建，促进企业、科研机构和高校之间的紧密协作，营造协同创新的良好氛围。
- 从科研角度，悉尼的量子科技企业借助交流平台，与当地高校开展产学研合作，加速量子安全技术从实验室走向市场的进程。澳大利亚国立大学、悉尼大学等为量子安全生态提供了丰富的理论与技术支撑，不断拓展量子安全技术的应用边界。

国际合作也是澳大利亚在量子安全领域的重要战略方向。澳大利亚积极整合全球资源，成立国际量子发展联盟，构建起灵活且富有弹性的量子供应链，不仅保障了本土量子安全产业发展所需资源的稳定供应，还提升了其在全球量子安全产业链中的地位。

- 英国Quantum Motion被澳大利亚丰富的量子人才资源吸引，在悉尼创新中心设立新量子实验室。
- 加拿大BTQ Technologies与麦考瑞大学开展战略研究合作，致力于量子算法和通信安全的研发。
- 通过成立国际投资网络，澳大利亚推动印太地区新兴量子技术的发展，加强区域内技术交流与合作，共同应对量子安全挑战。

资金投入上，政府拨款10亿澳元用于量子及其他关键技术，启动首轮3600万澳元的量子关键技术挑战计划等，充足的资金为产业链的完善提供了坚实保障。

政策与标准制定方面，澳大利亚积极加入组织联盟，共同参与政策标准制定。

- 澳大利亚加入国际标准化组织量子技术委员会（JTC 3），深度参与量子信息技术标准的制定，为澳大利亚量子安全产品和服务走向国际市场铺平道路。
- 借助奥库斯（AUKUS）联盟，澳大利亚与美国、英国在量子技术领域展开深度合作，共享资源、共同研发，加速了量子安全技术在国防和安全领域的应用。
- 政府通过国家重建基金（NRF）优先支持量子技术研发，利用高级战略能力加速器加速颠覆性量子技术的市场培育，为量子安全产业链各环节营造了良好的政策环境。

澳大利亚有望继续深化生态建设与国际合作两大战略举措，进一步提升在全球量子安全领域的影响力，为其经济发展和国家安全提供强有力的支持。随着量子技术的持续进步，澳大利亚的量子安全产业也将迎来更广阔的发展空间。

05 日本：加速追赶，技术合作与政府规划并行，在量子安全领域奋力突围

在全球量子安全领域的竞争浪潮中，日本虽起步晚，但凭借技术合作与政府规划双轮驱动，发展势头迅猛，力求快速提升自身竞争力。

在**技术合作**层面，日本积极与国际伙伴携手前行。

- 2023年2月，日本量子革命战略产业联盟（Q-STAR）与美国量子经济发展联盟（QED-C）、欧洲量子产业联盟（QUIC）、加拿大量子产业联盟（QIC）共同签署谅解备忘录，正式成立国际量子产业协会理事会。各方围绕量子技术的国际规则制定和知识产权管理展开深度合作，日本借此不断汲取国际先进经验，持续提升自身技术实力。
- 2024年4月，日本东芝与韩国电信运营商KT合作，成功展示了利用混合量子安全通信技术（结合量子密钥分发和抗量子密码），保护银行和金融网络免受量子计算机的网络攻击。

从**政府规划**来看，日本对量子安全领域的重视程度日益加深。

- 日本政府计划在2030年前开发国产量子加密技术，该计划从2025年起，预计耗时五年，投入数百亿日元。
- 总务省计划在2030年前完成技术国产化，并建立网络攻击防御系统，旨在为金融机构、电信提供商和关键基础设施组织等提供安全的数据传输服务。
- 早在2021年2月，日本政府就建立统合管理协调量子技术研发的机构，在全国布局多个量子技术研发基地，其中部分专门针对量子安全方向展开研究。
- 在政策大力扶持下，东芝、日本电气等公司已被选为该项目的候选企业，积极投身量子安全技术的研发与创新。

不仅如此，日本新能源与产业技术综合开发机构（NEDO）资助相关研究项目，致力于加强日本量子网络安全防御，提升抗量子密码协议在日本技术供应链中的应用。

在**产业生态构建**上，日本政府鼓励企业联合推进量子安全项目，推动东芝、NTT、NEC、日立制作所、富士通等11家公司成立“基于量子技术的新产业创造协议会”，共同攻关量子技术产业应用，在量子安全相关的材料开发、人才培养等关键事项形成长效合作机制。

未来，随着技术合作的持续深化和政府规划的稳步推进，日本有望在量子安全领域实现更大突破，逐步缩小与领先国家的差距，在全球量子安全产业格局中占据更为重要的地位，其发展成果也将为全球量子安全技术的进步与应用提供宝贵经验。

06 韩国：标准先行，技术紧随其后，推动量子安全技术在多领域应用

在全球量子安全领域竞争日益激烈的2024年，韩国凭借“标准先行、技术跟进、应用拓展”的清晰策略，积极布局，在量子安全赛道上快速前进，已取得一系列显著成果。根据韩国科学技术信息通信部（MSIT）发布的《2024年量子技术发展路线图》，韩国计划到 2035 年对量子科学技术投资 3 万亿韩元（23 亿美元）。

韩国将**标准制定**视为量子安全领域发展的关键突破口。

- 一方面，积极整合国内资源，通信、科研等多领域的企业与机构紧密合作，全力推动量子安全标准的建立。2024年，韩国电子通信研究院（ETRI）主导制定了光传输网络量子抗攻击密码应用标准，以及量子密钥分发网络国家标准的相继出台，为量子通信基础设施的规范化发展提供了坚实保障。
- 另一方面，韩国计划成立以自身为主导的全球标准化组织——亚洲量子安全标准联盟（AQSA），帮助韩国在全球量子安全市场中占据有利地位，为韩国量子安全技术与产品走向世界开辟道路。

在**技术研发**层面，韩国汇聚各方力量，在量子安全的多个关键领域积极探索。根据韩国产业通商资源部（MOTIE）的数据表明产学研紧密结合是韩国技术创新的核心模式。

- 韩国首尔大学量子信息研究中心与三星电子合作，成功开发出抗量子攻击的加密芯片，该芯片可在现有通信设备中无缝集成，显著提升了数据安全性。
- 韩国科学技术研究院（KAIST）实现了量子密钥分发技术的突破，将密钥生成速率提高了30%，为大规模商用奠定了基础。
- 韩国积极参与国际技术交流与合作，与美国NIST签署了量子安全技术合作备忘录，共同研发下一代抗量子密码算法。

韩国大力推动量子安全技术在**多领域应用**，以市场需求反哺产业发展。

- 在国防军事领域，韩国国防科学研究所（ADD）与LIG Nex1合作，成功研发了量子加密通信无人机，并且已在2024年的韩美联合军演中进行了实战测试，显著提升了军队通信的安全性和作战效能。
- 在金融领域，韩国国民银行（KB Bank）在2024年推出了基于量子加密技术的数字资产托管平台，为加密货币和数字资产提供高安全性保障。
- 在医疗领域，韩国首尔国立大学医院与韩国QunaSys合作，开发了量子加密医疗数据共享平台，确保患者隐私数据在传输过程中的绝对安全。

韩国的量子安全战略不仅为其在全球竞争中赢得了先机，也为其他国家提供了可借鉴的发展模式。通过标准制定、技术研发和应用拓展的三重驱动，韩国正逐步构建起完整的量子安全生态系统。



05

投融资分析

目录

05
投融资分析

01 融资总额：较2023年有所上升，但趋势缓慢

02 融资分布：资金集聚头部企业，多元格局初显

03 融资轮次：比较分散，仍处于融资早期阶段

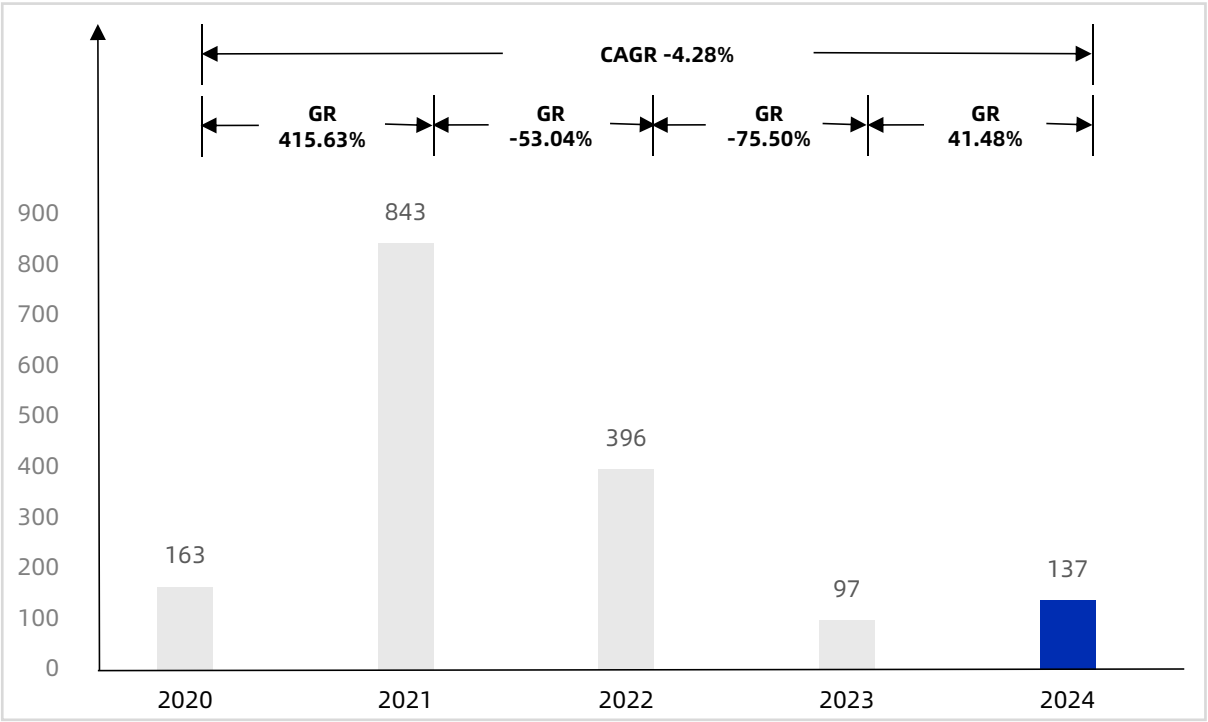
04 融资领域：抗量子密码最高，量子密钥分发紧随其后

05 融资次数：连续四年持续下降

01 融资总额
融资较2023年有所上升，但趋势缓慢

2024年量子安全领域共有11家公司获得1.37亿美元融资。相较于2023年，融资金额有所上升，但是上升趋势缓慢。全球量子安全产业在吸引资本方面虽有进展，却仍面临如行业规模小、投资回报不确定性大等诸多挑战，使得社会资本流入未能呈现显著跃升。

图表 2020-2024年全球量子安全领域融资总额（单位：百万美元）



ICV TA&K & 光子盒研究院 QUANTUMCHINA | 2025.2

技术发展角度看，一是量子安全技术目前仍处于快速发展阶段，技术成熟度与稳定性有待提高，技术更新迭代快、验证周期长。投资者对于技术风险的考量，导致其在投入资金时较为克制，不会像在一些技术相对成熟、市场前景清晰的领域那样快速大量地投入资金；二是量子安全领域要实现重大技术突破面临着较高的门槛和难度。每一次的技术进步都需要大量的资金、人力和时间投入，且成果具有不确定性。这使得投资者在决策时更加谨慎，资金投入相对保守。

市场竞争角度看，一是随着量子安全领域的发展，越来越多的企业进入，市场竞争日益激烈。投资者在选择投资对象时会更加挑剔，使得资金的分配更加分散，难以形成集中的、大规模的融资事件；

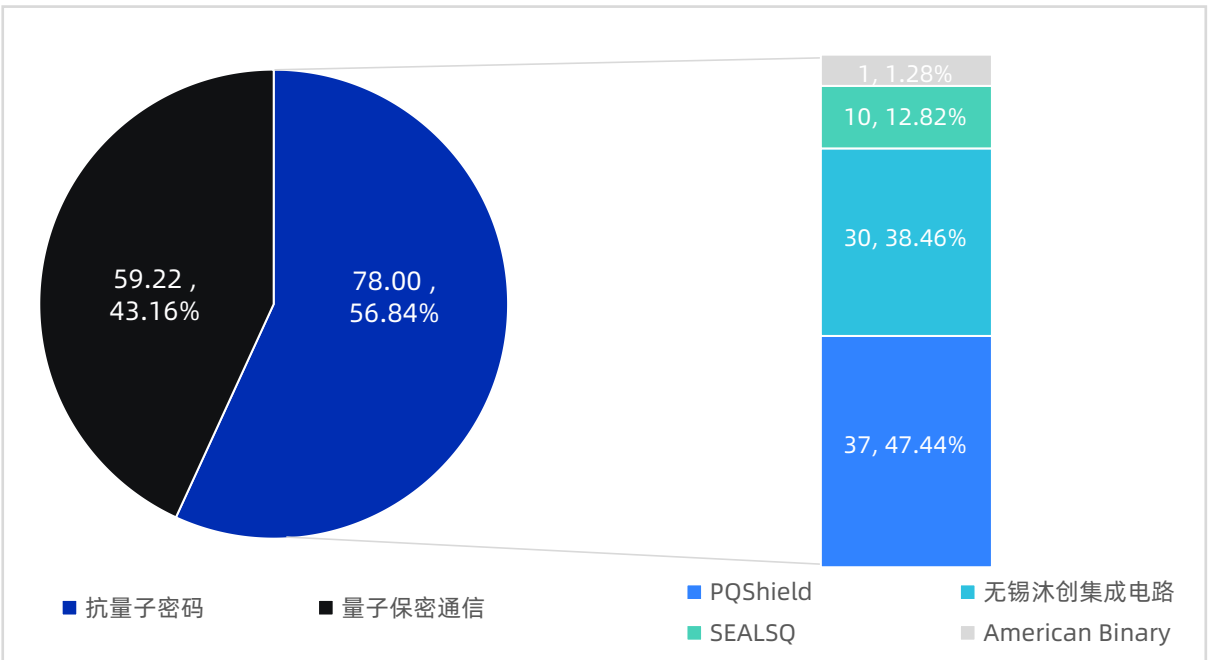
二是目前量子安全领域尚未形成具有绝对优势的头部企业，各企业在技术水平、市场份额等方面差距相对较小。投资者难以找到具有明显引领作用和垄断潜力的企业进行大规模投资，而是更倾向于在多个企业中进行小额投资，以分散风险，这也使得融资总额的增长趋势较为平缓。

2024年，全球量子安全领域投融资活跃度一般，产业发展仍处在起步期阶段。在抗量子密码领域，2024年有4家抗量子密码企业获得了融资，融资额大约占量子安全领域的56.84%。

- 中国无锡沐创集成电路设计有限公司完成数亿元A3轮融资，此轮融资由蚂蚁集团领投。
- 英国PQShield获3700万美元B轮融资，在NIST抗量子标准化项目中作用重大。
- 美国American Binary致力于抗量子安全解决方案，技术潜力获资本认可，获得100万美元战略投资。
- 瑞士SEALSQ专注量子安全技术，本轮股权融资获得1000万美元，主要帮助其拓展市场。

以上获得投资的企业，融资轮次分布于4个不同的阶段，表明抗量子密码领域目前仍处于发展成长阶段，具有潜力和挑战并存的特点。

图表 2024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）



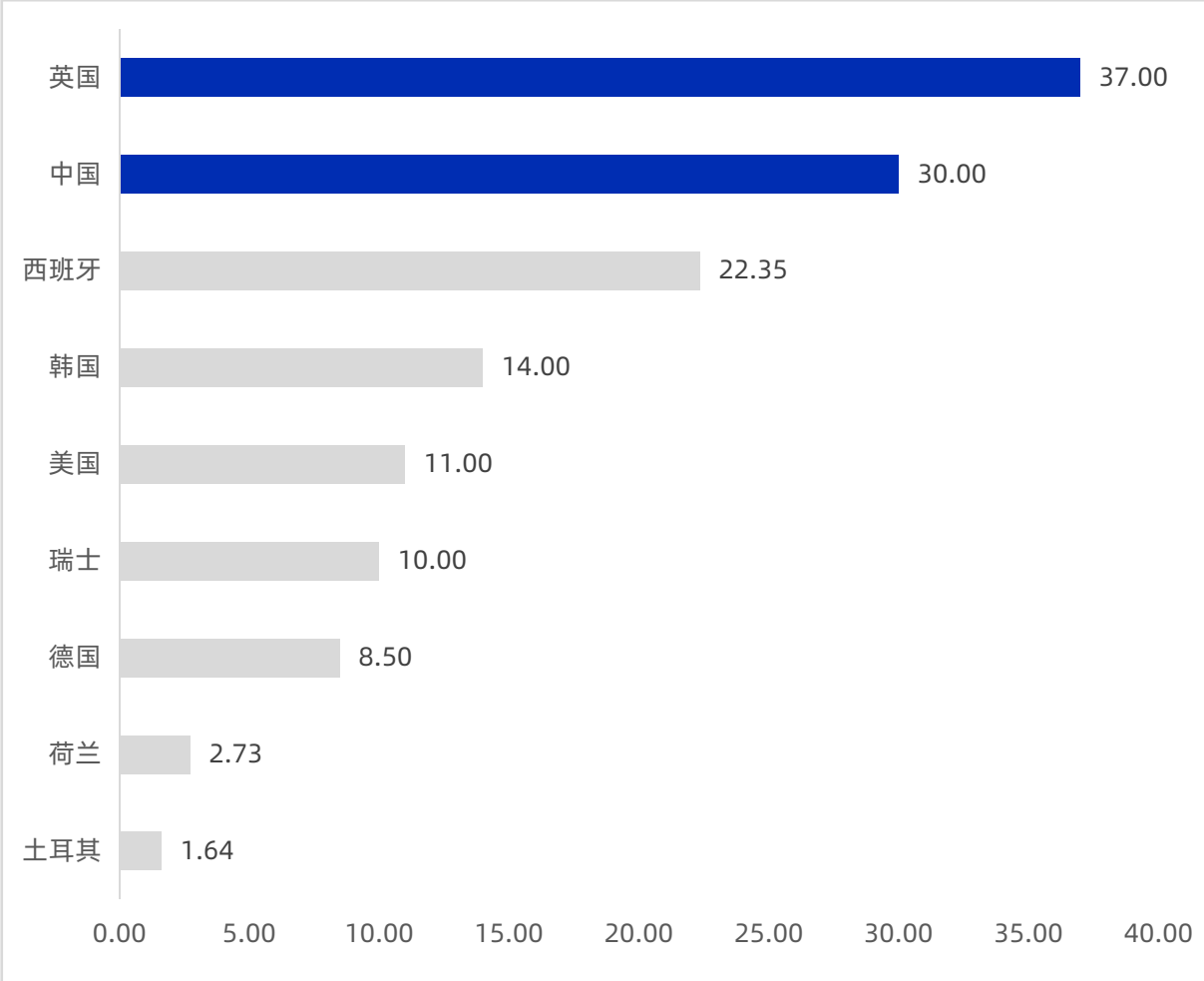
ICV TA&K & 光子盒研究院 QUANTUMCHINA | 2025.2

02 融资分布
资金集聚头部企业，多元格局初显

2024年被投企业来自9个国家，分别是美国、中国、英国、德国、西班牙、荷兰、土耳其、瑞士和韩国。从已披露的融资金额来看，资金投向英国的金额最高（约0.37亿美元，1家公司），其次为中国公司（约0.3亿美元，1家公司）、西班牙公司（约0.22亿美元，2家公司）。

量子安全领域的融资地域分布广泛，美国、欧洲、亚洲各个国家和地区不仅融资规模有所增长，活跃度也进一步提升，表明全球更多地区正在积极布局量子安全领域，加大资源投入，以抢占该领域的发展先机。

图表 2024全球各国量子安全领域的融资总额（单位：百万美元）



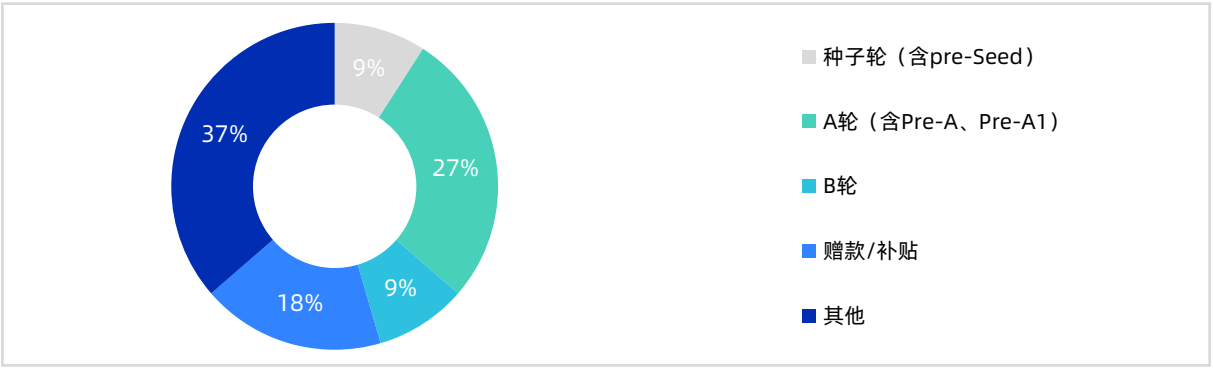
ICV TA&K & 光子盒研究院 QUANTUMCHINA | 2025.2

03 融资轮次比较分散，仍处于融资早期阶段

2024年融资轮次分散，无集中趋势，在种子轮、A、B以及政府赠款/补贴都有所涉及。表明量子企业在各个阶段都有了不同程度的进展。

2023年融资轮次以A轮和其他战略性投资为主，无B轮之后投资。但是，2024年英国PQShield企业完成了B轮融资，整体融资轮次有向后期推进的趋势，说明部分量子安全领域企业有了进一步的发展，开始进入相对更成熟的阶段。

图表 2024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	量子网络
种子轮	QUBITRIUM			
A	QUANTUM CORRIDOR QUANTUM OPTICS JENA		沐创集成电路 MICRO INNOVATION INTEGRATED CIRCUIT	
B			PQ SHIELD	
赠款/补贴	LUXQUANTA			Q bird quantum connectivity
其他	sener	sdt	AMERICAN BINARY SEAL SQ semiconductors + quantum	

ICV TA&K & 光子盒研究院 QUANTUMCHINA | 2025.2

04 融资领域
抗量子密码最高，量子密钥分发紧随其后

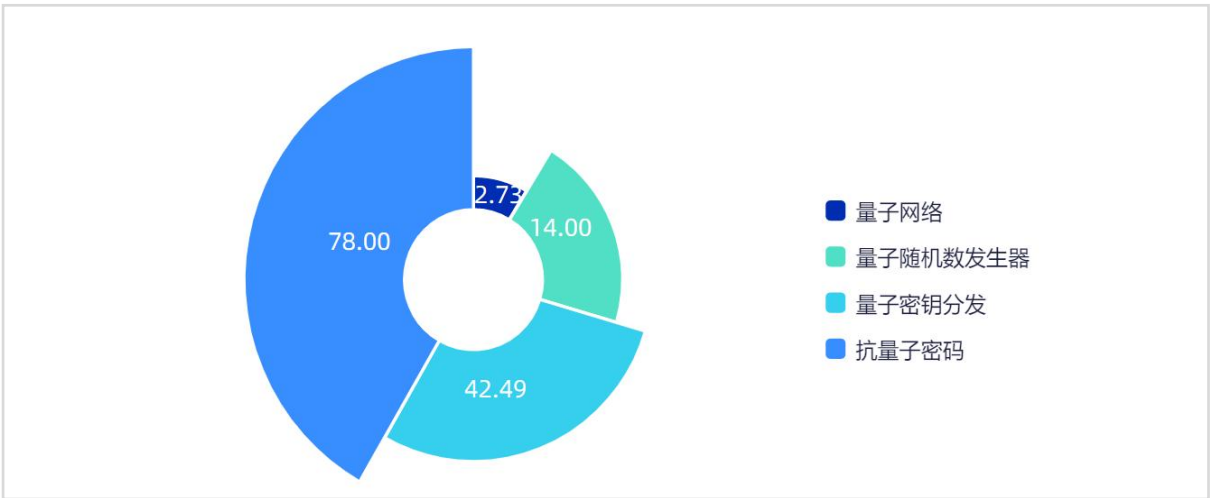
2024年，量子安全融资领域较为分散，包括量子密钥分发、基于软件的端到端抗量子密码解决方案、量子网络、安全通信、量子纠缠和抗量子密码学芯片等。抗量子密码领域融资占比首次达到最高，究其原因：

从计算优势角度看，一方面是抗量子密码的技术成熟度不断提升，随美国NIST在抗量子密码领域的标准化工作推进，抗量子密码技术迎来成长期，技术的成熟度和可靠性得到提升，使得投资者对其未来发展更有信心。另一方面是市场需求增长，全球范围内对信息安全的关注度不断提高，特别是在量子计算快速发展可能带来的安全威胁背景下，企业和组织对抗量子密码解决方案的需求急剧上升，从而吸引了大量资金投入。

从成本角度看，经过多年的研发和探索，抗量子密码算法的研究逐渐深入，一些关键技术难题得到解决，研发成本有所降低，使得更多的企业能够参与到抗量子密码技术的研发和应用中，推动了整个领域的发展。同时，抗量子密码的硬件实现市场逐渐成熟，相关芯片和设备的生产成本逐渐减少，降低了抗量子密码技术的应用门槛，促进了其商业化进程，吸引了更多投资机构的关注。

从产业角度看，商业化进程加速，抗量子密码商业化的推进使得更多企业和组织寻求将现有加密算法迁移到抗量子密码体系，带动了相关产品和服务的市场需求，推动了抗量子密码产业的快速发展，吸引了大量资金涌入。美国NIST主导的抗量子密码标准化工作的持续推进，为抗量子密码技术的广泛应用奠定了基础，使得投资者加大了对抗量子密码领域的投资。

图表 2024年量子安全各领域融资额分布情况（单位：百万美元）



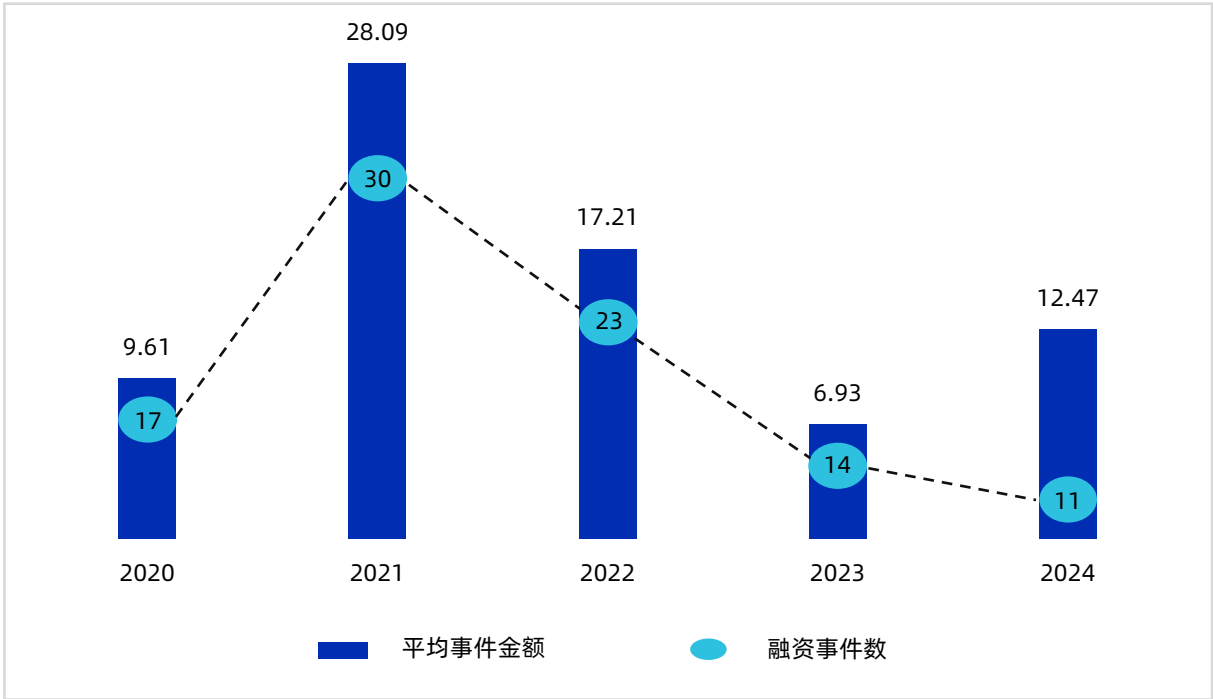
05 融资次数连续四年持续下降

2024年度总计发生融资事件11件，较2023年融资事件数有所降低。但是，2024年平均融资额为1247.45万美元，较2023年上升了554.66万美元。可以看出，在公司数量减少的情况下融资金额有所增加，平均每家公司的融资金额也有所上升，表明单个项目的吸引力可能增强，投资者对优质项目的投入力度加大。

自2021年至2024年，量子安全领域的融资次数逐年降低，但是抗量子密码作为量子安全领域的一个重要分支，正在吸引越来越多的投资。同时投资者展现出多元化的投资布局，通过在量子安全不同领域进行一至两轮的融资，以分散风险并寻求更广泛的增长机会。

此外，尽管近两年量子安全领域的融资出现下滑，但全球政府正积极布局量子安全领域产业，并出台了一系列政策措施，以推动量子通信的研发和应用，为该领域的发展提供政策支持。

图表 2020-2024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 & 光子盒研究院 QUANTUMCHINA | 2025.2



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

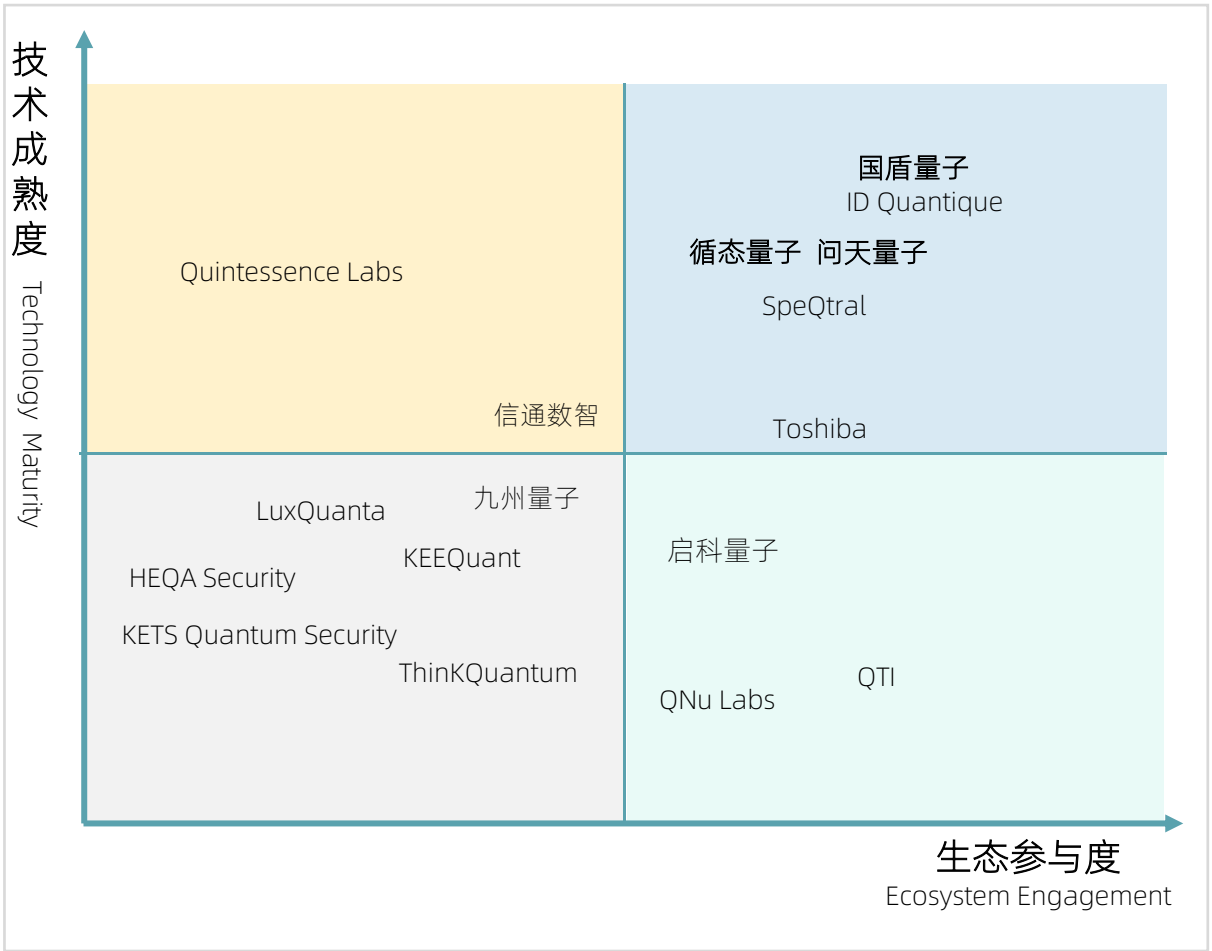
04 量子安全代表性厂商分析

01 量子密钥分发供应商分析

当前，量子密钥分发技术已实现量子安全领域产品的商业化，并在较大范围内应用。因此，量子密钥分发供应商在技术成熟度和生态参与度方面分布较为均衡。

从量子密钥分发供应商的Q-EMC模型可以看出，设备方面，澳大利亚Quintessenc Labs等处于左上方，技术成熟度尚可，但生态建设投入不足，短期内可凭技术吸引特定客户，长期则需加强产业合作以拓展市场。右下方的日本Toshiba等积极参与生态建设，虽技术成熟度有待提高，但可借助生态快速改进技术，有实现双重突破的潜力。

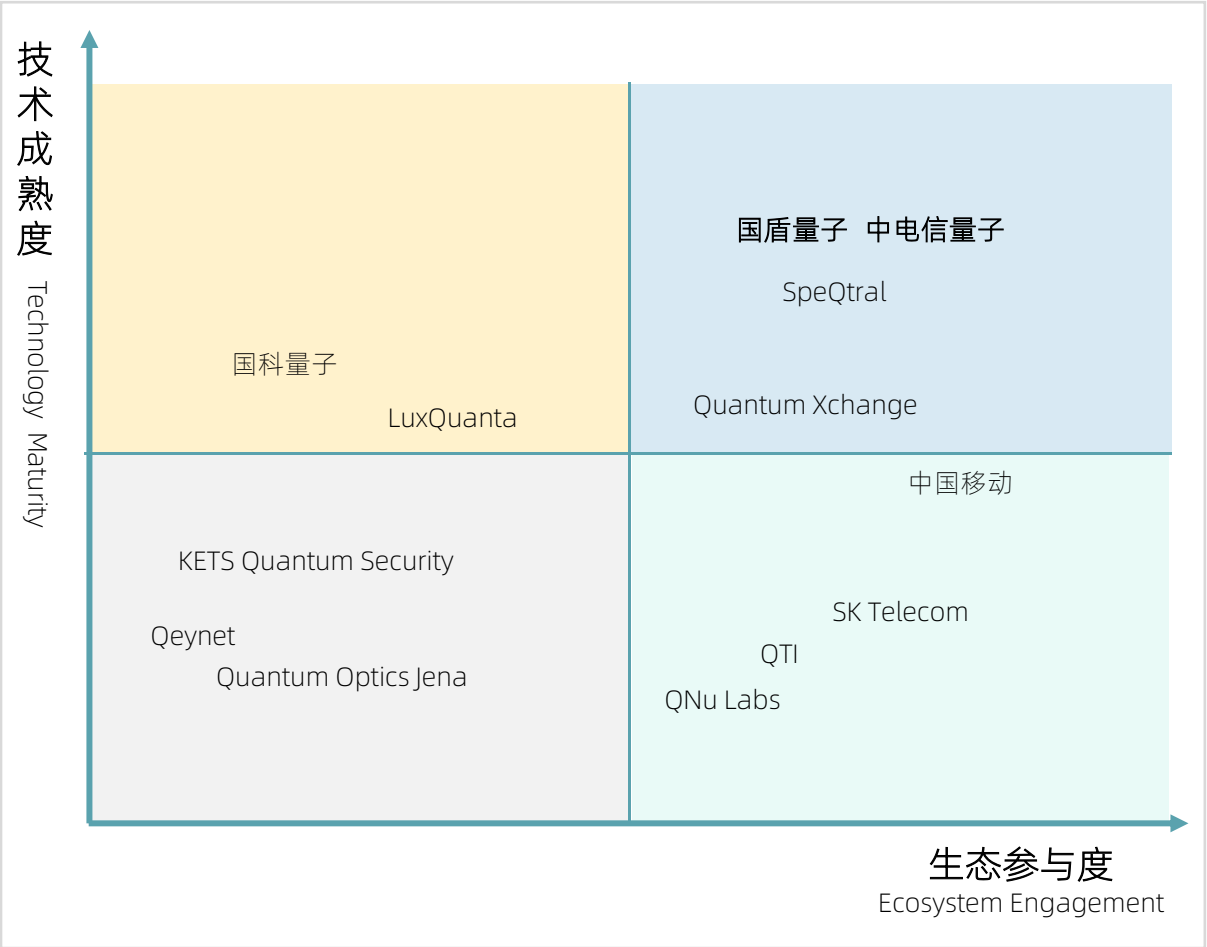
图表 量子密钥分发供应商（设备方面）的Q-EMC模型



光子盒研究院 QUANTUMCHINA | 2025.2

网络方面，中国中电信量子等位于右上方，凭借成熟技术与广泛生态合作，在产品商业化上成果显著，市场优势明显，未来有望持续领先。加拿大Qeynet等处于左下方的企业多处于起步阶段，不过当前市场机遇良好，若能兼顾技术研发与生态拓展，便有机会在市场中崭露头角。

图表 量子密钥分发供应商（网络方面）的Q-EMC模型



光子盒研究院 QUANTUMCHINA | 2025.2

从企业发展策略维度看，有的企业追求全面发展，兼顾技术成熟度提升与生态参与度加强，这类企业有望在市场竞争中占据有利地位。有的企业则选择先专注技术攻坚，待技术成熟后再拓展生态，或者先大力发展生态，借助生态力量推动技术进步。

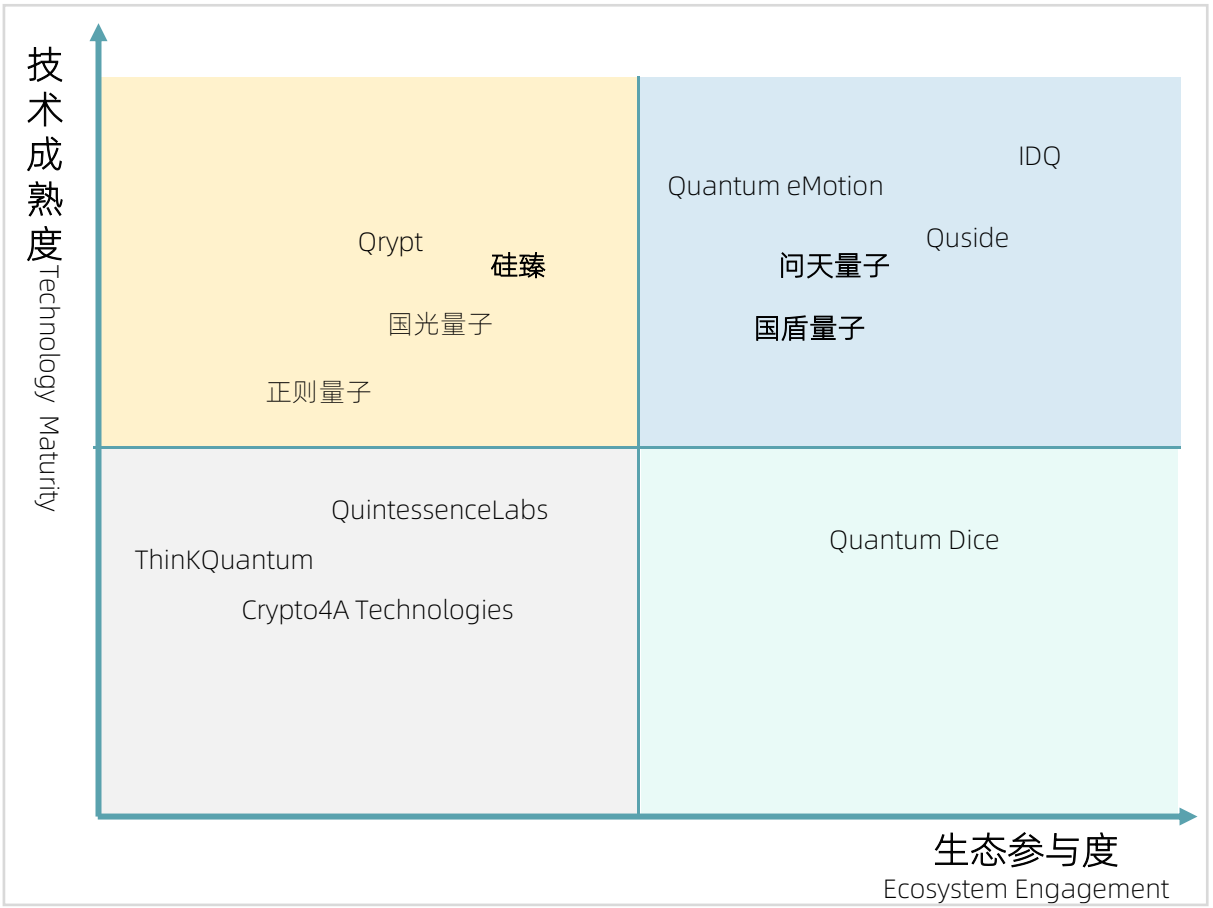
不同策略各有优劣，企业需根据自身资源和市场定位灵活选择。随着量子安全市场的发展，技术成熟度高且生态参与度强的企业将更具竞争力，而处于起步阶段的企业也有机会通过合理策略实现快速发展。整个量子密钥分发市场将在各企业的技术竞争与生态合作中不断进步，推动量子安全技术产业的繁荣。

02 量子随机数发生器供应商分析

目前，量子随机数发生器供应商之间的差距较大，这种差距不仅体现在技术研发的成熟度、创新速度等技术层面，还延伸至生态合作、活动联合等生态维度。

从量子随机数发生器供应商的Q-EMC模型来看，左下方的澳大利亚Quintessence Labs、加拿大Crypto4A Technologies等供应商，技术成熟度相对较低，由于处于发展初期或技术迭代较慢，在产品性能和稳定性上与其他供应商存在差距，在技术创新速度上也可能滞后。

图表 量子随机数发生器供应商的Q-EMC模型



光子盒研究院 QUANTUMCHINA | 2025.2

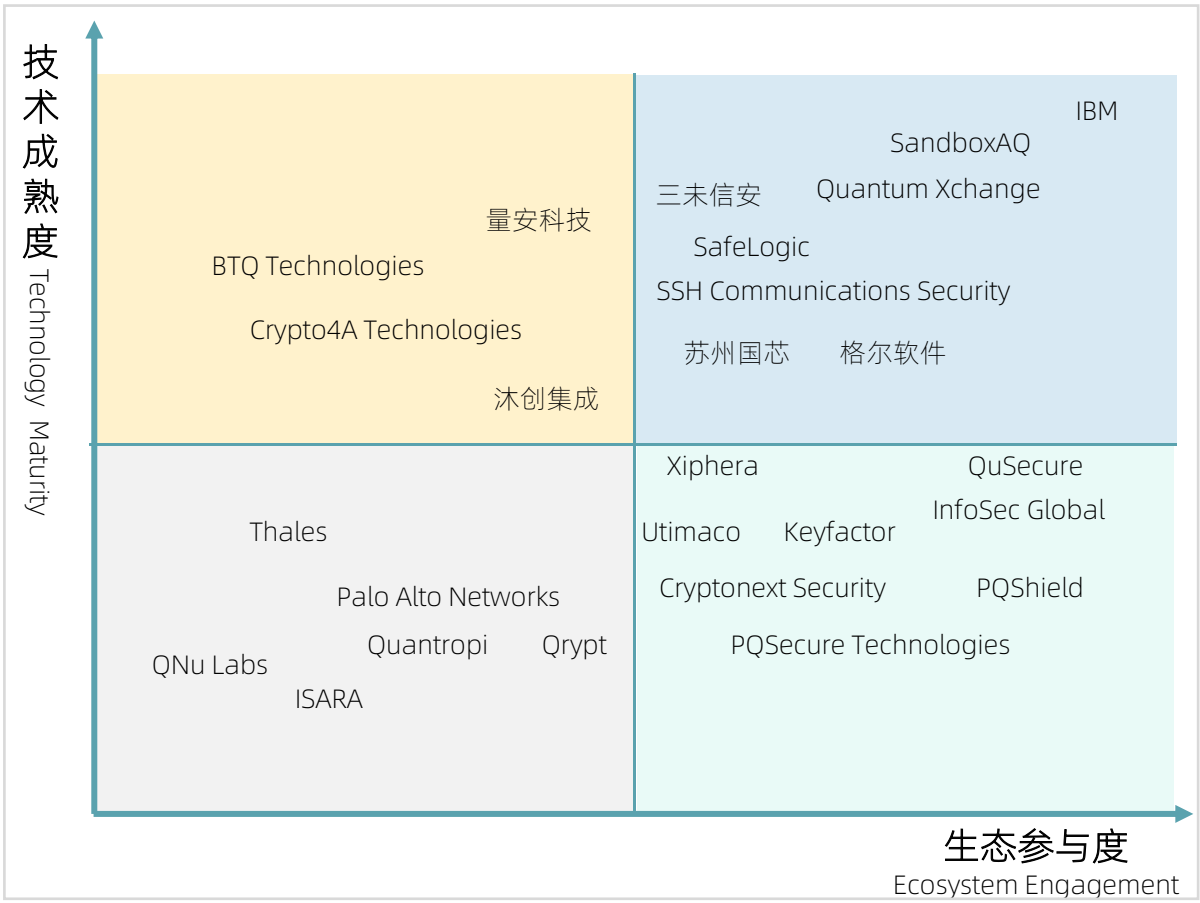
相比较而言，加拿大Quantum eMotion、西班牙Quside、瑞士IDQ等长期在量子随机数发生技术领域投入大量的人力、物力和财力资源。经过多年的发展，企业积累了大量的技术专利和研发成果，形成了一套成熟的技术体系，满足随机数安全性和准确性要求极高的应用场景需求。由于供应商能够及时获取市场反馈，不断优化和改进技术，进一步提升技术成熟度。同时，供应商具有较强的战略眼光和市场意识，通过与产业上下游合作，整合各方资源，实现优势互补，有助于提升企业的品牌知名度和行业影响力，共同推动量子随机数发生技术的应用和发展。

03 抗量子密码供应商分析

抗量子密码供应商普遍重视生态建设，通过广泛合作拓展市场和提升影响力，这反映了其在面对激烈市场竞争时的战略眼光。在技术层面，尽管存在成熟度不足的情况，但各供应商也在通过不同策略努力提升技术水平。

多数抗量子密码供应商生态参与度较高，积极与产业上下游展开合作。像美国SandboxAQ、Quantum Xchange等处于右上方区域的供应商，通过与各类企业、机构合作，构建起广泛的生态网络。例如，与通信企业合作可将抗量子密码技术应用于网络通信安全，与金融机构合作则能保障金融交易的安全性。此外，参与行业标准制定、技术交流等活动，提升了企业在行业内的话语权和影响力。

图表 抗量子密码供应商的Q-EMC模型



光子盒研究院 QUANTUMCHINA | 2025.2

抗量子密码供应商的Q-EMC模型右下方供应商虽然整体生态参与度较高，但供应商在技术成熟度上稍有逊色。处于左下方区域的供应商，如法国Thales等，技术成熟度相对较低。它们可能在技术研发上投入相对不足，或者面临技术难题尚未攻克。然而，即使是技术成熟度较高的右上方区域供应商，也仍需不断投入研发资源。部分供应商计划将重点放在特定领域的技术优化上，期望在细分市场中取得技术优势，以点带面推动整体技术成熟度提升。

04 量子安全代表性厂商分析

美国：多家竞逐，着力量子安全标准制定

图表 美国量子安全代表性厂商



光子盒研究院 QUANTUMCHINA | 2025.2

Qrypt

Qrypt成立于2019年，位于纽约。是一家专注网络安全的量子技术公司，通过与国家实验室等合作，提供量子安全加密技术和产品，如量子熵、量子安全密钥生成技术等，获多项行业奖项。

Qrypt在AWS Marketplace上推出了量子熵即服务（EaaS），为用户提供了基于量子技术的熵服务，可满足数据加密等领域对高质量随机数的需求。荣获AFWERX颁发的SBIR第一阶段合同，将利用此合同对Mattermost安全聊天进行量子强化，提升其安全防护能力。在抗量子密码方面，加入PKI联盟，凭借自身技术和专家资源，助力制定抗量子密码学最佳实践与政策。为NVIDIA BlueField-3 DPU提供量子安全加密技术，集成至IPsec管理密钥生成与建立，利用量子随机熵生成加密密钥，消除密钥传输风险，保障AI集群通信安全。还与AIC、NVIDIA合作，为AIC的TB116-DL网络安全平台提供量子加密支持，共同打造先进多层安全解决方案。

PQSecure Technologies成立于2017年，位于佛罗里达州博卡拉顿。专注抗量子加密解决方案，为物联网等设备提供对称和非对称算法。推出了Suite-Q HW等产品。

PQSecure Technologies与东北地区国防技术中心（NORDTECH）合作，推动CHIPS、IoT和Edge的量子安全加密IP开发。为DARPA的AISS项目贡献力量，参与开发抗量子且物理安全的芯片设计方法与解决方案。协助Flex Logix Technologies探讨侧信道攻击及对策，助力提升加密技术安全性。此外，加入抗量子密码联盟，凭借在量子安全加密硬件IP方面的专长，致力于推动抗量子密码算法的研究、开发与应用，为构建安全的数字未来贡献力量。

Qusecure成立于2019年，位于加利福尼亚州圣马特奥。是抗量子网络安全领域的佼佼者。推出QuProtect软件平台，提供量子安全即服务。与思科、英伟达等合作，获美国空军资助，拥有多项专利。

在业务拓展上，QuSecure获美国空军、陆军合同，产品应用于军事项目；加入AWS ISV Accelerate计划，拓展市场。行业合作中，参与白宫会议提供经验，加入抗量子密码联盟助力技术发展，与NVIDIA合作推进抗量子密码学研究。荣誉奖项方面，其QuProtect解决方案荣获零信任安全卓越奖，被Frost & Sullivan评为全球产品领导者，彰显技术实力。此外，QuSecure还获得SOC 1和SOC 2Type 2合规认证，保障产品安全性和可靠性，持续推动抗量子网络安全技术的应用与发展。

SandboxAQ于2022年从Alphabet独立而来。融合量子技术与AI，提供抗量子密码系统、新型导航系统等产品。客户遍布120多个国家或地区，获多轮巨额融资，估值超56亿美元。

SandboxAQ与埃森哲合作，助力企业抵御人工智能驱动的网络威胁和量子解密攻击，后又扩大合作，强化企业数据加密并防范未来威胁。作为抗量子密码学联盟创始成员，推动抗量子密码学发展。SoftBank选用其AQtive Guard，识别现有IT基础设施中潜藏的安全漏洞。此外，SandboxAQ发布网络安全科学技术，展示自身技术实力与对行业的贡献，为保障网络安全、应对量子时代挑战积极布局。

Keyfactor成立于2001年，总部位于俄亥俄州。是数字身份管理解决方案提供商，提供云优先PKI即服务等产品。可管理数字证书，实现端到端自动化。

在技术创新方面，Keyfactor于Microsoft Azure市场推出下一代抗量子密码实验室，助力企业为抗量子时代做准备；其Bouncy Castle获得NIST FIPS 140-3认证，提升了加密技术的可靠性。在合作拓展上，加入AWS ISV Accelerate计划，扩大与AWS的合作；与丰田通商株式会社建立战略伙伴关系，加速加密技术在日本的实施；还成为Climb Channel Solutions新的北美渠道合作伙伴，拓展业务范围。此外，Keyfactor连续四年荣获2024年CRN合作伙伴计划指南五星评级，彰显其在行业内的优势地位。

Palo Alto Network成立于2005年，总部在加利福尼亚州圣克拉拉。是全球网络安全领军企业，以提供下一代防火墙著称。产品涵盖云安全、端点保护等。客户超7万家，遍布150多国。

在网络安全领域，Palo Alto Networks与Quantropi合作，借助Palo Alto Networks在网络安全领域的优势，双方围绕量子安全等技术展开探索，致力于提升安全防护水平。同时，Singtel借助Palo Alto Networks和Fortinet的技术与资源，依托Quantum-Safe网络升级自身网络安全体系。通过整合各方优势，为用户构建更安全的网络环境，积极应对不断变化的网络安全威胁，保障网络安全和用户数据安全。

SafeLogic是一家位于加州帕洛阿尔托的信息安全软件公司，成立于2012年。专注于提供加密软件与服务，以FIPS 140-2验证服务和开发加密引擎产品闻名。主要产品有CryptoComply、Rapid Cert等。

SafeLogic参与美国NIST的抗量子密码迁移项目，为行业发展贡献力量。推出FIPS 140-3早期访问计划，助力客户提前了解相关标准。在RSA大会上发布抗量子密码早期访问计划，推动技术应用。其CryptoComply加密软件获FIPS 140-3验证，彰显技术实力。与Carahsoft合作，为公共部门提供验证过的加密技术。还推出CryptoComply PQ TLS早期访问计划，不断探索量子安全加密在传输层安全方面的应用，持续推动抗量子密码技术的发展与落地。



Quantum Xchange成立于2018年，位于马里兰州贝塞斯达。是专注量子通信安全的公司，推出了网络监控工具CipherInsights和量子安全密钥交付平台Phio TX。与多家企业合作推动量子安全技术发展，致力于保护数据免受量子计算等威胁。

Quantum Xchange的风险评估工具CipherInsights取得早期成功且需求增长，助力企业应对欧盟数据安全法规。与瞻博网络合作，为高监管行业提供量子安全网络方案。举办网络研讨会，聚焦抗量子密码迁移。推出结合AI与量子安全的VPN，增强网络安全性。与多方合作推出抗量子网络攻击创新方案。此外，其加密平台Phio TX获得FIPS 140 - 3认证，并完成FIPS 203验证测试，支持NIST标准算法和迁移建议，不断推动量子安全技术的应用与发展，为企业提供更安全的网络环境。

中国：
以中电信量子、国盾量子为首，积极开拓市场

图表 中国量子安全代表性厂商



光子盒研究院 QUANTUMCHINA | 2025.2

中电信量子集团
CHINA TELECOM QUANTUM GROUP

中电信量子于2023年5月成立于安徽省合肥市。公司积极攻坚量子底层核心技术，致力于推动量子通信产业化。承担多项重大项目，融合量子密钥分发系统，打造量子密码全场景解决方案。

2024年，中电信量子获批组建安徽省量子信息产业创新研究院，争创国家级创新平台；入选国务院国资委首批启航企业。在技术研发与创新上，牵头成立“量子通信创新联合体”，推进关键技术协同攻关。在项目建设与应用中，中电信量子承建的“合肥量子城域网建设”入选国家数字中国建设典型案例，主持研发的“智慧法务量子视讯技术平台”获评安徽省信息化年度优秀项目。凭借“技术-产业-人才”发展模式入选新质生产力发展案例，在多领域发挥重要作用，推动量子信息产业发展。

国盾量子成立于2009年，作为专业的量子通信设备制造商和量子安全解决方案供应商，国盾量子的产品广泛应用于“京沪干线”等骨干网络，以及合肥、北京、上海等城市的城域网，深度赋能政务、金融、电力等关键领域，为这些行业的信息安全筑牢防线。

2024年在创新探索与合作实践方面，国盾量子携手中国电信等单位，共同推进“基于抗量子计算的城市级密钥分发基础设施建设及应用推广探索”项目，该项目成功入选上海市未来产业试验场“揭榜挂帅”项目。与此同时，上海电信量子城域网一期顺利建成，这一成果为向区域内的政企事业单位全面、高效地提供安全可靠的量子通信服务奠定了坚实基础，进一步推动量子通信技术在城市信息化建设中的深度应用。

硅臻成立于2020年，是一家专注于光量子集成芯片设计的公司。拥有20年光学集成芯片与量子密码实验室经验积累，研发团队专注于将量子光源、光量子操作及量子测量的核心通用部分集成到可扩展的光学芯片上。

2024年，硅臻研发的QRNG-10芯片成功通过国家密码管理局商用密码中心检测，突破了产业化应用的“尺寸关”，为产业化提供真量子熵源。此外，硅臻还与国芯科技共建联合实验室，推动量子技术与智能终端行业融合。



问天量子成立于2009年，由中科大与芜湖建投共同发起。依托中科院量子信息重点实验室，拥有多项行业级专利，是行业标准制订牵头单位。产品涵盖科研及教学产品、量子密码产品、量子密码管控产品、“量子+”产品和量子安防产品等5大系列，提供信息安全系统整体解决方案。

问天量子在量子随机数芯片技术上取得重大突破，其研发的量子随机数芯片成功通过国家密码管理局检测。这一检测通过意义非凡，意味着芯片在安全性、随机性、稳定性等关键指标上达到了国家密码行业的严苛标准，可广泛应用于数据加密、身份认证、数字货币等对安全要求极高的领域，为各行业信息安全提供坚实的量子级保障。



国科量子于2016年11月由中科院控股联合中国科大等在上海成立。作为国家级高新技术企业，是国际电信联盟部门成员。公司专注量子通信技术，建设国家广域量子骨干网等，推动量子与信息通信技术融合，牵头多项国内外标准制定。

2024年，国科量子通信网络有限公司申请一项名为“连续变量高斯调制压缩态量子不经意传输方法”的专利。该方法应用于量子通信领域，发送端生成相关序列制备压缩态量子序列发给接收端，接收端测量后生成位置集合反馈给发送端，双方协商生成加密密钥以保障信息安全，具有广泛的应用前景。



循态量子2017年孵化自上海交通大学量子感知与信息处理（QSIP）研究所，作为中国连续变量量子保密通信技术的先驱企业，矢志于将信息安全防护提升至量子层级。企业持续深耕连续变量量子密码技术研发与创新，构建完备的产品体系，塑造全栈式量子安全方案，凭借技术领先优势得到客户认可，为中国量子保密通信技术的发展与普及筑牢根基。

循态量子在产品开发和应用拓展方面，助力中国联通在第25届中国国际光电博览会发布通密一体量子（QKD）光传输设备；另外，推出自主研发的面向多场景融合的、集成化的QKD模块化产品QKD202系列产品及量子+X的系列融合性产品。此外，还推出了可实现一次一即时消息、音频通话等功能的强安全即通信产品信源密信(量子版)。其连续变量量子密钥分发技术及其产品成果入选《2024年度上海市网络安全产业创新攻关目录》。



苏州国芯成立于2001年，是聚焦自主可控嵌入式CPU技术研发与产业化的芯片设计公司。为客户提供芯片定制和自主芯片及模组产品，产品主要应用在信息安全、网络通信领域。

苏州国芯量子安全芯片A5Q与量子密码卡CCPUH3Q03内部测试成功。A5Q基于量子散粒噪声提取随机性，可用于量子安全类智能终端；CCPUH3Q03基于高性能密码芯片设计，适用于多种安全设备和云安全应用领域。新研发的量子安全芯片CCP907TQ也通过内部测试，内嵌自研CPU，采用量子随机数生成技术，数据加密性能最高达20Gbps，可用于量子安全网关等设备。

三未信安是密码基础设施提供商，成立于2008年8月，总部位于北京，在多地设有子公司或分公司。三未信安专注于密码关键技术的创新突破和核心产品的研发、销售及服务，致力于为网络信息安全领域提供全面的商用密码产品和解决方案，产品广泛应用于金融、能源、电信等众多行业及政府部门。

2024年，三未信安成功举办“探索无限量 安全新未来”密码创新大会，探讨传统密码技术在量子计算时代面临的安全挑战及应对策略，并发布《抗量子密码技术与应用白皮书（2024）》。同时，推出新一代抗量子密码系列产品，覆盖芯片、板卡、UKEY、密码机、网关、数字证书认证系统、密钥管理系统等全产业链产品，支持全系抗量子密码算法，为各行业应对量子时代密码安全需求提供有力保障。

格尔软件成立于1998年3月，是中国商用密码领域的骨干企业。格尔软件以公钥基础设施PKI为核心，致力于提供身份治理为中心的数字资产安全整体解决方案。

2024年，格尔软件启动全线密码产品的抗量子迁移工作，研发基于抗量子密码算法的系列基础产品，初步形成面向多领域的抗量子解决方案。在生态合作上，格尔软件联合多家量子技术企业成立G60量子密码应用创新中心，共建全产业链生态。同年11月，其抗量子密码安全认证网关通过中国信通院等机构的验证性测试，标志着该产品具备实用化条件，推动中国抗量子密码生态体系建设更进一步。

欧洲：多维布局，初创企业较多

图表 欧洲量子安全代表性厂商



光子盒研究院 QUANTUMCHINA | 2025.2

QTI Quantum Telecommunications Italy

QTI是意大利第一家量子通信公司，专注于量子密钥分发系统的研发与生产。其产品通过认证，能抵御经典和量子攻击，采用欧洲供应链生产。业务面向私企、政府和科研机构，曾为多地提供量子通信安全保障，目前正在广纳各类专业人才。

2024年，QTI公司在业务拓展、技术革新、战略合作等多维度取得了突破性进展。在科研合作方面，与意大利拉奎拉大学共同完成通过特殊先进光纤实现多维量子态量子通信的现实环境演示，为量子网络通信技术发展提供了理论与实践支撑。在技术交流方面，参加美国OFC 2024会议、2024年威尼托太空会议、欧洲量子技术会议（EQTC 2024）等重要会议活动，推动量子安全通信技术在不同场景的应用探讨。在应用拓展方面，QTI在“Guglielmo Marconi”活动、第50届G7峰会等场合进行现场演示或提供安全保障服务，验证了技术的可靠性与实用性。此外还与Sparkle、Telsy、MEO等公司合作，成功在雅典数据中心间建立高容量链路以及在里斯本进行陆地和海底光纤量子密钥分发安全通信试验。

意大利ThinkQuantum成立于2021年，源自于帕多瓦大学。由Officina Stellare等出资，核心成员多来自量子未来研究小组。公司专注量子通信与网络安全，提供量子密钥分发、量子随机数发生器等技术产品，产品能通过光纤、自由空间等实现安全通信，为客户提供可靠欧洲供应链。

ThinkQuantum在2024年世界移动通信大会上演示量子安全通信，展示了相关技术成果。并且成为IDQ推出的Clarion KX平台的生态合作伙伴，助力实现多厂商量子密钥分发互操作。此外，ThinkQuantum与Retelit、Telebit合作，成功完成将量子密钥分发用于光纤电缆数据加密的试验，验证了该技术在实际应用中的可行性，为通信安全提供更可靠保障，推动量子通信技术迈向新台阶。

德国KeeQuant公司成立于2020年，总部位于德国巴伐利亚州菲尔特。公司专注量子密钥分发技术，基于标准相干电信技术，运用集成光子学实现可扩展性，能抵御复杂攻击。公司产品涵盖量子密钥分发系统和密钥管理系统，服务关键客户，助力欧洲数字主权。

2024年KeeQuant在量子密钥分发领域稳步推进。1月参与维也纳QCI Days，展示相关技术；4月参加SQuaD-研讨会，积极投身行业交流。6月首次亮相AFCEA研讨会，作为量子密钥分发领域唯一参展商，凸显安全量子密钥分发技术在国防领域的关键价值。此外，公司持续研发，致力于将量子密钥分发设备小型化，计划从机架大小缩至公文包尺寸，以便于应用和推广，不断推动量子密钥分发技术向前发展。

德国Quantum Optics Jena成立于2020年，位于耶拿。专注量子技术，提供量子通信、成像等解决方案。以纠缠光子对进行防窃听通信，产品用于量子密钥分发等。

2024年获850万欧元A轮融资，活跃于多个国家，参与欧洲量子通信基建。Quantum Optics Jena在11月与区域网络运营商和电信服务提供商envia TEL一起在专家观众面前展示了其防窃听量子加密。这是量子技术提供商和DE-CIX节点首次在德国合作展示量子密码学。

西班牙LuxQuanta Technologies成立于2021年。作为ICFO的子公司，专注量子密钥分发技术。推出的首款商用产品Novalq为连续变量量子密钥分发系统。致力于将量子加密技术融入传统光通信设施，服务于电信、金融等多行业，为数据安全保驾护航。

LuxQuanta主导EIC加速器计划，获得250万欧元融资，为发展注入强大动力。开发由亚马逊网络服务支持的管理平台软件，提升量子密钥分发管理效率。在行业活动中，通过参加世界移动通信大会进行现场演示，展示技术实力。此外，与IDQ合作，推动量子安全解决方案部署；参与多供应商量子密钥分发演示，展现网络构建能力；携手多家企业测试低延迟光纤，探索量子密码新应用，全方位推动量子密钥分发技术的进步与拓展。

西班牙Quside成立于2017年，是巴塞罗那光子科学研究所的衍生公司。专注于量子随机数发生技术，提供量子熵芯片等产品。其产品有Nellit等多个系列，性能高且获NIST SP800-90B认证。

2024年，Quside被EIC Scaling Club评为欧洲高潜力深度科技扩展企业。在市场拓展上，与Altech Corporation签约以开拓亚太市场，与Equinix合作利用量子随机数技术防御网络攻击，还与Telefónica、IDEMIA合作为物联网设备部署量子安全方案，和西门子Cre8Ventures合作推动汽车领域技术进步。在技术认证与合作方面，量子熵源获NIST SP800-90B认证，并且与PQShield合作推出集成量子随机数发生器和抗量子密码学的加密解决方案。

英国KETS Quantum Security最初创办于英国布里斯托大学量子工程技术实验室。专注于量子安全通信技术研发，提供量子安全加密产品与解决方案。主要产品有量子密钥分发工具、量子随机数发生器。曾获英国创新署资助及310万英镑融资。

KETS Quantum Security赢得Innovate UK资助的170万英镑合同。该合同旨在推动其下一代量子密钥分发解决方案开发，项目聚焦于提供具备安全性、可扩展性和互操作性的量子密钥分发系统，以满足电信生产环境需求。



瑞士ID Quantique，2001年由日内瓦大学四位科学家创立。总部位于瑞士日内瓦，在多地设有办事处与实验室。是全球量子安全领域领导者，提供量子安全加密等解决方案，产品涵盖单光子探测器等，在60多国被广泛应用。

在产品研发上，推出紧凑自主的ID281 Pro超导纳米线单光子探测器系统，以及智能量子增强密钥交换平台Clarion KX，还开展长距离、高密钥率量子密钥分发研究，研发新型28像素并行SNSPD。

在合作拓展方面，和众多企业如HEQA Security、LuxQuanta等推出量子安全通信生态系统，助力量子网络推广。与Orange实现抗量子密码-量子密钥分发混合，和日内瓦大学共同研究SNSPD技术。与SK Telecom合作推出了三星第五代智能手机“Galaxy Quantum 5”。IDQ和BTQ Technologies签署谅解备忘录，共同研究和开发结合量子随机数发生器和抗量子密码学的身份验证系统。

在实际应用中，为阿丽亚娜6号提供监测设备，助力摩根大通实施高速量子安全网络，与GRNET等合作成功演示三节点量子密钥分发环网络，参与空芯光纤网络量子密码学测试。此外，与ORCA Computing合作融入单光子检测技术，与新加坡电信合作推出该国首个QSN，并举办研讨会推动量子安全迁移。

英国Quantum Dice成立于2020年，是牛津大学物理系的衍生公司。主要开发世界上首个紧凑且完全嵌入式的自认证量子随机数发生器，利用量子系统特性提供可信、安全的随机数。

Quantum Dice与BT Group探索量子随机数发生器在电信加密应用；和汇丰银行合作增强金融蒙特卡罗模拟；携手Channel Tools提供网络安全服务；支持IQN Hub推进量子安全网络。与SCI Semiconductor合作将量子加密技术引入高级安全系统，为多领域安全提供保障。此外，还入选Digital Catapult的数字安全设计技术访问计划，通过与各方合作，充分发挥其量子随机数发生器技术优势。QNu Labs的混合方法是融合量子和抗量子加密技术，实现面向未来的安全性。

英国PQShield成立于2018年，总部位于牛津。为硬件、软件和云提供量子安全加密解决方案，客户涵盖AMD等知名企业。在美国NIST的抗量子密码标准化项目中发挥重要作用，获多家机构投资。

2024年，PQShield凭借技术优势被评选为深度科技先锋，还受邀参加白宫会议，参与抗量子算法相关讨论。积极拓展业务，与日本多行业探讨合作，推动抗量子密码学应用。多次参与行业活动，包括硬件先锋Max 2024，提升行业影响力。在合作方面，与Si-Five、Cryptomathic等建立合作或战略联盟，推进抗量子加密技术发展与应用。同时，不断提升自身实力，获得FIPS 140-3认证，加入安全技术联盟、ADS集团、全球半导体联盟等组织，加强行业协作，加速行业发展，助力构建更安全的数字环境。

荷兰Q*Bird成立于2022年，是代尔夫特理工大学的衍生公司。专注量子安全网络技术开发，提供量子加密产品与解决方案。其核心产品Falqon可实现量子密钥分发。已获250万欧元融资，与鹿特丹港、Eurofiber等合作，在量子安全领域发展潜力巨大。

Q*Bird与Eurofiber达成合作，致力于将量子密钥分发技术融入其光纤网络，为多行业提供数据安全保障。Falqon技术在鹿特丹港进行世界首次试用，用于保护港口数字基础设施及对外通信，应对日益复杂的网络安全威胁。此外，Q*Bird携手SURF和Quantum Delta NL在乌得勒支成功部署多用户、多点对多点的量子密钥分发网络，该网络由Eurofiber提供光纤，连接多个关键地点，为科研教育领域的数据安全保驾护航，推动了量子安全网络的发展。

法国Cryptonext Security成立于2019年，位于巴黎。是由法国国家数字科学和技术研究所及索邦大学衍生出的公司。专注抗量子密码学，提供抗量子加密解决方案、加密库等产品。

CryptoNext Security与MBDA合作推进国防领域安全研究，和Tiempo Secure携手提升高端抗量子IP安全创新水平。参与法国2030计划宣传活动，助力法国量子研究发展。在技术标准方面，符合首个NIST标准，并积极参与相关验证与认证工作。凭借在量子安全领域的突出表现，被评为2024年IDC创新者。其技术还应用于法国银行和新加坡金融管理局的抗量子电子邮件系统实验，为金融通信安全提供保障，推动量子安全技术在实际场景中的应用。

法国Thales前身为Thomson-CSF，2000年更名。业务涵盖航空、航天、数字身份与网络安全等。拥有超2万项专利，多次入选全球创新百强等榜单。

Thales与Quantinuum合作推出抗量子密码入门套件。该套件为用户提供快速简便的测试和衡量抗量子准备情况的方式，以抵御量子计算攻击。它为企业提供可信环境，助其测试量子强化的抗量子加密密钥，理解量子计算对基础设施安全的影响。鉴于多数组织认识到量子计算对传统密码学的威胁，但很多尚未制定抗量子世界策略，此套件可让企业在可信实验室环境中测试各种安全用例，识别加密部署潜在弱点并改进IT基础设施。

芬兰Xiphera成立于2017年，位于埃斯波。是一家专注硬件加密安全的公司，在传统及抗量子密码技术上实力强劲。产品为基于FPGA和ASIC的加密IP核。广泛应用于通信、航天、物联网等领域，致力于为关键系统提供硬件层面安全防护。

Xiphera将在日本展示基于硬件的抗量子密码算法IP核，向市场展示其技术成果。已依据标准最终版本，对系列中的ML - KEM（Kyber）密钥封装机制和ML - DSA（Dilithium）数字签名IP核进行更新，确保产品符合最新标准。还推出nQrux安全启动硬件信任引擎系列中的新型安全启动解决方案，增强启动过程安全性，为系统提供抵御量子攻击的能力。

芬兰SSH Communications Security成立于1995年。是Secure Shell协议的发明者，在网络安全领域地位重要。提供加密传输、身份认证等安全服务，产品广泛应用于远程登录、文件传输等场景。客户遍布全球，为众多企业和组织保护关键数据与通信安全。

SSH Communications Security推出量子安全NQX 加密器3.0，支持最新量子安全加密算法，具备强大、可扩展、更安全的特性，满足数据传输需求。获批成为北约NCI机构供应商，参与其竞争采购，提升市场地位。宣布与多个伙伴建立合作，包括Deloitte Finland、Onaware等，覆盖多领域，助力业务全球拓展。与亚洲领先金融服务集团签署110万美元多年期安全通信协议，为其提供加密、密钥管理等服务，还将开展量子安全加密项目，推动业务增长。

澳大利亚：重点提供量子安全加密解决方案

图表 澳大利亚量子安全代表性厂商



光子盒研究院 QUANTUMCHINA | 2025.2

Quintessence Labs

QuintessenceLabs成立于2008年。公司旗舰产品有Trusted Security Foundation，还推出了qStream量子随机数发生器、qOptica量子密钥分发等产品

QuintessenceLabs在网络安全领域积极拓展业务。与Carahsoft达成合作，致力于为政府机构提供高性能的网络安全解决方案，助力提升公共部门应对常规和量子计算攻击的能力，保护敏感数据，增强网络安全性。同时，在Equinix的堪培拉数据中心部署了Trusted Security Foundation密钥和策略管理器设备，还计划向美国和亚太地区其他Equinix数据中心扩展，并且将通过推出虚拟密钥管理功能，推动全球业务扩张。QuintessenceLabs的qStream量子随机数发生器表现卓越，能生成1Gbit/s的真随机数，并提供100%的量子熵，为数据加密等应用提供了高度可靠的随机数源，可有效提升信息安全防护水平。

加拿大：多数企业选择发展抗量子密码

图表 加拿大量子安全代表性厂商



光子盒研究院 QUANTUMCHINA | 2025.2

QEYnet

Qeynet成立于2016年，总部位于安大略省旺市，由航天工程师和量子通信专家创立。致力于打造基于微卫星的全球量子密钥分发网络，以实现超安全通信，获加拿大政府等机构投资。

QEYnet参与了由滑铁卢大学牵头的项目，该项目获国防部和加拿大武装部队近300万美元资助，旨在开发下一代量子密钥分发网络技术，QEYnet将凭借卫星量子密钥分发专业知识助力项目推进。此外，QEYnet成功交付首个自由空间量子密钥分发系统，该系统被加拿大国家研究委员会用于一系列地面量子密钥分发网络实验。

Quantum eMotion成立于2012年。专注量子安全加密领域，基于谢尔布鲁克大学物理系研究成果拥有专利技术。开发量子随机数发生器等产品，为金融、军事等行业提供加密方案。

Quantum eMotion取得第一代量子随机数发生器微芯片的重大进展，还申请基于量子的区块链钱包专利，为加密货币钱包安全提供保障，并推出创新硬件钱包技术。获得ISO/IEC 27001网络安全认证，提升自身安全管理水平，在印度获得关键专利，增强全球知识产权组合。因开创性的量子安全通信解决方案在量子世界大会获认可，参与加拿大贸易代表团前往菲律宾推进全球扩张，还部署量子安全平台以满足美国医疗网络安全新提议标准。

Crypto4A Technologies成立于2016年。专注于下一代网络安全。提供量子安全硬件安全模块等产品，具备加密灵活性、移动性和可扩展性。可用于云、物联网等多领域，曾获FIPS 140-2 3 +级验证，助力构建安全的数字未来。

Crypto4A Technologies与多方合作开展智能电网项目，聚焦量子技术、深度学习等在智能电网中的应用，提升电网安全性。推出创新硬件安全模块QxHS，其具备独特优势，可适应技术发展需求。获得NIST算法标准认证，彰显技术实力。推出的Quantum-Safe HSM平台软件版本4.4，支持NIST抗量子密码算法，功能升级，还获权威机构认可。Crypto4A Technologies与南安大略省联邦经济发展局达成合作，将投资750万美元用于实施量子安全制造计划，致力于推动量子安全领域在制造方面的发展。

ISARA成立于2015年，总部位于安大略省。是一家专注网络安全的公司，提供量子安全加密解决方案。推出了ISARA Radiat等产品。曾获加拿大政府战略创新基金资助，拥有56项专利。

ISARA和TOPPAN Digital、NICT合作开发出SecureBridg智能卡系统，采用混合方法支持抗量子密码学和当前公钥密码学。鉴于当前公钥算法未来可能受量子计算机威胁，而向抗量子密码过渡又需时间，该系统应运而生。它支持NIST公布的ML - DSA等算法，能在系统过渡的不同阶段进行身份验证，已在NICT的医疗系统试点测试中证实了有效性。三方计划2025年在医疗、金融等领域进行有限的实际应用，2030年全面部署，还将拓展在多领域的应用。

Quantropi于2018年在渥太华成立。专注量子安全数据通信，其Qi Spac平台提供Masq、Qeep、Sequr等产品，可实现量子安全非对称加密、对称加密及量子密钥分发等功能，获诸多奖项与行业认可。

Quantropi作为ST合作伙伴计划成员，将抗量子加密技术引入STM32。随着AI使量子计算机攻击效率提升，Q-day可能提前至2025年，抗量子加密技术需求增大。Quantropi的QiSpace平台提供系列解决方案，如uLoadXLQ保护固件启动、应用层。

InfoSec Global于2009年成立，总部位于多伦多。是一家网络安全服务提供商，专注于下一代灵活数据安全。其Agile Crypto Platform可实现加密资产全面管理等功能，与Synopsys等合作，拥有超14项核心专利。

InfoSec Global与Utimaco合作，助力企业应对抗量子密码学迁移挑战，加强加密风险管理；与1touch.io合作，整合数据与加密管理，保护敏感数据。参加NIST会议小组讨论，参与推动行业发展。推出与Utimaco的集成解决方案，提升加密可视性和管理能力。参与网络研讨会，探讨公私部门加密弹性建设。与Zühlke建立战略伙伴关系，结合双方优势，为客户提供全面加密资产管理服务，开拓抗量子密码应用新领域。

BTQ于2021年在列支敦士登成立。是抗量子区块链技术领域企业，提供量子安全、可验证脚本等服务。产品包括Kenting、PQ Scale等。技术团队由密码学等领域专家组成。

BTQ和IDQ签署谅解备忘录，将共同研发融合量子随机数发生器和抗量子密码学的创新身份验证系统。BTQ开发的抗量子密码签名算法Preon获NIST认可。此次合作旨在开拓基于量子随机数发生器和抗量子密码学的身份验证系统新市场，推动网络安全技术发展，保障关键任务网络在量子时代的安全。

印度：
代表性企业较少，处于探索阶段



QNu Labs是印度首家运用量子密钥分发技术开发量子网络安全产品的公司，2016年创立，总部位于班加罗尔，在美国马萨诸塞州设有子公司。公司推出Armos、Tropos等产品，获政府资助与多方投资，致力于提供量子安全网络技术，业务面向全球。

QNu Labs在2024年印度移动通信大会上展示突破性的量子安全加密解决方案。同时，宣布地理扩展计划，旨在将量子加密解决方案推向美国及其他主要市场，开拓更广阔的业务版图。此外，还获得印度政府认可并入选国家量子计划，这有助于其获取更多资源支持，进一步推动公司在量子加密领域的发展，提升其行业影响力。

日本：
部分企业拥有多年技术经验



Toshiba正在全球开发利用数字和量子技术的业务，拥有20多年量子技术研究经验。在量子密钥分发领域技术领先，如开发出世界首个基于芯片的量子密钥分发系统、实现超600公里光纤TF-QKD等，积极推动量子技术商业化。

在量子密钥分发方面，Toshiba与Orange评估了其与传统数据信号的共存及高速加密传输；和软银演示光无线通信的量子密钥分发操作；与Ciena在OFC展示量子安全通信；携手Single Quantum扩展长距离部署能力；还联合BT Group、Equinix提供数据中心间的量子安全连接。同时，TOSHIBA研发出可量产的量子随机数发生器，推动了量子安全技术的广泛应用。此外，和SpeQtral与ST Engineering签署备忘录，加速东南亚量子安全通信解决方案的发展。

新加坡：注重量子安全应用合作



SpeQtral成立于2017年。公司专注于量子密钥分发和抗量子密码技术，提供基于光纤和卫星的量子安全产品与服务。业务遍布多个地区，服务超100个国家客户。曾与东芝、ST Engineering等合作，推动量子安全通信发展。

SpeQtral推出移动量子光地面站TarQis，降低卫星量子密钥分发技术使用门槛。与Antaris合作部署量子安全密钥分发卫星；和Arquimea签署战略谅解备忘录，探索量子安全解决方案与卫星技术融合。与Qosmosys携手开拓月球量子通信。和东芝为新加坡企业展示量子安全解决方案，并在纽约建立卫星量子密钥分发接收节点保障金融服务安全。与多方开展量子安全合作，参与新加坡金融领域应用研究。还与东芝、ST Engineering合作加速东南亚量子安全通信发展，并交付符合太空标准的量子密钥分发系统用于新加坡-英国联合卫星任务，推动量子通信技术迈向新高度。



07

产业分析预测

目录 07 产业分析预测

01 量子密钥分发五年内有望翻一番

02 多场景应用拓展，量子随机数发生器稳步上扬

03 标准引领技术，抗量子密码至2030年飙升十几倍

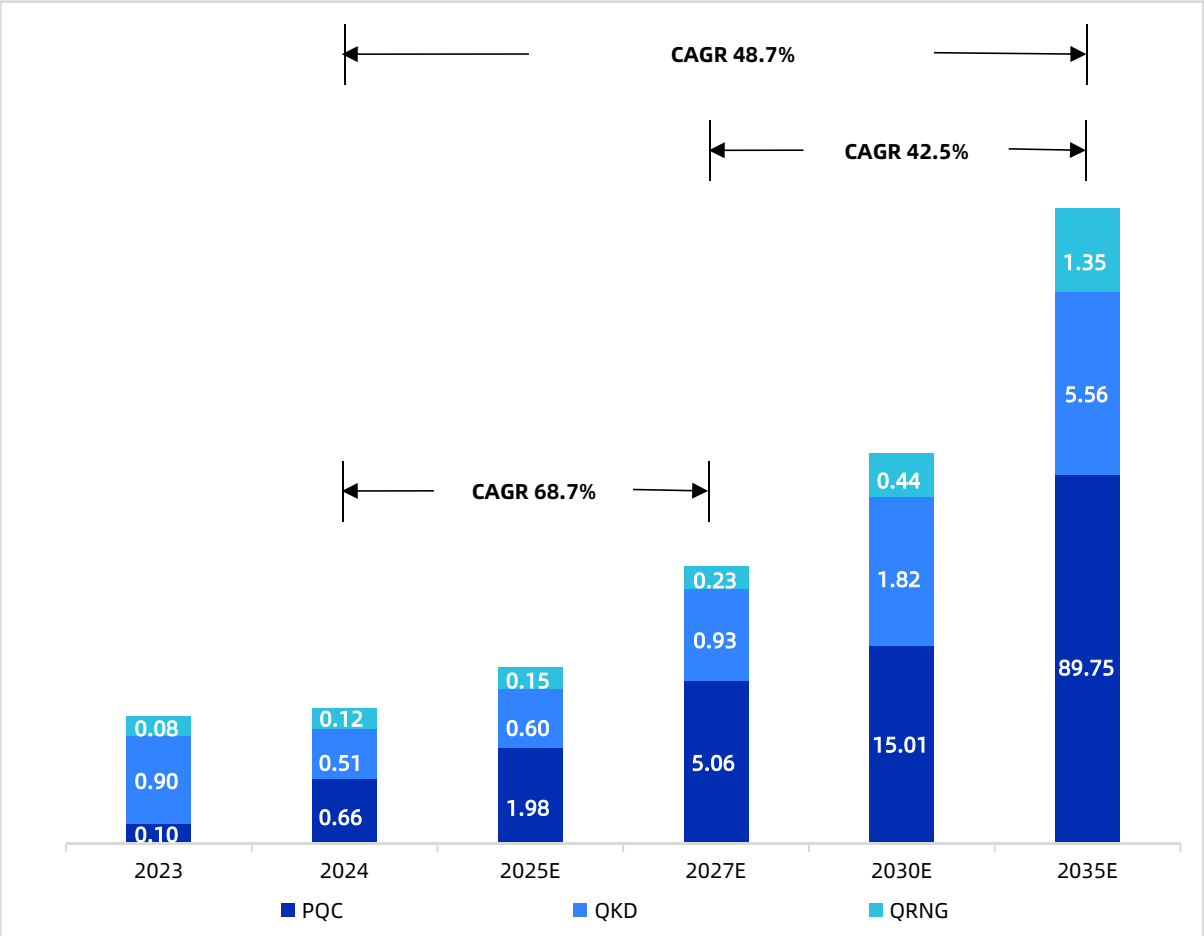
全球产业规模分析预测

2024年全球量子安全产业规模进一步扩大，体现出产业发展的加速态势，标志着量子安全领域正吸引更多资源投入，市场对其关注度和认可度显著提升。

从长期趋势看，预计到2035年将达到966.6亿美元，2024-2027年期间年复合增长率约为68.7%，2027-2035年期间年复合增长率约为42.5%。整体呈现出保持较高增长水平的趋势，显示出产业广阔的发展前景。

从细分领域视角审视，量子密钥分发成功扭转2024年的下行态势，自此开启逐年上扬的增长曲线；量子随机数发生器则呈现出稳健攀升的发展态势，尽管增长步伐相对平缓，却始终保持稳定增长的势头；而抗量子密码更是异军突起，迎来爆发式增长，展现出强大的发展潜力。

图表 全球量子安全产业规模预测（2023-2035E, 单位: 十亿美元）



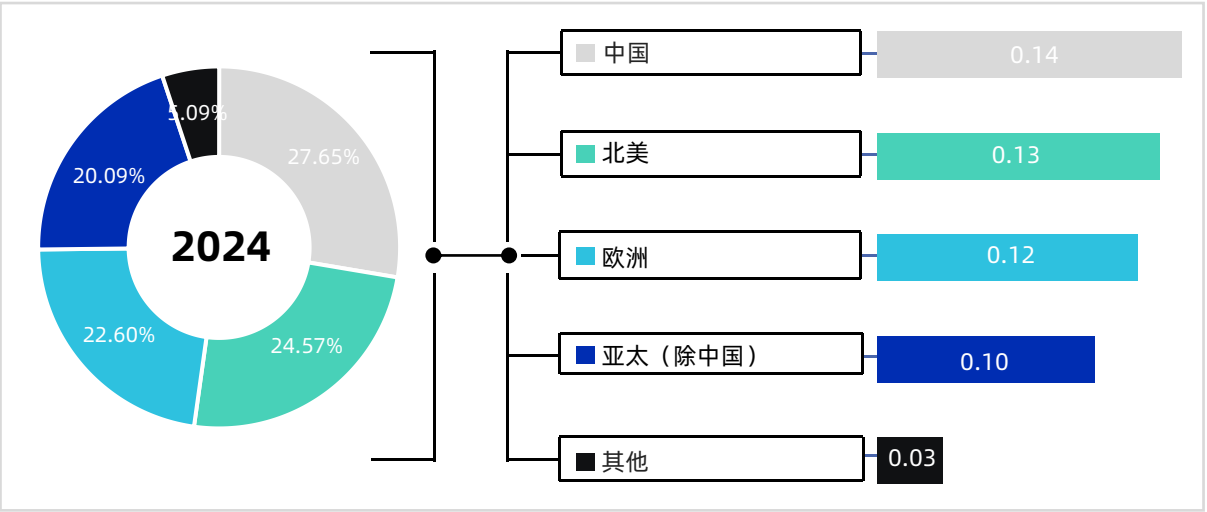
ICV TA&K & 光子盒研究院 QUANTUMCHINA | 2025.2

01 量子密钥分发五年内有望翻一番

量子密钥分发产品技术历经发展已趋于成熟，量子密钥分发2024年规模为5.09亿美元，作为保障信息传输安全的关键技术，量子密钥分发产品未来的发展方向将深度融入不同领域，为安全通信构建更为全面且创新的解决方案。预计到2030年将增长至18.21亿美元，2024-2030期间年复合增长率约为24.22%；2035年达到55.58亿美元，2030-2035期间年复合增长率约为25.01%，持续保持稳定增长。

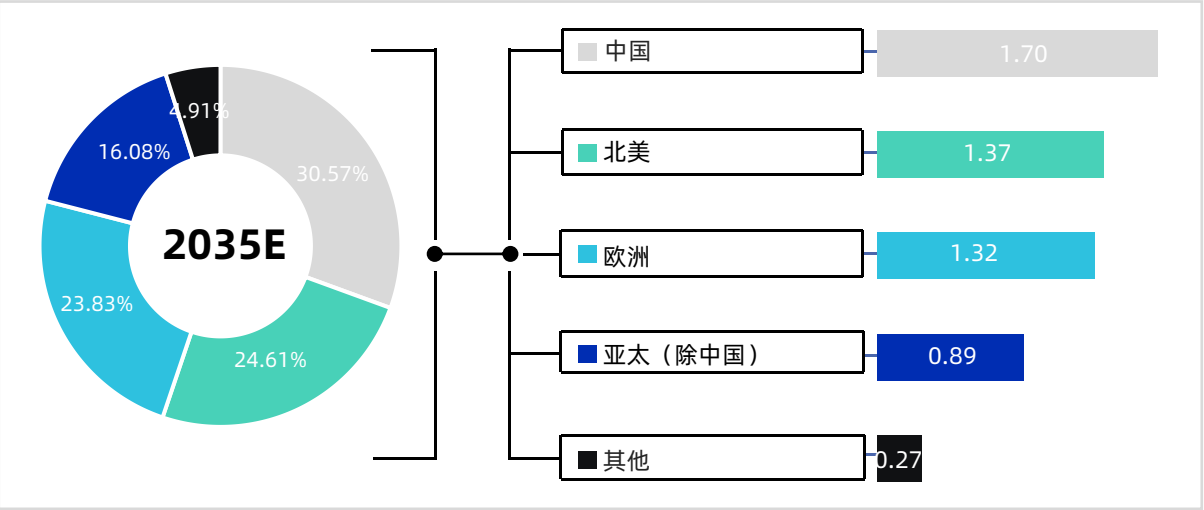
2024年，中国在全球量子密钥分发产业规模中占比领先，北美、欧洲、亚太（不含中国）也占据较大份额。到2035年，中国持续领跑，且占比进一步提升。各地区产业规模均呈增长态势，其中中国增长幅度更为突出，显示出强劲的发展势头和巨大潜力。

图表 2024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 & 光子盒研究院 QUANTUMCHINA | 2025.2

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 & 光子盒研究院 QUANTUMCHINA | 2025.2

从全球来看，国防军工领域应用份额占比较大且逐年递增，电信、金融领域也稳步增长，电力领域份额有所下降。在中国市场，国防军工份额不断提升，铁路领域增长趋势显著，将在2025-2035年快速上升。电信和电力领域份额呈下降态势，而政府服务领域份额则逐步增长。这些领域份额的变化，反映出不同行业对量子密钥分发技术的需求差异与发展态势。

图表 全球量子密钥分发下游应用预测（2024-2035E）

分部份额	2024	2025E	2030E	2035E
国防军工	25.85%	26.11%	26.64%	27.03%
电信	10.42%	10.53%	10.62%	10.88%
政府服务	10.22%	11.71%	12.11%	12.29%
电力	21.36%	16.41%	15.56%	15.32%
金融	16.41%	17.55%	18.30%	18.57%
铁路	12.64%	15.41%	15.00%	14.69%
其他	3.10%	2.28%	1.77%	1.22%

ICV TA&K & 光子盒研究院 QUANTUMCHINA | 2025.2

图表 中国量子密钥分发下游应用预测（2024-2035E）

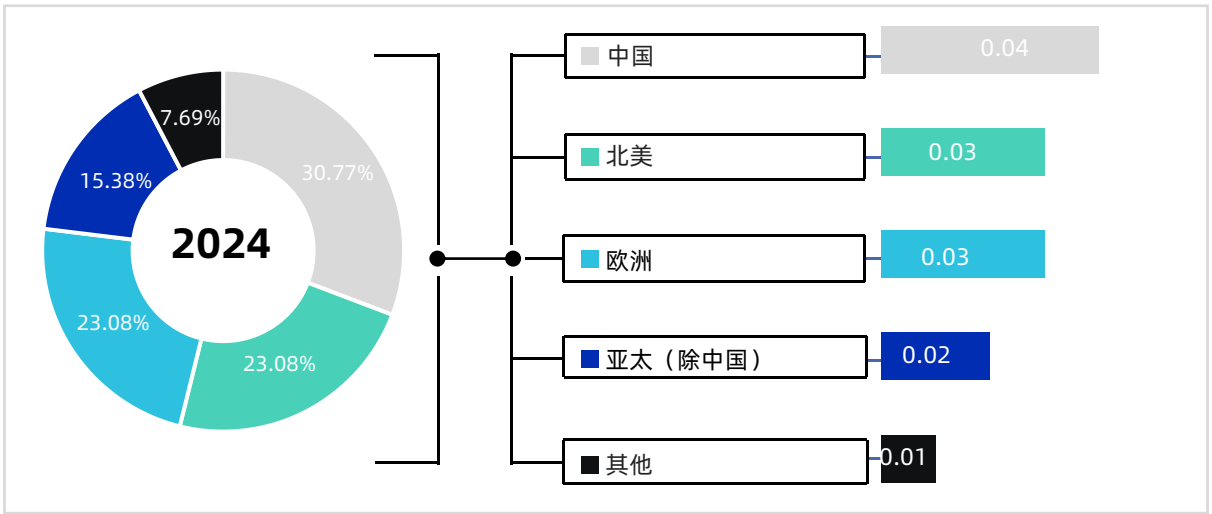
分部份额	2024	2025E	2030E	2035E
国防军工	21.41%	25.75%	27.32%	27.48%
电信	12.82%	9.96%	8.77%	8.04%
政府服务	10.06%	10.54%	13.31%	15.51%
电力	23.90%	17.54%	15.42%	14.10%
金融	14.81%	13.39%	13.01%	12.56%
铁路	12.84%	19.81%	20.27%	20.36%
其他	4.16%	3.01%	2.78%	1.95%

ICV TA&K & 光子盒研究院 QUANTUMCHINA | 2025.2

02 多场景应用拓展，量子随机数发生器稳步上扬

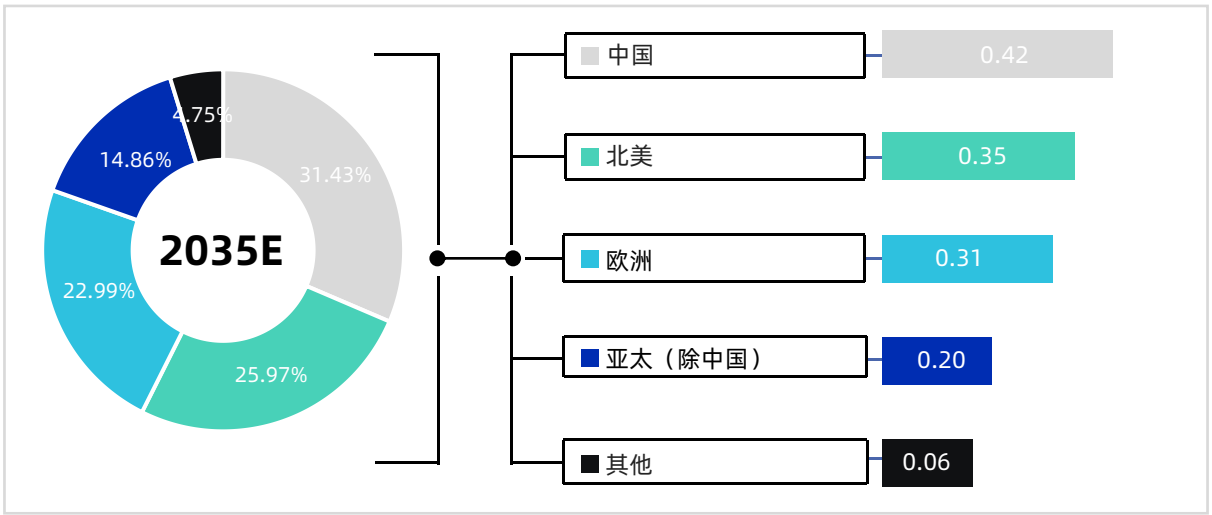
近年来，量子随机数发生器芯片技术取得了显著进展，通过不断创新的制造工艺和材料优化，其尺寸不断缩小，成本大幅降低，这使得芯片得以在多个关键领域广泛应用。量子随机数发生器2024年规模为1.16亿美元，虽在整体产业中占比相对较小，但也在稳步发展。预计到2030年将增长至4.42亿美元，2024-2030期间年复合增长率约为25.23%；2035年达到13.47亿美元，2024-2035期间年复合增长率约为24.49%。随着量子随机数在密码学、模拟等更多新兴领域的应用被挖掘，其市场规模有望逐步提升。

图表 2024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 & 光子盒研究院 QUANTUMCHINA | 2025.2

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 & 光子盒研究院 QUANTUMCHINA | 2025.2

在2024年全球量子随机数发生器的产业格局中，中国处于领先位置，以一定优势领先于北美和欧洲。亚太（不含中国）地区以及其他地区的产业规模相对较小。到了2035年，这种区域间的位次关系基本保持稳定，中国仍占据首位，北美和欧洲紧随其后，各地区间的相对比例差异没有出现剧烈变动，显示出该领域竞争格局具备一定的稳定性。

从时间维度的发展趋势来看，2024年至2035年期间，全球各个主要地区的量子随机数发生器产业规模均呈现出显著的增长态势。这意味着在未来一段时间内，量子随机数发生器领域在全球范围内都将是一个快速发展的赛道，无论是领先的中国、北美和欧洲，还是规模相对较小的亚太（不含中国）及其他地区，都将迎来产业扩张的机遇，反映出该技术在全球范围内受重视程度不断提升，应用前景广阔。

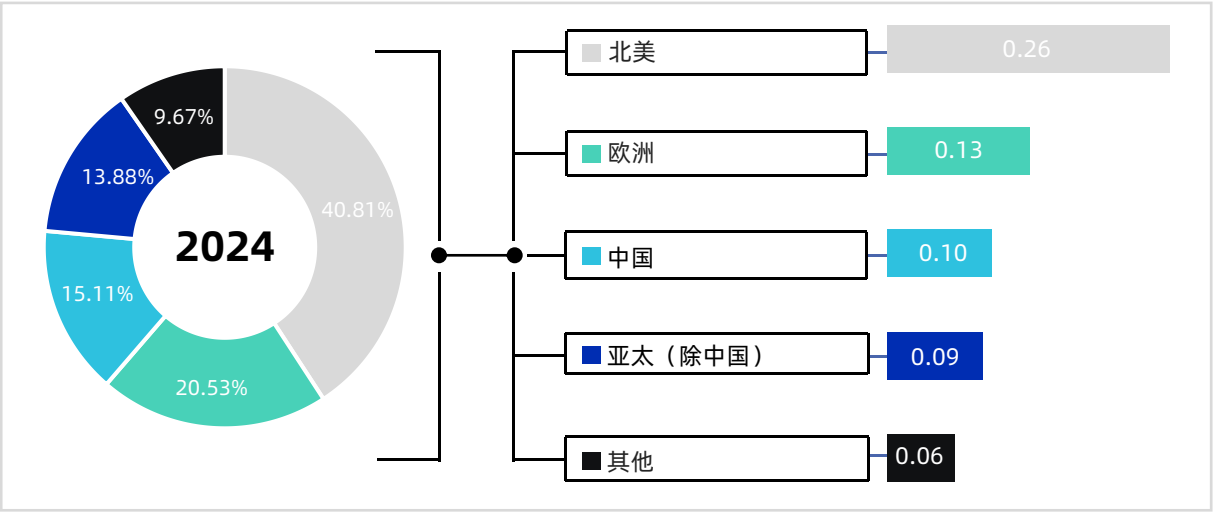
2024年，量子随机数发生器与抗量子密码的结合成为行业内备受瞩目的发展趋势，有望成为推动市场规模扩大的关键因素。量子随机数发生器能够为抗量子密码提供高度真随机的高质量随机数，而抗量子密码则凭借这些随机数生成更为安全的密钥，从而有效抵御量子计算带来的威胁，满足当下日益增长的安全需求。这种创新性的结合正推动相关技术在更广泛的商业和工业应用中落地生根。不少企业敏锐捕捉到这一趋势，积极投入研发基于量子随机数发生器和抗量子密码的混合加密解决方案，力求实现更高水平的数据安全保障。

预计在未来几年，随着技术的不断成熟、应用场景的持续拓展，以及与抗量子密码结合的深入发展，量子随机数发生器市场规模将持续扩大。在产业结构方面，随着市场规模的扩大，量子随机数发生器的产业链将更加完善，上游的芯片研发制造、中游的设备生产以及下游的应用服务等环节都将迎来新的发展机遇。尤其在终端应用领域，随着各行业对数据安全重视程度的不断提高，对量子随机数发生器相关产品和服务的需求将持续增长，这将进一步推动产业规模的扩张。

03 标准引领技术，抗量子密码至2030年飙升十几倍

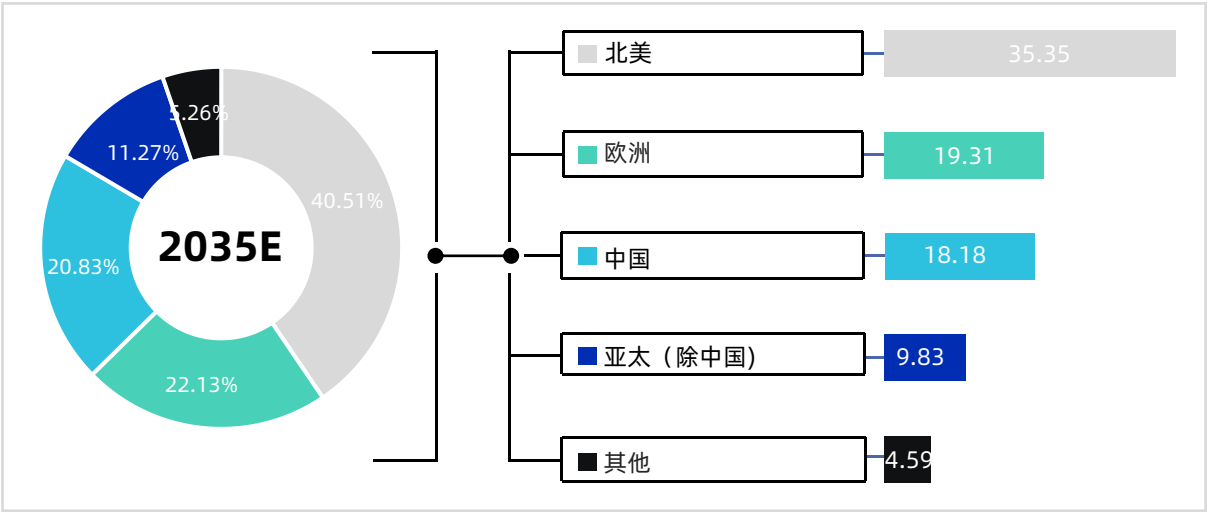
抗量子密码2024年产业规模增长迅速，为6.56亿美元，随着美国NIST首批抗量子加密正式标准的发布，这一年成为抗量子密码全行业发展的关键转折点，此后行业发展驶入快车道。随着量子计算技术的发展，传统密码面临被破解的风险，抗量子密码技术成为应对这一挑战的关键，受到市场的高度关注。预计到2030年将飙升至150.08亿美元，2024-2030期间年复合增长率约为72.64%；2035年更是高达897.46亿美元，2024-2035期间年复合增长率约为51.97%。未来，随着量子计算威胁的临近，各行业对抗量子密码技术的需求将呈爆发式增长，成为推动全球量子安全产业规模快速扩张的核心力量。

图表 2024年全球各地区抗量子密码产业规模（单位：%，十亿美元）



ICV TA&K & 光子盒研究院 QUANTUMCHINA | 2025.2

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 & 光子盒研究院 QUANTUMCHINA | 2025.2

从地区对比上进一步看，2024年北美产业规模远超其他地区，优势显著。欧洲与中国的规模有一定差距，亚太（除中国）和其他地区则规模相对较小。到2035年，北美依旧领先，但中国与欧洲的规模大幅提升，尤其是中国增长迅猛，与欧洲的差距缩小，且远超过亚太（除中国）地区。

从趋势角度，全球各地区抗量子密码产业规模都呈爆发式增长，说明随着时间推移，抗量子密码技术受重视程度不断提高，应用场景逐渐拓展，市场需求快速上升。同时，各地区增长势头强劲，反映出抗量子领域的发展潜力巨大，未来可能成为全球抗量子密码产业的重要力量，推动全球产业格局的变化。

抗量子密码作为对当前密码体系的升级与加固方案，正逐渐崭露头角。在早期阶段，它对现有安全产业的冲击较小，不过从长远来看，其具备替代现有安全软件或安全芯片的潜力。随着量子计算机技术的飞速发展，对抗量子密码的应用将起到极大的推动作用。一方面，量子计算机性能的提升使得现有传统密码面临更大的被破解风险，从而促使各行业急切寻求抗量子密码的保护；另一方面，量子计算机的发展也会带动相关技术产业链的完善，为抗量子密码的发展提供更坚实的技术支撑和产业环境。



08

产业展望

目录 08 产业展望

01 全球争相布局量子通信卫星网络

02 量子保密通信基础设施建设仍然是核心

03 量子安全科技成果创新与产业规模不断扩大

04 多国逐步部署后量子密码的迁移工作

05 抗量子密码与量子密钥分发结合，扩大量子安全防护力度

06 技术创新要求标准化工作全面落实、持续推进

07 量子保密通信与人工智能、神经网络的创新协同

08 量子安全与量子计算、量子传感的多重融合

01 全球争相布局量子通信卫星网络

量子通信卫星网络已成为各国在通信安全领域的战略重点。卫星网络能够突破地面量子通信的距离瓶颈，实现洲际甚至全球范围的超远距离量子密钥分发，构建起全方位、无死角的安全通信链路。全球各主要科技国积极参与其中，目的在于抢占未来通信安全的技术制高点，强化自身在信息交互过程中的安全保障能力。

当前卫星量子通信领域展现出多维度的强劲发展趋势。在技术创新上，不断朝着更轻便、高效的方向突破。

致力于减轻卫星重量以降低发射成本与难度

英国爱丁堡市会议批准并提供250万英镑资助，由赫瑞瓦特大学、布里斯托尔大学、斯特拉斯克莱德大学和约克大学合作购买望远镜，在爱丁堡的大学研究园建立枢纽光学地面站，旨在演示和测试卫星量子安全通信，并对抗网络攻击。

提升卫星载荷性能，增强通信质量与稳定性

新加坡SpeQtral推出移动量子光学地面站（Q-OGS），命名为TarQis，旨在通过卫星量子密钥分发降低安全通信的门槛。TarQis将与SpeQtral即将推出的量子卫星无缝协作，使用户能快速熟悉和测试卫星量子密钥分发技术，验证使用案例，为在机构中部署和集成量子密钥分发解决方案做好准备。

由德国弗劳恩霍夫应用光学与精密工程研究所（IOF）领导的CubEniK项目为“立方体卫星”（CubeSat）开发出迄今最小的卫星载荷，可以用于基于卫星的量子密钥分发。

各地区加强合作，打造量子卫星网络

加拿大利用量子卫星网络测试量子通信协议。滑铁卢大学的量子计算研究所（IQC）成功开发了一种量子源，名为ReFQ，将被用于量子加密和科学卫星（QEYSSat）。QEYSSat将是加拿大首个量子卫星，将测试参考框架独立的量子通信协议，为未来的全球量子通信网络奠定基础。

荷兰TNO启动了Qu-STAR项目，携手空客，共同设计量子卫星网络。

韩国SDT和釜山大学已完成技术小型化和改进，计划通过FPGA基的光波混合和Hong-Ou-Mandel干涉的自动测量来验证设备性能，并推进原子基量子光源设备的最终产品化。

在量子保密通信组网方面成果显著

通过成功研制并发射“墨子号”量子科学实验卫星，中国在国际上率先实现了星地量子通信，有力地验证了利用卫星平台实现全球化量子通信的可行性。

中国还成功构建了世界上首个广域量子通信网络，该网络集成了700多条地面光纤量子密钥分发链路以及两个卫星对地自由空间高速量子密钥分发链路。网络覆盖四省三市共32个节点，接入了金融、电力、政务等多个行业的150多家用户。

此外，中国在实时空对地量子安全通信方面也取得初步成效，不仅减轻了卫星的运行负担，还借助双向复用的卫星-地面光通信系统实现了实时的空对地安全通信，使量子通信系统具备更强的灵活性，能够为政府、企业、武装力量和研究机构等提供服务。

随着越来越多的国家参与到量子安全领域，未来有望形成一个覆盖全球、坚不可摧的量子通信网络，彻底重塑全球信息安全格局，为人类信息交互的安全与稳定提供强有力的保障。

02 量子保密通信基础设施建设仍然是核心

量子保密通信基础设施是实现量子安全的关键基础，需要资金、先进技术以及广阔市场作为坚实后盾。

全球各主要科技国积极加强合作，大力投入，推动了量子通信基础设施建设

美国橡树岭国家实验室（ORNL）宣布和美国查塔努加电力和电信解决方案公司EPB成立新的能源弹性和量子科学合作组织，并获得1.8亿美元资金。

中国电信推进量子安全基础设施与云网基础设施深度融合，加快量子技术的商业化进程。

对基于基础设施的量子密钥分发技术自主研发的重视程度不断攀升

掌握自主研发的量子密钥分发技术，能有效减少对外部技术的依赖，确保通信安全自主性，牢牢掌握核心技术优势。

比利时国家研究网络Belnet已成功建立所需的基础设施，并与比利时imec和UGent一起实现了第一个量子密钥分发链接。

阿联酋航天局宣布与阿布扎比先进技术研究委员会的技术创新研究所（TII）签署战略合作协议，将基于阿联酋自主研发的量子密钥分发技术，建立一个全面的量子通信基础设施。

随着全球范围内量子密钥分发基础设施持续拓展，量子通信网络的覆盖范围得以扩大，稳定性也显著提升。目前，全球已有超30个国家在部署或已实施量子密钥分发基础设施建设，为量子保密通信技术在不同国家和地区的应用提供有力支撑。从欧洲到亚洲，从美洲到中东，各地区的积极参与使量子通信网络初步成型。它宛如一张坚固的安全防护网，为金融领域的大额资金交易、军事领域的机密情报传输、政务领域的重要文件流转等提供安全保障。

而这仅仅是开端，未来随着基础设施的进一步完善，量子保密通信将深度融入社会生活的各个方面，下游应用诸如智能交通系统的安全调度、医疗领域患者隐私数据的保护、物联网设备间的安全通信等，都拥有着巨大的发展潜力，有望开启一个全新的安全通信时代。

03 量子安全科技成果创新与产业规模不断扩大

在商业化布局方面，量子安全产业链正逐步完善，已具备初步商用条件。量子通信技术的应用场景不断拓展，从最初的金融、国防、政务等对信息安全要求极高的领域，逐渐向智慧城市、物联网、5G通信、人工智能等新兴领域延伸。随着量子通信基础设施的不断完善，如国家广域量子保密通信骨干网络的建设，量子通信的网络覆盖范围和稳定性得到了显著提升，为规模化应用奠定了基础。

在科技成果创新方面，2024年，量子安全行业成绩斐然。量子密钥分发技术作为当前最为成熟且应用广泛的量子通信技术，为数据加密提供了极高的安全保障。其基于量子力学原理，能够在通信双方之间生成绝对随机且理论上不可窃听、不可破解的密钥，极大地增强了数据传输的安全性。在实际应用中，从金融机构间大额资金转账的信息安全防护，到政府部门机密文件传输的保密需求满足，量子密钥分发技术都发挥着关键作用。例如，中国循态量子助力中国联通发布的通密一体量子（QKD）光传输设备以及推出的自研基于接入OTN场景的QKD模块化QKD202系列产品，大大提升了量子保密通信网络部署便捷性，降低了建设和运维成本，为量子保密通信技术大规模商业化部署开辟了新的道路。

在实际应用方面，从金融机构间大额资金转账的信息安全防护，到政府部门机密文件传输的保密需求满足，量子密钥分发技术都发挥着关键作用。例如，循态量子助力中国联通发布的通密一体量子（QKD）光传输设备以及推出的自研基于接入OTN场景的QKD模块化QKD202系列产品，大大提升了量子保密通信网络部署便捷性，降低了建设和运维成本，为量子保密通信技术大规模商业化部署开辟了新的道路。

在产业规模扩大方面，众多量子安全相关企业在技术研发与产品创新上持续突破。例如，中国国盾量子则专注于量子通信网络的构建与优化，成功实现了长距离、高稳定性的量子链路传输，为城域、广域量子通信网络的建设奠定了坚实基础，在市场拓展方面成效显著。中国中电信量子充分利用自身在通信基础设施领域的深厚积累，将量子通信技术与传统通信网络进行深度融合，推动了量子通信技术在民用通信市场的广泛应用，进一步扩大了市场版图。

未来，随着量子卫星通信技术日益成熟，有望打破地域限制，实现全球范围的量子网络覆盖，为跨国、跨洲的数据安全传输提供有力支撑。同时，在量子计算技术快速发展的背景下，促使量子通信技术不断升级创新，企业积极探索大规模商业化应用路径，开拓更广阔的市场空间，共同推动量子安全产业规模实现跨越式增长。

04 多国逐步部署抗量子密码迁移工作

随着量子计算技术迅猛发展，量子计算机对现有加密体系构成潜在威胁，全球多国逐步在关键领域部署抗量子密码学迁移工作，以保障信息安全。预计到2025年，这一趋势将愈发显著。

美国在推进抗量子密码学标准化算法的同时，也实施了一系列配套政策措施，以确保平稳过渡到更安全的加密技术。这些措施旨在为从传统加密算法向抗量子密码迁移的工作提供全面保障。

一方面是抗量子密码算法的安全性评估。抗量子密码算法主要集中在寻找一类或多类在量子计算攻击下的NP数学困难问题，而目前仅是利用Shor算法和Grover算法本身或其优化算法作为攻击的源算法。随着量子计算的发展，存在产生新的量子算法的可能性，或将再次颠覆现有的抗量子密码算法体系。因此，在抗量子算法的选择、试点探索、应用部署等任一阶段，针对已知和未知攻击的安全性评估将一直是抗量子密码研究的重要方向。

另一方面是抗量子密码迁移应用验证探索。美国国家安全局（NSA）已发布了抗量子迁移时间表，使用已遴选出的基于格、哈希函数的签名的抗量子算法作为基础开展抗量子迁移，它们与现有经典密码算法相比均存在尺寸更大、资源消耗更多的情况。因此，有必要探索抗量子密码迁移所需软件和硬件平台极限，提前研究能同时兼容经典密码与抗量子密码的可自适应的密钥管理系统、密钥分发系统、终端硬件平台，实现向抗量子迁移的平稳过渡。

除美国外，加拿大、日本、韩国、澳大利亚和荷兰等国家也发布了各自的抗量子密码迁移计划和指南。中国对抗量子密码算法迁移工作重视程度不断提升，在金融、通信、国防等重点领域已开展相关标准或国家重点课题研究。但与国际先进水平相比，中国存在参与主体较少、产业链关键环节有短板、不同领域工作协同性不强等问题，导致整体进度相对滞后。

此外，与抗量子密码配套的硬件市场增长潜力巨大。虽重点在算法，但也离不开硬件辅助，众多芯片及安全相关公司纷纷入局。例如，德国Infineon开发实现NewHope算法的非接触式智能卡芯片，德国Utimaco的硬件安全模块（HSM）可生成并安全存储加密密钥。目前，已有众多顶尖芯片设计和网络信息安全公司将抗量子密码列为重要发展方向。

05 抗量子密码与量子密钥分发结合 扩大量子安全防护力度

量子密码技术以物理学、光学为理论根基，在采用一次一密时，能实现信息论证明的绝对安全，有效抵御量子计算的超高并行算力。

当前量子密钥分发技术存在一些亟待解决的实用化难题

其一，小型化、低成本、高速率、远距离等系列技术有待突破。

其二，因其与经典密码学实现基础截然不同，难以直接与现有通信网融合。

而抗量子密码技术正处于提升过渡阶段，尽管在算法研究和硬件实现上取得一定进展，也有硬件加速器提升内存利用率，但仍面临算法性能需优化、与现有系统兼容性欠佳、硬件支持不足等问题。

因此，探索量子密钥分发技术与抗量子密码技术互补，构建能保护特定关键基础设施、抵御量子攻击的密码网络，对未来做好网络安全防护意义重大。

部分运营商走在结合抗量子密码和量子密钥分发技术的前列

韩国移动通信运营商SK电讯将自主研发的抗量子密码软件集成到了量子加密公司IDQ发布的量子密钥分发系统“Clavis XG”上，产品主要是采用双重加密技术来保护信息，即在同一设备上同时进行量子密钥分发和抗量子密码加密。

新加坡电信（Singtel）宣布将扩展其量子安全产品套件，将抗量子密码学技术集成到国家量子安全网络（QSN）中，为企业提供更为强大的网络安全保障。同时，解决方案将结合抗量子密码和量子密钥分发技术，支持Singtel开发安全、可扩展的QSN。

此外，量子密钥分发和抗量子密码两种技术并非“二选一”的零和博弈，而是能够实现优势互补。

从下游应用来看，存在以下现实问题

一方面，量子密钥分发存在远距离成码率低，网络建设周期长、投资高、服务能力有限，缺乏规模效应，安全标准与测评体系不完善等困境。

另一方面，抗量子密码算法性能有待优化，与现有系统及不同方案间兼容性差，密钥管理复杂，专用硬件研发滞后，硬件与软件协同优化不足。

未来，新型安全认证方案可借助抗量子密码简化量子密钥分发在复杂网络环境下的身份认证和密钥管理；量子密钥分发则为抗量子密码等公钥体系提供无法提供的无条件安全性，进一步保障量子保密通信网络系统的安全性，还能提升量子保密通信网络的经济性与便利性，极大地推动量子保密通信的应用与推广。

06 技术创新要求标准化工作全面落实持续推进

加密标准是信息安全的重要保障。标准化工作是实现量子安全大规模产业应用的必要前提，其中抗量子密码标准化工作尤为关键。2024年，美国NIST在抗量子密码标准化方面取得了重要进展。首批三项抗量子加密标准的制定为抗量子密码算法的广泛应用奠定了基础，确保了加密系统在量子时代的安全性。

然而，在抗量子密码标准化及应用进程中，仍存在一些阻碍。部分抗量子密码标准缺乏清晰的实施指南，致使在适配与兼容性上存在短板。比如，现有的网络协议和安全技术标准（像TLS、SSH等）需要调整和更新，以适配抗量子密码算法，支持新的密钥交换机制与抗量子身份验证方法。同时，软件加密库（如OpenSSL等）和加密硬件模块（如HSM、TPM等）也需要升级换代或重新设计，从而支持新算法并确保高效运行。

以美国NIST的CRYSTALS-KYBER、FALCON、CRYSTALS-Dilithium和Sphincs+4个抗量子密码标准化算法为例，除Sphincs+是基于哈希函数的签名算法外，其余均为基于格的密码算法。

中国同样投入大量科研力量，聚焦基于格的密码算法研究。然而，抗量子密码算法除了基于格、哈希函数、多变量、编码的技术路线，还有基于同源曲线的技术路线。因此，有必要拓展更多抗量子密码算法体制的研究方向，以积极应对充满未知的量子计算世界。毕竟密码学源于数学，探索密码学与数学的跨学科融合，借助现代数学理论推动密码学研究拓展，探寻新的数学困难问题，有助于研制具有自主技术特色的抗量子密码体制。

未来，在开拓新算法技术路线之后，还需深入研究抗量子密码算法在量子条件下的安全性证明，切实保障算法面对潜在量子攻击时的安全性。一方面，研究算法针对现有及可能出现的量子攻击的安全强度评估，估算其攻击复杂度；另一方面，研究抗量子密码结构的可证明安全分析方法，通过设计针对性的量子安全模型，研究量子证明工具来简化安全证明流程，同时开展计算机辅助证明技术研究，如形式化证明技术等。

07 量子保密通信与人工智能、神经网络创新协同

未来几年，量子保密通信与人工智能、神经网络的融合势必成为技术发展的热点方向。从技术原理来看，人工智能凭借强大的算法优化能力，能够对量子密钥分发协议进行深度调整，从而提升其效率与安全性。比如，通过机器学习算法可以更精准地分析量子密钥分发过程中的噪声、干扰等因素，进而动态调整分发策略，确保密钥的安全、高效传输。

神经网络在量子通信领域也有着独特的应用价值，其强大的模式识别能力可用于量子通信信号的识别与分类。在复杂的通信环境中，量子通信信号容易受到各类噪声的干扰，神经网络能够对接收的信号进行智能分析，准确区分有效信号和噪声，提高通信的可靠性。

二者协同合作，有望攻克量子通信面临的诸多难题

加拿大Scope Technologies等为北美医疗保健提供商提供量子安全数据解决方案和AI驱动工具，将授权使用Scope的量子抗性加密和去中心化存储解决方案，旨在保护患者数据，同时通过先进AI改善诊断和治疗方案。

中国上海交通大学、上海量子科学研究中心、合肥国家实验室等合作研究，引入基于长短期记忆（LSTM）神经网络的载波恢复策略优化自引用连续变量量子密钥分发系统。实验中，该方法使过量噪声减少近50%，密钥率大增，是中导多路复用系统的替代，适用于片上及星地通信。

爱沙尼亚QANplatform已成为IBM的官方业务合作伙伴，并推出了QAN Q-Cluster——一个利用AI进行日志异常检测的防篡改和自我审计系统，结合抗量子区块链技术以实现数据的可证明耐用性和持久性，为政府、银行、金融、医疗保健和供应链领域提供服务，保护敏感交易数据并确保符合监管要求。

未来，量子安全技术与人工智能、神经网络的结合将形成一种灵活的“混搭”模式，以适应更广泛的应用需求。然而，随着技术协同程度的加深，恶意行为者可能利用AI策划更复杂、更有针对性的攻击。因此，有必要将AI驱动的威胁检测和自动化响应能力融入量子网络安全框架中，建立起更加完善、智能的安全防护体系，保障量子保密通信与人工智能、神经网络融合发展的安全与稳定。

08 量子安全与量子计算、量子传感多重融合

目前，量子安全、量子计算与量子传感的融合已成为量子技术发展的重要趋势之一。而在这一融合趋势下，资源共享和科研合作将成为关键驱动力。通过整合各方资源，研究机构和企业能够在量子技术的研发上形成合力，共同推动量子技术的进步。

量子安全和量子计算的融合为算力网络带来了新资源

量子优化、量子搜索、量子信号处理和量子机器学习等技术，能够显著提升网络能力和业务质量。通过量子云平台，第三方应用与服务得以拓展，为部分应用场景带来了颠覆性的改变。美国西北大学研究人员成功在互联网光缆上进行量子隐形传态实验，IBM公司实现跨QPU协同运行超大规模量子电路，这些成果都展示了量子安全和量子计算融合的潜力。

未来，这一融合趋势将继续在提升量子计算系统性能、推动标准化工作等方面取得新的进展。中国启科量子承接中国移动通信有限公司研究院的“面向通信网络的量子算法优化与验证研究”项目，旨在完成分布式量子近似优化算法（QAOA）的优化与验证，进一步推动量子计算技术在通信网络中的应用。

量子安全与量子传感的融合同样具有广泛的应用前景

量子传感技术凭借其超高的测量精度和准确度，为量子安全中的关键参数测量提供了有力支持。例如，量子传感器能够精确测量光子的相位、偏振等量子态参数，从而提高量子通信系统的性能。

此外，量子传感技术还可以用于实时监测和调整量子安全系统中的量子态，提高系统的稳定性和可靠性。中国北京大学与北京邮电大学研究团队在200公里商用光纤上实现了微波钟飞秒级同步，显著降低了附加不稳定性，这一成果对于提高量子通信链路的时间同步精度具有重要意义，有助于提升量子通信的效率和准确性。

在产业层面，企业和研究机构的合作将推动量子密钥分发技术的标准化和商业化进程。标准化的建立能够确保不同厂商的产品和服务之间的兼容性和互操作性，降低市场准入门槛，促进市场的健康发展。商业化则能将量子安全技术推向更广泛的应用场景，加速其在各行业的落地。

总的来说，量子安全、量子计算与量子传感的多重融合正重塑科技格局。未来三者的融合，将在提升测量精度、构建测评体系等方面取得更多突破，在金融、通信、科研等领域释放出巨大潜能，推动各行业迈向更安全、高效的发展阶段。



09

附件

目录 09 附件

01 量子生态成熟度罗盘（Q-EMC）

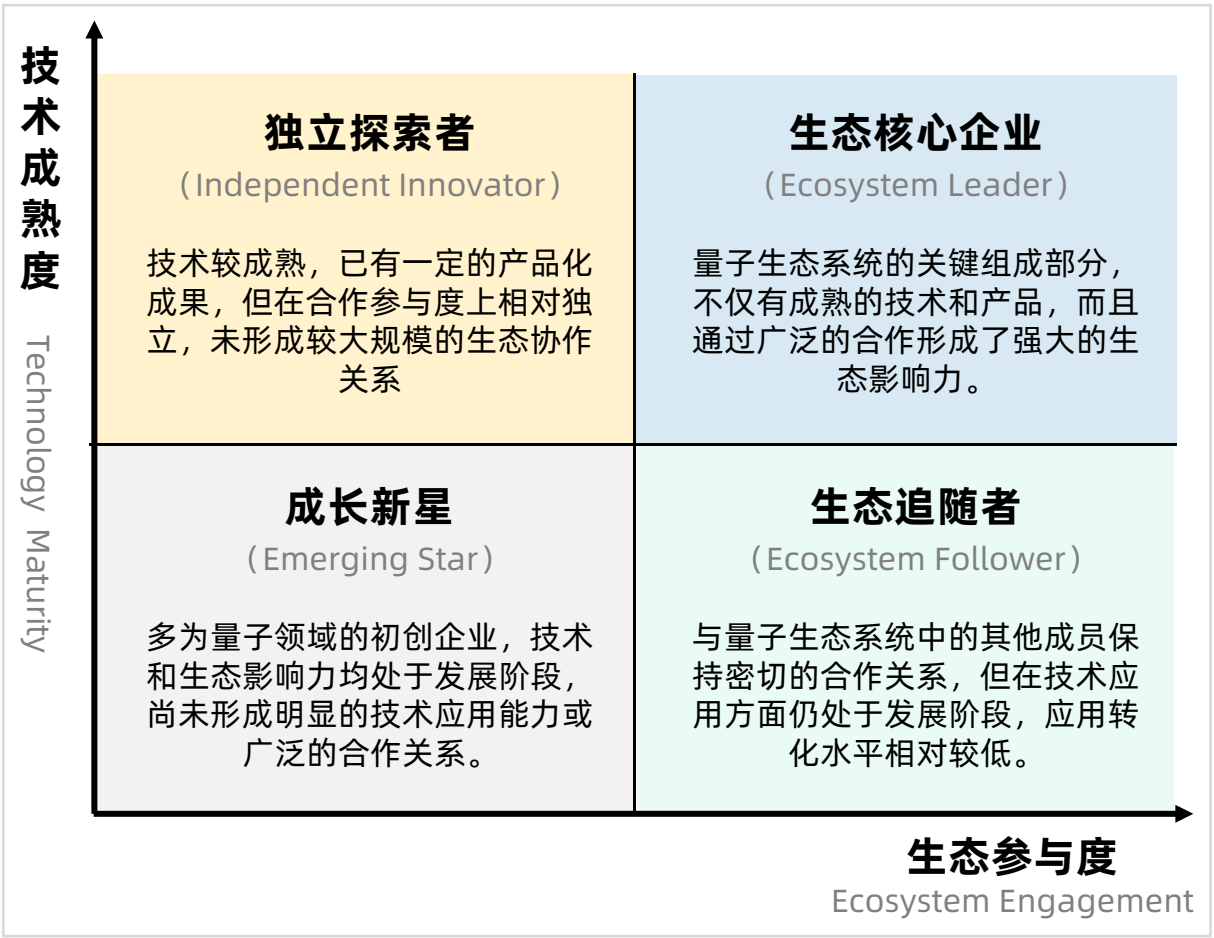
02 2024年政府主导的量子资助项目

03 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）



光子盒研究院 QUANTUMCHINA | 2025.2

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《2025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、2024年技术进展等；生态参与度具体权重指标包括2024年合作进展情况、标准制定情况、联盟情况等。

02 2024年政府主导的量子资助项目

9月，加拿大专注于量子安全通信技术开发的公司Quantum Bridge宣布被纳入加拿大政府的快速通道政府采购计划。此前，加拿大政府对该公司的对称密钥分发系统（SDS）进行了全面测试。

10月，日本总务省宣布，将于2025年开始推进下一代密码技术“量子密码通信”的实际应用。东芝、日本电气等公司已被选为该项目的候选企业。总务省将鼓励开发可远距离、高速度使用的技术。这项工作将从2025年开始，共花费五年时间，计划投入数百亿日元。此外，总务省计划在2030年之前完成技术的国产化，并建立网络攻击防御系统。

11月，英国政府创新署Innovate UK宣布，将提供资金支持量子网络项目，以加速技术发展并消除商业化障碍。项目申请者需识别关键技术障碍并提出创新解决方案，对量子网络项目的资助金额高达100万英镑。项目周期为8至12个月，申请者需为英国注册企业，项目工作和成果应用需在英国进行。

11月，印度科技部部长宣布，通过国家量子任务和国家跨学科网络物理系统任务已经选定了八家量子领域初创公司，并将为它们提供资助。这八家公司包括：量子通信公司QNu Labs等。此外，部长还指出，量子技术的进步将为金融系统提供无与伦比的保护，确保在线交易的安全，以应对日益严重的网络威胁。

12月，加拿大BTQ Technologies宣布将从加拿大国家研究委员会工业研究援助计划（NRC IRAP）获得高达15万美元的资金。这笔资金将用于支持“利用分布式共识算法实现安全共享量子随机数发生”的研发项目，该项目旨在开发用于安全量子随机数发生的分布式共识算法，并将其作为一种可靠的服务。随机数生成在密码学以及科学模拟技术的诸多应用中都处于核心地位，并且在区块链、电信和金融等行业至关重要。BTQ计划寻求更多的研发资金并开展合作，扩大其在加拿大量子网络安全生态系统中的影响力。

12月，英国赫瑞瓦特大学在首届光子学和量子加速器（PQA）首轮资助中获得三项项目资助，PQA是一项470万英镑的计划，旨在推动苏格兰光子学和量子技术发展。这些项目涉及量子通信、光网络和半导体设备，显示了赫瑞瓦特大学在这些领域的领导地位。这些成果不仅促进了研究成果的工业转化，还支持了技术熟练劳动力的发展，预期到2030年，苏格兰光子学行业产值将超过40亿英镑。这些项目的资助凸显了赫瑞瓦特大学在推动创新和实现经济社会效益方面的积极作用。

03 参考链接

https://arxiv.org/abs/2303.15795
https://www.nature.com/articles/s41566-023-01166-4
https://terraquantum.swiss/news/terra-quantum-breaks-records-in-quantum-key-distribution-paving-way-to-offering-unprecedented-security-over-existing-fiber-optic-networks-globally
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.130.030801
https://www.nature.com/articles/s41534-023-00754-0
https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.20.024048
https://www.quantum-dice.com/quantum-dice-and-speqtral-unveil-quantum-communication-developments-with-zenith-qrng-for-speqtral-1-mission/
https://www.pnas.org/doi/10.1073/pnas.2205463120
https://eprint.iacr.org/2022/1713
https://sjzyj.ah.gov.cn/szjh/zxdt/40654579.html
https://www.qusecure.com/qusecure-uses-starlink-for-post-quantum-cryptography-in-satellite-to-earth-communications/
https://www.thalesgroup.com/en/worldwide/group/press_release/thales-pioneers-post-quantum-cryptography-successful-world-first
https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-pioneers-quantum-protection-for-ai-powered-fx-trading
https://newsroom.accenture.com/news/2023/qusecure-and-accenture-team-in-first-successful-multi-orbit-communications-link-showcasing-post-quantum-crypto-modernization
https://pqshield.com/pqshield-partners-with-tata-consultancy-services-and-eshard/
https://www.honeywell.com/us/en/press/2023/09/honeywell-leverages-quantum-computing-encryption-keys-to-bolster-utilities-data-security-against-cyber-threats
https://www.cpnn.com.cn/qiye/jishu2023/202307/t20230712_1617341.html
https://www.aliroquantum.com/blog/real-world-quantum-network-deployments
https://www.hpcwire.com/off-the-wire/qrypt-partners-with-lanl-to-advance-quantum-random-number-generation-tech/
https://www.softbank.jp/en/corp/news/press/sbkk/2023/20230228_01/
https://uploads-ssl.webflow.com/637deec5b8a2a6508d3d1159/6409fce19d51fcd809735ede_20230309-PR-Cryptonext%20Quandela-VDef.pdf
https://newsroom.ibm.com/2023-05-10-IBM-Unveils-End-to-End-Quantum-Safe-Technology-to-Safeguard-Governments-and-Businesses-Most-Valuable-Data
https://www.wisekey.com/press/wisekey-and-sealsq-develop-ai-based-quantum-solutions-demonstrator-for-post-quantum-cryptography/
https://ir.quicklogic.com/press-releases/detail/672/securing-the-future-quicklogic-and-xiphera-partner-to
https://www.qusecure.com/qusecure-earns-validation-in-amazon-web-services-partner-network-apn-quprotect-awarded-aws-qualified-software-certification/
http://www.chinatelecom.com.cn/news/06/5G/zxdt/202311/t20231121_78632.html
http://www.chinatelecom.com.cn/news/03/202311/t20231130_78883.html
http://www.chinatelecom.com.cn/news/03/202311/t20231114_78015.html
http://www.chinatelecom.com.cn/news/06/5G/zxdt/202311/t20231121_78637.html
https://www.zdxlz.com/newsDetail.html?id=23
https://mp.weixin.qq.com/s/W2Zo-VwWElnjLf38oyIz2Q
http://www.10086.cn/aboutus/news/groupnews/index_detail_46753.html
https://arqit.uk/press-releases/arqit-bt-and-fortinet-launch-quantum-safe-vpn-to-protect-against-evolving-cyberthreats
https://www.idquantique.com/sk-telecom-and-samsung-unveil-the-galaxy-quantum-4/
https://www.telekom.com/en/media/media-information/archive/deutsche-telekom-leads-build-of-high-security-communications-network-for-the-eu-1026404
https://newsroom.orange.com/frances-industry-quantum-startups-academic-and-institutional-players-join-forces-to-build-the-future-of-the-french-quantum-internet-communication-system/?lang=en

https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Kryptobibliothek-Botan/kryptobibliothek-botan_node.html
https://www.etsi.org/events/2117-2023-02-9th-etsi-iqc-quantum-safe-cryptography-workshop
https://www.tc260.org.cn/front/postDetail.html?id=20230616154140
https://www.ding-lab.com/archives/3rd-pqc-asia-forum
https://www.nict.go.jp/press/2023/03/14-1.html
https://www.koit.co.kr/news/articleView.html?idxno=114989
https://www.global.toshiba/ww/news/digitalsolution/2023/11/news-20231124-01.html
https://doi.org/10.1103/PhysRevApplied.20.044005
Orangehttps://www.toshiba.eu/quantum/news/toshiba-europe-and-orange-demonstrate-viability-of-deploying-quantum-key-distribution-with-existing-networks-and-services/
https://www.global.toshiba/jp/news/digitalsolution/2023/09/news-20230920-01.html
https://www.global.toshiba/jp/company/digitalsolution/news/2023/0705.html
https://www.global.toshiba/content/dam/toshiba/ww/ir/corporate/news/20231219_1.pdf
https://www.idquantique.com/docusign-qscd-appliance-embedding-idq-qrng-chip-fips-140-2-level-3-approved/
https://www.idquantique.com/id-quantique-kcs-and-sk-telecom-release-a-new-quantum-enhanced-cryptographic-chip-at-mwc23/
https://www.idquantique.com/sk-telecom-and-samsung-unveil-the-galaxy-quantum-4/
http://www.itnewsonline.com/PRNewswire/ID-Quantique-joins-EAGLE-1-Europes-pioneering-quantum-key-distribution-initiative/923595
https://www.idquantique.com/packetlight-and-id-quantique-announce-successful-integration-of-quantum-key-distribution-in-packetlight-devices/
https://www.idquantique.com/singtel-quantum-safe-network/
http://www.quantum-info.com/News/qy/News/qy/2023/2023/1123/770.html
http://www.quantum-info.com/News/qy/News/qy/2023/2023/0317/746.html
http://www.quantum-info.com/News/qy/News/qy/2023/2023/1122/764.html
http://www.quantum-info.com/News/qy/News/qy/2023/2023/1122/766.html
http://www.quantum-info.com/News/qy/News/qy/2023/2023/1123/771.html
http://www.quantum-info.com/News/qy/News/qy/2023/2023/1123/772.html
https://cs.com.cn/cj2020/202312/t20231213_6380372.html?bsh_bid=5976552742
https://www.newindianexpress.com/business/2023/dec/15/quantum-cybersecuritystartup-raises-usd-65-mnin-pre-series-a1-funding-round-2641784.html
https://economictimes.indiatimes.com/news/defence/qnu-labs-bags-contract-from-indian-navy-for-quantum-encryption-systems/articleshow/100796060.cms
https://www.indianeconomicobserver.com/news/accops-qnu-labs-unite-to-harness-quantum-advancements-for-enhanced-cybersecurity20231127124701/
https://speqtralquantum.com/newsroom/speqtral-collaborates-with-archangel-lightworks-to-develop-quantum-enabled-optical-ground-station
https://speqtralquantum.com/newsroom/speqtral-and-sptel-appointed-to-build-nqsn-singapores-first-nationwide-quantum-safe-network
https://speqtralquantum.com/newsroom/speqtral-and-toshiba-forge-deeper-partnership-amidst-landmark-national-quantum-safe-network-plus-nqsn-project
https://speqtralquantum.com/newsroom/quantum-dice-and-speqtral-unveil-quantum-communication-developments-with-zenith-qrng-for-speqtral-1-mission
http://www.qudoor.com/index.php?c=show&id=165
http://www.qudoor.com/index.php?c=show&id=162
http://www.qudoor.com/index.php?c=show&id=151
http://www.qudoor.com/index.php?c=show&id=137
http://www.qudoor.com/index.php?c=show&id=129
http://www.qudoor.com/index.php?c=show&id=128
http://www.qudoor.com/index.php?c=show&id=122
http://www.qudoor.com/index.php?c=show&id=125
http://www.qudoor.com/index.php?c=show&id=139
https://qudice.eu/developing-quantum-communications-in-space-for-the-future-euroqci/
https://www.luxquanta.com/quantum-secure-networks-partnership-25m-project-with-more-than-40-partners-n-33-en

https://www.nature.com/articles/s41598-024-51212-6
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.132.047001
https://doi.org/10.1103/PhysRevA.109.012401
https://doi.org/10.1126/sciadv.adk3258
https://kns.cnki.net/nzkhtml/xmlRead/xml.html?pageType=web&fileName=WLXB202406032&tableName=CJFDTOTAL&dbCode=CJFD&topic=&fileSourceType=1&taskId=&from=&groupId=&appId=KNS_BASIC_PSMC&act=&customReading=&invoice=r4YuFeGpvzEscSZu9juU7n7cZPHHOO9tA9eiGAdLla+AebMqZAZRjFCkFBHa2UiZ8BaPipXmpzW7FYsX6msPKC9u8sO8rtBiYTlzMmS6dlboJlyyX1dLKR8M21RPNMlfoMOiNM/iIgqsrkpUsK+Eq4DDP+V/hX5ESUkxCb9Vojs=
https://kns.cnki.net/nzkhtml/xmlRead/xml.html?pageType=web&fileName=HWYH202401007&tableName=CJFDTOTAL&dbCode=CJFD&topic=&fileSourceType=1&taskId=&from=&groupId=&appId=KNS_BASIC_PSMC&act=&customReading=&invoice=rrw6Rua2EW6PJmkLwJ9OYOA0VZi/tO7o6dHJD0CtE5BaSEFZbSy2fnIhcf/N35zyC/DEwhlU/OAVwRFBccaKCazr4kkgHqGUYYiMBn2bb7POIWepwTF2XNvDJSdwJhI7xA6Bw/+9UX9lUEBCXuozweIiKAo4ZjgdLZbfsy6zJwU=
https://doi.org/10.1038/s41534-023-00800-x
https://www.nature.com/articles/s41567-023-02319-6
https://doi.org/10.1103/PRXQuantum.5.010303
https://doi.org/10.1126/sciadv.adi9474
https://arxiv.org/abs/2402.09108
https://doi.org/10.1103/PhysRevApplied.21.024012
https://doi.org/10.1103/PhysRevA.109.022416
https://doi.org/10.1103/PhysRevA.109.022424
https://doi.org/10.1038/s41598-024-52987-4
https://doi.org/10.1038/s41467-024-45876-x
https://doi.org/10.1364/OL.514837
https://www.nature.com/articles/s41534-024-00812-1
https://ele.pku.edu.cn/info/1012/3032.htm
https://phys.org/news/2024-03-world-closer-quantum-communication-global.html
https://www.nature.com/articles/s41586-024-07125-5
https://www.dtu.dk/english/newsarchive/2024/04/100-kilometres-of-quantum-encrypted-transfer
https://www.idquantique.com/idq-launches-quantum-safe-communication-ecosystem/
https://www.jpmorgan.com/technology/news/firm-establishes-quantum-secured-crypto-agile-network
https://quantumcomputingreport.com/terra-quantum-demonstrates-qkd-over-a-1707-km-1060-mile-fiber-optic-cable/
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.132.260802
https://www.imec-int.com/en/press/new-leap-belgian-quantum-communication-infrastructure-imec-ugent-and-belnet-realise-first-qkd
https://www.nature.com/articles/s41377-024-01488-0
https://opg.optica.org/optica/fulltext.cfm?uri=optica-11-6-883
https://www.163.com/dy/article/J6B57GFS05565EU3.html
https://www.quantum-info.com/News/qy/2024/2024/0724/809.html
https://www.sciencedirect.com/science/article/pii/S2667325823003047
https://www.mas.gov.sg/news/media-releases/2024/mas-collaborates-with-banks-and-technology-partners-on-quantum-security
https://ieeexplore.ieee.org/document/10628025
https://spacenews.com/german-cubesat-to-test-quantum-key-distribution/
https://arxiv.org/abs/2408.10994
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.133.120803
https://digital-strategy.ec.europa.eu/en/news/eu-invests-eu65-million-quantum-chips
https://journals.aps.org/pra/abstract/10.1103/PhysRevA.110.032401
https://www.nature.com/articles/s41467-024-52086-y
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.133.110801
https://journals.aps.org/pra/abstract/10.1103/PhysRevA.110.032413
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.133.110201
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.133.120804

https://www.quantinuum.com/press-releases/quantinuum-together-with-mitsui-advance-unforgeable-quantum-tokens-over-fibre-network-in-first-ever-trial
https://www.miit.gov.cn/zwgk/zcwj/wjfb/gg/art/2024/art_4e789ceb8ef64b49a67d0764bd219aec.html
https://journals.aps.org/prresearch/abstract/10.1103/PhysRevResearch.6.043196
https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.22.054082
https://www.gruppotim.it/en/press-archive/market/2024/PR_Telsy_QTI_and_MEO_QKD_Lisbon.html
https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.22.064018
https://mp.weixin.qq.com/s/G5NI9bI3uA8Tp1tCL_uJyw
https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.22.064037
https://journals.aps.org/prresearch/abstract/10.1103/PhysRevResearch.6.043269
https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.22.064057
https://www.etnews.com/20241206000151
https://www.eurofiber.com/press/eurofiber-partners-with-quantum-bridge-and-juniper-networks-to-enhance-quantum-safe-infrastructure-solutions/
https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.5.040345
https://journals.aps.org/prresearch/abstract/10.1103/PhysRevResearch.6.043300
https://journals.aps.org/prresearch/abstract/10.1103/PhysRevResearch.6.L042067
https://journals.aps.org/prresearch/abstract/10.1103/PhysRevResearch.6.043316
https://mp.weixin.qq.com/s/Wlyp9gleXjFXe1VlgZr81g
https://www.toshiba.eu/quantum/news/toshiba-creates-quantum-random-number-generation-ready-for-mass-manufacture/
https://pqshield.com/quside-and-pqshield-announce-integration-to-deliver-quantum-safe-cryptography-with-superior-randomness-generation/
https://www.quantum-dice.com/quantum-dice-and-sci-semiconductor-announce-partnership-to-bring-quantum-backed-cryptography-to-advanced-security-systems/
https://www.dongascience.com/news.php?idx=68790
https://mp.weixin.qq.com/s/coxS05FBDbflh15Ky78DRw
https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.5.030307
https://www.science.org/doi/10.1126/science.adp6016
https://www.nature.com/articles/s41598-024-74702-z
https://www.nature.com/articles/s41598-024-76220-4
https://www.nature.com/articles/s42005-024-01828-x
https://www.nature.com/articles/s41534-024-00910-0
https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.22.054045
https://journals.aps.org/prapplied/abstract/10.1103/PhysRevApplied.22.054070
https://www.nature.com/articles/s44310-024-00046-1
https://opg.optica.org/optica/fulltext.cfm?uri=optica-11-12-1700&id=565936
https://www.sandboxaq.com/post/sandboxaq-partners-with-carahsoft-to-expand-distribution-of-its-cybersecurity-and-ai-enabled-quantum-solutions-in-the-public-sector
https://www.quantum-dice.com/quantum-dice-and-bt-group-explore-the-use-of-qrngs-for-cryptographic-applications-in-telecommunications/
https://arqit.uk/press-releases/arqit-and-mastercard-enhance-digital-asset-security-and-compliance-for-financial-institutions
https://arqit.uk/press-releases/ampliphae-hpe-athonet-and-arqit-deliver-quantum-safe-private-5g-using-symmetric-key-agreement
https://quantum-emotion-website.webflow.io/press-release/quantum-emotion-announces-the-creation-of-quantum-ehealth-a-new-subsidiary-focused-on-healthcare-cybersecurity-applications
https://epb.com/newsroom/press-releases/epb-and-ornl-announce-plans-for-energy-resilience-and-quantum-tech-research-collaborative/
https://www.idquantique.com/id-quantique-joins-a-quantum-safe-satellite-data-link-project/
https://arqit.uk/press-releases/arqit-and-carahsoft-partner-to-bring-symmetric-key-agreement-cybersecurity-product-to-the-us-public-sector
https://www.defense.gov/News/Contracts/Contract/Article/3701831/

https://optech.org/en/projet/support-for-technology-integration-on-the-kirq-test-platform/
https://www.quantumemotion.com/press-release/quantum-emotion-deploys-its-quantum-safe-security-platform-for-digital-therapeutics-in-landmark-commercial-alliance-greybox-solutions-partners-with-becton-dickinson-canada
https://www.hw.ac.uk/news/articles/2024/state-of-the-art-telescope-paves-way-for.htm
https://www.ornl.gov/news/epb-ornl-announce-plans-research-collaborative-focused-energy-resilience-quantum-technology
https://www.zawya.com/en/press-release/companies-news/technology-innovation-institute-unveils-abu-dhabi-quantum-optical-ground-station-for-ultra-secure-global-communications-e88f5vh1
https://www.nature.com/articles/s41534-024-00873-2
https://www.tii.ae/news/tii-and-uae-space-agency-unveil-pioneering-unhackable-quantum-tech-gitex-2024
https://www.arianespace.com/press-release/arianespace-wins-new-contract-to-launch-sentinel-1c-observation-satellite-on-board-vega-c/
https://www.antaris.space/news/vamkadih9in1ewlbo43mcc71ozdi0z
https://spacenews.com/german-cubesat-to-test-quantum-key-distribution/
https://investors.boeing.com/investors/news/press-release-details/2024/Boeing-Pioneering-Quantum-Communications-Technology-with-In-Space-Test-Satellite/default.aspx
https://www.group.sener/en/noticias/sener-seleccionada-para-el-desarrollo-del-primer-demostrador-de-un-sistema-de-distribucion-cuantica-de-claves-desde-orbita-leo/
https://science.nasa.gov/science-research/biological-physical-sciences/nasa-science-on-health-safety-to-launch-on-31st-spacex-resupply-mission/
https://www.nature.com/articles/s41467-023-44281-0
https://onlinelibrary.wiley.com/doi/abs/10.1002/qute.202300343
https://www.nature.com/articles/s41467-023-44220-z
https://doi.org/10.1103/PhysRevApplied.21.014048
http://www.cas.ac.cn/cm/202405/t20240517_5014978.shtml
https://www.nature.com/articles/s41586-024-07252-z
https://uwaterloo.ca/institute-for-quantum-computing/news/quantum-sources-satellite-missions
"https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.133.020801
https://pme.uchicago.edu/news/new-method-could-yield-fast-cross-country-quantum-network
https://umass-qnet.nonlocally.org/event/2024-04-25%2013:00:00/0"
https://www.nasa.gov/general/nasas-first-ever-quantum-memory-made-at-glenn-research-center/
https://journals.aps.org/prxquantum/pdf/10.1103/PRXQuantum.5.030330
https://www.tno.nl/en/newsroom/2024/09/tno-launches-qu-star-pioneer-quantum
https://www.nature.com/articles/s42005-024-01796-2
https://www.nature.com/articles/s41534-024-00886-x
https://newsroom.bt.com/access-to-quantum-secure-communications-made-easier-for-businesses-in-uk-first-data-centre-to-data-centre-connection/
https://doi.org/10.1364/OPTICA.530224
https://ionq.com/news/ionq-announces-largest-2024-u-s-quantum-contract-award-of-usd54-5m-with
https://www.rit.edu/news/rit-receives-96-million-award-improve-quantum-system-networking-initiatives
http://sh.people.com.cn/n2/2024/0925/c134768-40989013.html
https://mp.weixin.qq.com/s/aFUC6pGbVgIK9NYoVSK2JQ
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/CEF-DIG-2024-EUROQCI-WORK
https://www.telus.com/en/about/news-and-events/media-releases/telus-and-photonic-join-forces-to-build-canadas-quantum-future
https://www.nature.com/articles/s42005-024-01844-x
https://www.science.org/doi/10.1126/sciadv.adp6442
https://www.aliroquantum.com/products/alironetquickstart

https://www.nyu.edu/about/news-publications/news/2023/september/nyu-takes-quantum-step-in-establishing-cutting-edge-tech-hub-in-.html
http://www.ahnews.com.cn/yaowen1/pc/con/2023-06/07/496_860981.html
https://labsoflatvia.com/en/news/formation-of-a-national-quantum-communications-infrastructure-begins
https://marketing.idquantique.com/acton/attachment/11868/f-0cca1474-5f49-4e62-9372-2135c42395d3/1/-/-/-/-/Press%20release%3A%20Numana%20Oct%2023%202023.pdf
https://newsroom.orange.com/frances-industry-quantum-startups-academic-and-institutional-players-join-forces-to-build-the-future-of-the-french-quantum-internet-communication-system/
https://qci.dk/
https://irelandqci.ie/2023/04/24/quantum-technology-experts-gather-in-waterford-for-irelandqci-opening-meeting/
https://beqci.eu/project/
https://euroqci-spain.eu/
https://euroqci.bg/2023/02/10/bulgarian-national-plan-kick-off-meeting-in-sofia/
https://prism-euroqci.eu/one-of-the-worlds-most-ambitious-quantum-networks-to-be-built-in-malta/
https://www.qusecure.com/qusecure-uses-starlink-for-post-quantum-cryptography-in-satellite-to-earth-communications/
https://www.qusecure.com/qusecure-accenture-team-up-on-satcom-security-test-using-pqc/
https://www.einpresswire.com/article/621893832/sky-and-space-sas-to-embed-world-s-first-quantum-resistant-encryption-solution-for-its-satellites-and-ground-terminals
https://spacenews.com/china-is-developing-a-quantum-communications-satellite-network/
https://speqtral.space/speqtral-announces-kongsberg-nano-avionics-and-mbryonics-as-key-partners-for-speqtral-1-mission/
https://uwaterloo.ca/news/science/connecting-canada-and-europe-through-quantum-satellite?utm_source=miragenews&utm_medium=miragenews&utm_campaign=news
https://www.vodafone.com/news/technology/vodafone-tests-quantum-safe-business-network-upgraded-smartphones
http://www.chinatelecom.com.cn/news/02/202309/t20230915_76791.html
https://www.kedglobal.com/tech,-media-telecom/newsView/ked202309060009
https://www.kedglobal.com/tech,-media-telecom/newsView/ked202309060009
https://www.ltimindtree.com/news-event/ltimindtree-with-quantum-xchange-fortinet/
https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms
https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38b-preliminary-draft.pdf
https://www.nccoe.nist.gov/sites/default/files/2023-12/pqc-migration-nist-sp-1800-38c-preliminary-draft.pdf
https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy
https://www.datanet.co.kr/news/articleView.html?idxno=185202
https://www.whitehouse.gov/briefing-room/presidential-actions/2023/08/09/executive-order-on-addressing-united-states-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern/
https://home.treasury.gov/news/press-releases/jy1686
https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4735
https://m-en.yna.co.kr/view/AEN20231213000500315
https://www.quantum-dice.com/quantum-dice-launches-the-new-generation-of-apex-the-worlds-fastest-quantum-random-number-generator-enabling-trusted-cybersecurity-for-enterprise-applications/
https://www.ses.com/press-release/ses-led-eagle-1-onboards-tno-and-airbus-deliver-ground-station-quantum-key
https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci
https://petrus-euroqci.eu/industrial-qkd-projects/

https://www.dmu.gov.hu/documents/prod/Nemzeti-Strategiai-Utemterv_Digitalis-Evtized-Szakpolitikai-Program-2030_Tervezet.pdf
https://qcihungary.hu/en/home/
https://quantumdelta.nl/qcined
https://www.inrim.it/sites/default/files/2023-06/Press%20Release%20QUID_DEF_ENG_20230606_2.pdf
https://www.ronaqci.upb.ro/media/
https://siquid.fmf.uni-lj.si/
https://skqci.qute.sk/news/
https://www.nature.com/articles/s41467-023-36573-2
https://www.rri.res.in/news/quic-lab-achieves-next-step-towards-realising-secure-satellite-based-quantum-communication
https://std.samr.gov.cn/gb/search/gbDetailed?id=F77AFB62AF85406CE05397BE0A0A57C1
https://www.cpnn.com.cn/qiye/dianwangPD2023/202312/t20231222_1663087.html
http://www.jinhua.gov.cn/art/2023/11/27/art_1229159979_60256434.html
https://www.shanghai.gov.cn/nw4411/20231109/6fa353cb87f8423fa4a2a7a3cfa3f260.html
https://www.hsbc.com/news-and-views/news/media-releases/2023/hsbc-pioneers-quantum-protection-for-ai-powered-fx-trading.
https://www.quantumcomputinginc.com/press-releases/quantum-computing-inc-to-launch-reprogrammable-and-non-repeatable-quantum-random-number-generator/
https://doi.org/10.1103/PhysRevLett.131.100802
https://www.nature.com/articles/s41467-023-37518-5
https://doi.org/10.1103/physrevapplied.20.024051
https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/12/fact-sheet-upgrading-the-u-s-singapore-strategic-technology-partnership/
https://ufm.dk/publikationer/2023/strategi-for-kvanteteknologi-del-1-forskning-og-innovation-i-verdensklasse
https://science.des.qld.gov.au/research/key-areas/quantum
https://www.msit.go.kr/bbs/view.do?sCode=user&mId=113&mPid=238&pageIndex=7&bbsSeqNo=94&nttSeqNo=3183541
https://www.hfss.gov.cn/zqdh/zfjg/tzcjj/gzdt/11272251.html
https://www.sc.gov.cn/10462/c105962/2023/1/20/00ade04b7fa54c5f81e1e9b895eb7f3e.shtml
http://quantumcas.ac.cn/2023/0202/c24874a590992/page.htm
http://www.jiangsu.gov.cn/col/col88024/index.html
http://www.shanxi.gov.cn/ztjj/2023sxlh/2023sxlhbg/202301/t20230119_7823686.shtml
https://www.beijing.gov.cn/zhengce/gfxwj/202301/t20230131_2909785.html
https://www.henan.gov.cn/2023/01-14/2673451.html
http://www.whwx.gov.cn/szyw/202302/t20230201_2142904.shtml
https://www.hefei.gov.cn/public/1741/108461202.html
https://www.beijing.gov.cn/zhengce/gfxwj/sj/202302/t20230203_2911253.html
http://www.jiangxi.gov.cn/art/2023/1/30/art_4968_4342426.html
http://www.gov.cn/zhengce/2023-02/06/content_5740407.htm
http://jr.sz.gov.cn/gkmlpt/content/10/10409/post_10409782.html#2814
http://www.gd.gov.cn/zwgk/zcjd/mtjd/content/post_4092646.html
http://district.ce.cn/newarea/roll/202304/06/t20230406_38483816.shtml
http://www.gov.cn/guowuyuan/zfgzbg.htm?ivk_sa=1025845k
https://www.cq.gov.cn/zwgk/zfxxgkml/szfwj/qtgw/202303/t20230323_11803613.html?eqid=ebdfcd5f000dba1a00000003642e2686
https://www.yn.gov.cn/zwgk/zfxxgkpt/fdzdgknr/zcwj/zfxxgkptyzbf/202303/t20230307_255865.html
https://www.ndrc.gov.cn/xxgk/zcfb/tz/202304/t20230403_1353195.html
http://www.moe.gov.cn/srcsite/A08/moe_1034/s4930/202304/t20230419_1056224.html
https://epaper.scdaily.cn/shtml/scrb/20230417/292841.shtml
http://kjj.wuhan.gov.cn/zwgk_8/fdzdnrgk/sjczzxzj/sbtzsbzn/202304/t20230407_2182908.shtml
http://zwgk.changchun.gov.cn/szf_3410/bgtxxgkml/202304/t20230418_3130749.html
https://www.nsfc.gov.cn/publish/portal0/tab442/info89245.htm
https://www.henan.gov.cn/2023/05-09/2739949.html

https://www.js.gov.cn/art/2023/9/3/art_37384_11002980.html
http://fgw.gz.gov.cn/gkmlpt/content/9/9217/post_9217431.html#480
https://www.beijing.gov.cn/zhengce/zhengcefagui/202309/t20230908_3255227.html
https://jxt.sc.gov.cn//scjxt/jxtzcwj/2023/9/15/1119dc76f8c948ba93c416d6e3a8607b.shtml
https://www.miit.gov.cn/zwgk/zcwj/wjfb/tz/art/2023/art_e715a9d4611742d5a5f7a4f36ea74974.html
http://www.hubei.gov.cn/zfwj/ezf/202309/t20230925_4867070.shtml
https://www.shanghai.gov.cn/jcsfbsbtz/20230927/1442c4a927024e7eaaf1a1afa3c18dd9.html
https://www.cnipa.gov.cn/art/2023/9/25/art_75_187769.html
http://jxt.hubei.gov.cn/fbjd/zc/qtzdgkwj/gwfb/202310/t20231027_4917118.shtml
http://www.shandong.gov.cn/art/2023/10/13/art_267492_59942.html
https://kjt.hunan.gov.cn/kjt/xmxx/xmsb/202310/t20231008_31620081.html
http://www.gl.gov.cn/xjwz/zfxxgk/qzbmptlj/qrmzfjzfgzbm/glqzfb/fdzdgknr/yfxz/202310/t20231009_4694111.htm
https://www.hys.gov.cn/hysrmzfw/c116484/2023-10/30/content_240dbb24c6984d328c71f404ed8ce5da.shtml
https://www.zmdkfq.gov.cn/newsdetail/54/6022.html
https://www.gd.gov.cn/zwgk/wjk/qbwj/ybh/content/post_4287596.html
http://bdb.shandong.gov.cn/art/2023/11/14/art_76147_10321709.html
http://amr.shandong.gov.cn/art/2023/11/24/art_92482_10305045.html
http://www.hubei.gov.cn/zwgk/hbyw/hbywqb/202311/t20231116_4947889.shtml
http://gdyjzx.gd.gov.cn/gkmlpt/content/4/4287/post_4287849.html#542
https://public.zhengzhou.gov.cn/D0104X/8049895.jhtml
https://www.jiangsu.gov.cn/art/2023/11/9/art_46143_11066954.html
https://www.sc.gov.cn/10462/zfwjts/2023/11/25/5c7b0dec3e864647aa0f50739afa4f63.shtml
https://www.wuhan.gov.cn/zwgk/xxgk/zfwj/bgtwj/202311/t20231108_2297022.shtml
https://www.nsfc.gov.cn/publish/portal0/tab1392/
https://sjzyj.ah.gov.cn/public/7061/40684913.html
https://gdca.miit.gov.cn/zwgk/zcwj/wjfb/art/2023/art_e86eab3c8daf4d87aabdceac26e6791b.html
https://sjzyj.ah.gov.cn/public/7061/40684913.html
https://jxj.beijing.gov.cn/zwgk/zcwj/bjszc/202312/t20231221_3507294.html
http://www.shandong.gov.cn/art/2023/12/29/art_267492_62983.html
https://gxt.hunan.gov.cn/gxt/xxgk_71033/tzgg/202312/t20231230_32615653.html
https://sti.xm.gov.cn/xxgk/tzgg/202312/t20231205_2801944.htm
http://kjj.nantong.gov.cn/ntskjj/gggs/content/5c01e3fe-b0f3-4d2a-a158-43305faf1267.htm
https://www.ndrc.gov.cn/xxgk/zcfb/ghwb/202312/t20231221_1362836.html
https://www.gd.gov.cn/attachment/0/538/538477/4303566.pdf
https://www.gd.gov.cn/attachment/0/538/538481/4303566.pdf
https://www.canada.ca/en/innovation-science-economic-development/news/2023/01/government-of-canada-launches-national-quantum-strategy-to-create-jobs-and-advance-quantum-technologies.html
https://www.gov.uk/government/publications/national-quantum-strategy/national-quantum-strategy-accessible-webpage
https://www.canada.ca/en/department-national-defence/corporate/reports-publications/overview-quantum-2030.html
https://www8.cao.go.jp/cstp/ryoshigijutsu/230414_mirai.pdf
https://www.pmindia.gov.in/en/news_updates/cabinet-approves-national-quantum-mission-to-scale-up-scientific-industrial-rd-for-quantum-technologies/
https://www.bmbf.de/bmbf/shareddocs/kurzmeldungen/de/2023/04/230425-handlungskonzept-quantentechnologien.html#searchFacets
https://www.industry.gov.au/publications/national-quantum-strategy?
https://ufm.dk/publikationer/2023/strategi-for-kvanteteknologi-del-1-forskning-og-innovation-i-verdensklasse
https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mPid=2&mId=4&bbsSeqNo=42&nttSeqNo=828

https://www.nature.com/articles/s42005-024-01894-1
https://www.keysight.com/us/en/about/newsroom/news-releases/2024/3004-PR24-062-Keysight-Introduces-New-Testing-Capabilities-to-Strengthen-Post-Quantum-Cryptography.html
https://terraquantum.swiss/news/terra-quantum-launches-tq42-cryptography-library-for-secure-data-transmission-storage-and-authentication
https://www.qusecure.com/qusecure-achieves-soc-1-and-soc-2-type-2-compliance-validating-security-controls-and-practices-of-its-leading-post-quantum-cryptography-solution/
https://www.csoonline.com/article/2119505/us-government-could-mandate-quantum-resistant-encryption-from-july.html
https://news.sktelecom.com/204858
https://www.qusecure.com/qusecure-collaborates-with-nvidias-revolutionary-cupqc-initiative-to-advance-post-quantum-cryptography/
https://www.ntu.edu.sg/news/detail/new-research-programme-to-strengthen-cybersecurity-in-a-post-quantum-world
https://www.prnewswire.com/news-releases/btq-and-id-quantique-sign-mou-collaboration-for-developing-next-generation-authentication-systems-302210846.html
https://www.yna.co.kr/view/AKR20240624026600017?input=1195m
https://mp.weixin.qq.com/s/IwA3AyeDl36dW-df5SWuMw
https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
https://www.secure-ic.com/news-and-events/news/secure-ic-signs-international-collaboration-with-taiwan-quantum-safe-association-and-pqc-cia/
https://www.taiwannews.com.tw/zh/news/5917969
https://www.wisekey.com/press/wisekey-partners-with-venafi-on-post-quantum-encryption-services/
https://pqshield.com/press-release-pqshield-and-si-five-collaborate-to-advance-post-quantum-cryptography-in-risc-v/
https://crypto4a.com/news/crypto4a-certified-to-nists-algorithm-standards/
https://pqshield.com/pqshield-builds-nist-ready-pqc-in-silicon/
https://dallasinnovates.com/dallas-hest-investments-invests-1m-in-quantum-computing-security-startup/#:~:text=Dallas%E2%80%99%20HEST%20Investments%20Invests%20%241M%20in%20Quantum%20Computing,computing%20era%2C%22%20the%20Dallas-based%20private%20equity%20firm%20said
https://www.newswire.ca/news-releases/btq-technologies-completes-acquisition-of-radical-semiconductor-s-processing-in-memory-technology-portfolio-advancing-post-quantum-cryptography-capabilities-824300756.html
https://www.tisparkle.com/media/press-release/sparkle-launches-its-network-service-naas-product-suite-quantum-safe-over
https://eviden.com/insights/press-releases/eviden-launches-pqc-hsmaas-a-eu-sovereign-post-quantum-cryptography-hardware-security-module-as-a-service/
https://softiron.com/resources/softiron-launches-worlds-first-post-quantum-safe-virtualization-and-private-cloud-solutions-with-q4-2024-updates/
https://www.telefonica.com/es/sala-comunicacion/prensa/telefonica-halotech-integran-cifrado-postcuantico-entornos-criticos/
https://www.fsisac.com/newsroom/fsisac-guidance-urges-financial-firms-to-implement-crypto-agility-as-a-key-defense-against-quantum-computing-threats
https://trustcloud.tech/trustcloud-platform/quantum-vault/
https://www.entrust.com/cybersecurity-institute/reports/2024-pki-and-post-quantum-trends-study
-and-Advanced-TIoT-Solu.html
https://www.businesskorea.co.kr/news/articleView.html?idxno=229726
https://www.wisekey.com/press/wisekey-announces-wisesat-satellite-launch-with-spacex-on-january-14-2025/
https://www.lexology.com/library/detail.aspx?g=17e52178-27a3-4850-bfca-a415bb86403e
https://newsroom.accenture.com/news/2024/banco-sabadell-collaborates-with-accenture-and-qusecure-to-advance-quantum-safe-infrastructure

https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17863
https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17873
https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17875
https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17874
https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=17876
https://www.itu.int/en/ITU-T/about/groups/2022-2024/Pages/sg13.aspx
https://www.ccsa.org.cn/standardDetail/?standardNum=GB%2FT%2042829-2023
https://www.iso.org/standard/77097.html
https://www.iso.org/standard/77309.html
https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf
https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19143
https://www.ietf.org/blog/pquip/
https://post-quantum.com/index.html https://www.mitre.org/news-insights/news-release/post-quantum-cryptography-coalition-launches
https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18760
https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18902
https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18903
https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19049
https://www.luxquanta.com/luxquanta-nova-lq-to-be-announced-at-the-mobile-world-congress-2023-n-26-en
https://qtict.com/frontier/detail?id=86
https://arqit.uk/press-releases/new-product-launch-and-business-update https://arqit.uk/press-releases/arqit-launches-the-worlds-first-integrated-solution-for-quantum-safe-vpn-connectivity-using-symmetric-key-agreement
https://arqit.uk/press-releases/aiee-sign-licence-contract-for-arqit-quantumcloud
https://arqit.uk/press-releases/arqit-bt-and-fortinet-launch-quantum-safe-vpn-to-protect-against-evolving-cyberthreats
https://arqit.uk/press-releases/babcock-develops-cutting-edge-communications-and-control-technology-in-partnership-with-arqit
https://arqit.uk/press-releases/consortium-wins-uk-government-funding-to-further-development-carrier-grade-testing-and-standards-in-open-ran-rics
https://arqit.uk/press-releases/arqit-and-exclusive-networks-announce-us-distribution-partnership
https://arqit.uk/press-releases/arqit-and-securecloud-partner-to-deliver-cyber-resilience-using-symmetric-key-agreement
https://arqit.uk/press-releases/arqit-and-snc-ms-uk-announce-strategic-teaming-agreement
https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19146
https://www.global.toshiba/jp/technology/corporate/rdc/rd/topics/24/2409-02.html
https://www.gruppotim.it/en/press-archive/sparkle/2024/PR-QKD-PoC-Greece.html
https://www.nature.com/articles/s41534-024-00879-w
https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2060379
https://aerospace.honeywell.com/us/en/about-us/press-release/2024/10/honeywell-partners-with-european-space-agency-to-protect-sensitive-information-transmitted-by-satellite
https://www.gov.uk/government/publications/regulating-quantum-technology-applications-government-response-to-recommendations-made-by-the-regulatory-horizons-council/regulating-quantum-technology-applications-government-response-to-the-rhc
https://phluxtechnology.com/latest/uk-collaborative-project-to-facilitate-secure-quantum-key-distribution-with-high-performance-oem-receiver-modules
https://ieeexplore.ieee.org/document/10707130
https://www.luxquanta.com/luxquanta-collaborates-in-pioneer-test-of-low-latency-fibre-in-data-center-networks-led-by-lyntia-n-71-en
https://arxiv.org/html/2310.20107v2
https://www.prnewswire.com/in/news-releases/stl-advances-multicore-fibre-portfolio---a-make-in-india-enabler-for-quantum-communications-and-silicon-photonics-302277816.html
https://www.chinanews.com.cn/cj/2024/10-25/10307804.shtm
https://www.nature.com/articles/s41377-024-01633-9

iCV TA&K
Technology Advisory
& Knowledgebase

在ICV，我们对新技术充满好奇，我们努力提供最强大的市场数据和洞察力，以帮助我们的客户做出正确的战略决策。

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

QUANTUMCHINA

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】

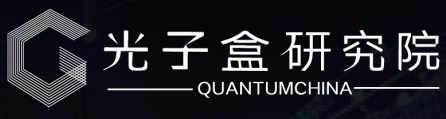
研究院构建了独特的"产学研政资"协同创新网络，为政府部门提供科技创新政策制定咨询，协助构建量子科技产业园区规划；为科研机构搭建技术转化评估模型，推动实验室成果与产业需求对接；为企业客户定制技术路线选择、市场竞争策略及专利布局方案；为投资机构建立科技项目价值评估体系，甄别具有突破潜力的早期技术项目。目前已形成季度产业研究报告、年度技术趋势预测、专项政策建议书等系列知识产品。

【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。

2025全球量子安全产业发展展望
量子科技年度系列报告



北京市海淀区上地三街中黎科技园1号楼618室

扫码关注光子盒

扫码与研究员交流