国投证券 SDIC SECURITIES

2024 年 07 月 15 日
计算机

行业深度分析

证券研究报告

量子科技：见微知著、革故鼎新

投资评级 领先大市-A
维持评级

首选股票	目标价（元）	评级

量子科技：未来科技的颠覆式创新，新质生产力的重要方向

两次量子革命带来颠覆式的科技创新。第一次量子革命发明与发展了原子能、激光、超导、晶体管、核磁共振成像等基于量子力学效应的信息技术，第二次量子革命基于操控微观粒子的叠加、纠缠等行为，进行信息获取、处理和传输，产生颠覆性的科技创新。当前量子科技产业主要包括量子计算、量子通信、量子测量、抗量子密码四大研究领域。

量子科技成为新质生产力重要方向，有望迎来政策支持。2024 年两会政府工作报告在“加快发展新质生产力”中，提出“制定未来产业发展计划，开辟量子技术、生命科学等新赛道，创建一批未来产业先导区”。3 月 29 日，国务院国资委遴选确定首批新质生产力的启航企业名单，重点布局了人工智能、量子信息和生物医药领域。5 月 10 日，李强总理来到中科院量子信息与科技创新研究院，再次体现政府的重视，量子科技产业有望成为新质生产力重要方向。

积极布局量子计算、量子通信、抗量子密码三条投资主线

量子计算：算力产业的颠覆式创新，未来科技的锋利之矛。量子计算机的量子比特利用量子叠加态原理实现处理信息量的指数级增长，以 Shor 算法为例，可以在 20 万个错误率在 0.1%的量子物理比特上在 8 个小时内破解 2048 位的 RSA 密码，而用经典计算机则需要几百年的时间进行破解。**从产业链来看**，量子计算芯片、稀释制冷机和室温测控系统成为量子计算机主要组成部分。根据 ICV 的报告，2023 年全球量子计算产业规模达到 47 亿美元，2023 至 2028 年的年平均增长率（CAGR）达到 44.8%，有望实现高速增长。**建议关注：**量子计算整体解决方案提供商【国盾量子】、量子测控系统提供商【普源精电】等。

量子通信：量子技术实现密钥分发，信息安全的坚固之盾。基于传统 RSA 算法的密钥分发和数字签名技术，在量子计算时代存在较大的安全风险。量子保密通信将经典密钥转换成量子形态的密钥，利用量子不可复制、纠缠等物理特性，实现密钥分发过程的绝对安全。**从产业链来看**，量子密钥分发设备（QKD）成为行业的核心设备，上游包括芯片+光源+单光子探测器+量子随机数发生器，下游主要在政府、金融、电力等关基行业率先落地。**从建设进度来看**，中国已经形成骨干网-城域网-空天一体的三步走发展战略，当前已经建成长度超过 1 万公里的广域量子保密通信一期骨干网，未来城域网和空天一体网络建设有望加速。**建议关注：**QKD 设备商【国盾量子】、系统集成商【神州信息】等。

抗量子密码：密码原理的底层创新，应对量子攻击的新型方案。抗量子密码（PQC）是能够抵抗量子计算对现有密码算法攻击的新一代密码算法。从产业进展来看，美国 NIST 将于今年夏季发布第一版的抗量子密码算法标准，从而开启美国抗量子密码迁移的路线图，预计美国对于软件/固件签名和传统网络设备的迁移将在 2030 年前完成。**建议关注：**密码厂商【吉大正元、信安世纪、格尔软件、三未信安】等。

风险提示：政策推进不及预期；技术突破不及预期；商业化落地不及预期。

行业表现

资料来源：Wind 资讯

升幅%	1M	3M	12M
相对收益	-2.7	-11.7	-26.5
绝对收益	-7.4	-15.1	-38.1

赵阳 分析师
SAC 执业证书编号：S1450522040001
zhaoyang1@essence.com.cn

夏瀛韬 分析师
SAC 执业证书编号：S1450521120006
xiayt@essence.com.cn

袁子翔 分析师
SAC 执业证书编号：S1450523050001
yuanzx@essence.com.cn

相关报告

科技自立自强，聚焦泛信创攻关和前沿领域探索	2024-07-01
华为 HDC 2024 开幕，纯血鸿蒙+盘古大模型联袂亮相	2024-06-23
Copilot PC 和 AI phone 双剑齐发，端侧 AI 渗透率拐点将至	2024-06-17
车路协同迎来密集催化，关注路侧、商用车、自动驾驶三条主线	2024-06-10
AIPC 进展加速，WoA 未来可期	2024-06-03

内容目录

图表目录

1. 两次量子革命引领技术发展，新质生产力带来政策催化

1.1. 技术：两次量子革命带来颠覆式技术创新

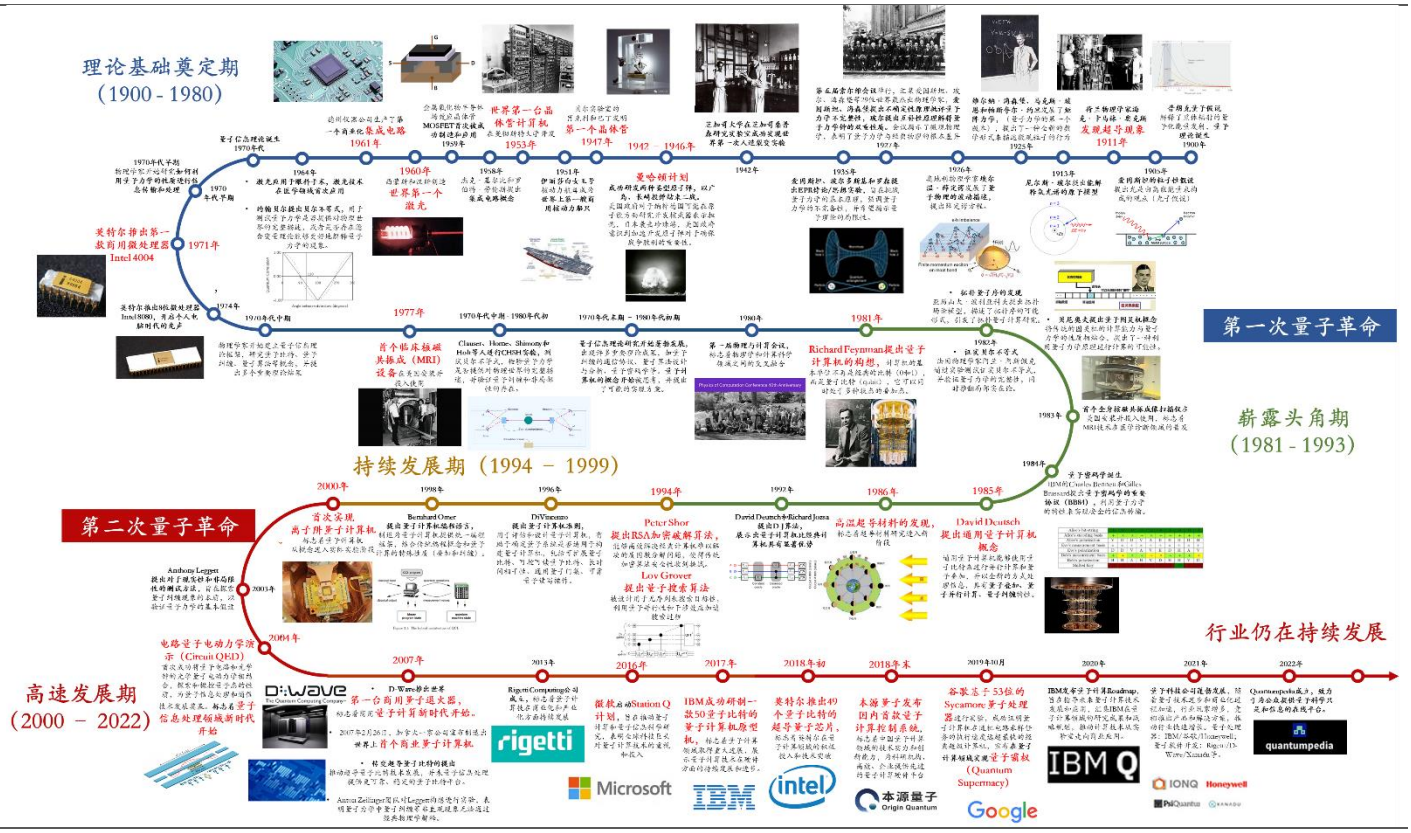
第一次量子革命（20 世纪 80 年代至 90 年代末期）：量子力学推动推动超导、晶体管、激光、核磁共振等技术诞生。上世纪 80 年来以来，物理学理论探索从经典物理学的连续性观念转向量子力学的离散型观念，普朗克的量子假说、爱因斯坦的光量子理论和玻尔的量子轨道等量子理论诞生并得到应用，推动超导、晶体管、激光、核磁共振等技术的诞生与应用，标志着量子理论的正确性得到验证，量子技术在信息科学实际应用中的巨大潜力逐渐显现，利用量子力学原理进行信息处理的可能性得到探索，为第二次量子革命奠定坚实理论与实验基础。具体而言，第一次量子革命可分为三个阶段。

1）理论基础奠定期（1900-1980）：物理学家开始探索微观物理学现象。1900 年，普朗克提出量子假说，标志着量子理论的诞生。随后，爱因斯坦的光量子理论和玻尔的原子模型进一步巩固了量子理论。1926 年，薛定谔和海森堡分别提出波动力学和矩阵力学，为量子力学奠定坚实基础。在此时期，量子理论成功解释了诸多实验现象，并在固体物理学、原子物理学和分子物理学等领域取得重大进展。在应用方面，超导、晶体管、激光、核磁共振等技术不断诞生并得到应用。1911 年，荷兰物理学家海克·卡马林·奥克斯发现超导现象；1947 年，贝尔实验室的肖克利和巴丁发明第一个晶体管；1953 年，曼彻斯特大学开发世界第一台晶体管计算机；1960 年，西蒙斯和汉斯创造世界第一个激光；1961 年，德州仪器公司生产了第一个商业化集成电路。

2）崭露头角期（1981-1993）：在量子理论的指导下，量子科技开始在世纪应用中崭露头角。1981 年，费曼提出量子计算的概念，并探讨了量子计算机的潜力；1982 年，量子纠缠的实验验证成功，为量子信息科学的发展奠定基础；1991 年，量子密钥分发概念被提出，为量子通信的安全传输提供理论基础。这一时期，量子科技的理论研究和实验验证为后续的技术发展和应用奠定基础。

3）持续发展期（1994-1999）：量子科技产业持续发展。1994 年，Peter Shor 提出 Shor 算法，展示了量子计算机在破解加密方面的巨大潜力；同年，Lov Grover 提出量子搜索算法，设计用于无序列表搜索目标性，利用量子并行性和干涉效应加速搜索过程。1996 年，DiVincenzo 提出量子计算机准则，用于评估和设计量子计算机，有助于确定量子系统是否适用于构建量子计算机，包括可扩展量子比特、可控可读量子比特、长时间相干性、通用量子门集、可靠量子读写操作。1998 年，Bernhard Omer 提出量子计算机编程语言，制造为量子计算机提供统一编程框架，结合传统编程概念和量子计算的叠加和纠缠特性。

图1. 量子科技产业整体发展历程梳理



资料来源：《物理学报》，New Scientist，Quantumpedia，国投证券研究中心

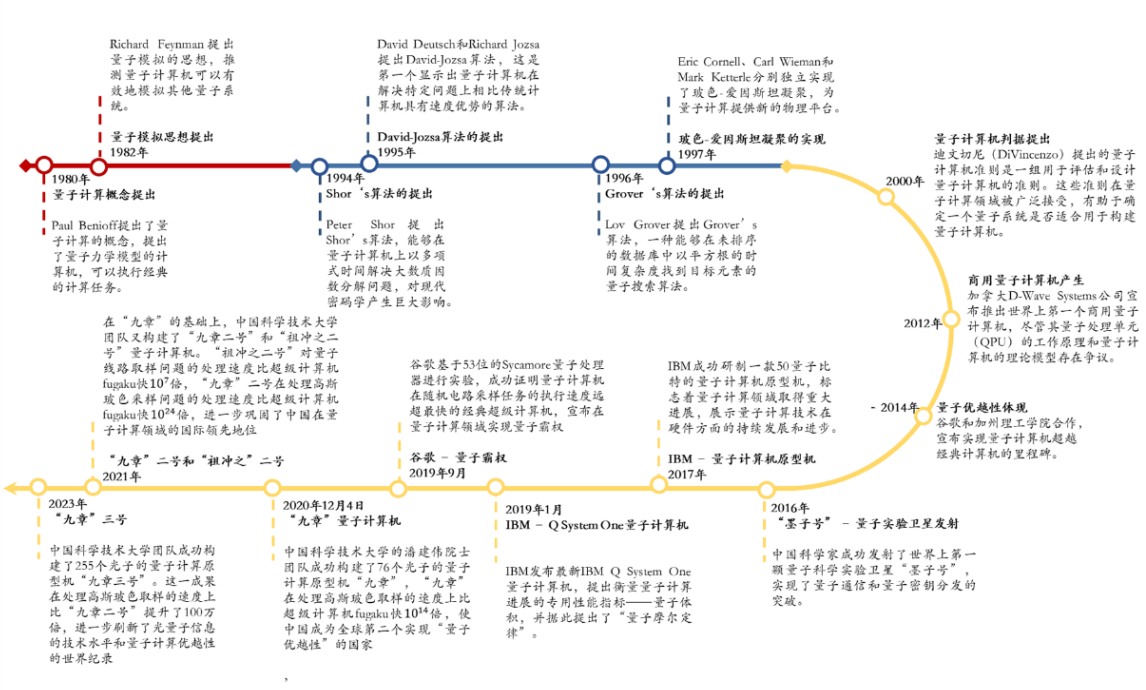
第二次量子革命（21 世纪初至今）：实现单个微观粒子操控，量子信息技术产业持续演进。第一次和第二次量子革命的核心区别在于第一次量子革命主要发明与发展原子能、激光、超导、晶体管和半导体器件、集成电路器件、微处理器、核磁共振成像等基于量子力学效应的信息技术，而第二次量子革命基于操控电子、光子等离子体系的微观量子行为发展量子信息技术，利用量子体系的叠加、纠缠等量子力学行为，进行信息获取、处理和传输，对多个领域产生基础共性与颠覆性的重大影响。**在这一时期，量子比特概念的提出，量子纠缠的实验验证、量子计算的原理性验证等，意味着量子层面上操控和利用量子现象成为可能**，为解决经典计算难以处理的问题、实现信息安全传输、探索量子模拟等提供全新途径，**标志着量子技术开始从理论探索转向实际应用，一系列突破性技术和商业化产品逐渐涌现。**

21 世纪以来，随着科技企业积极布局，量子计算进入了技术验证和原理样机研制的阶段。2000 年，DiVincenzo 提出建造量子计算机的判据。此后，加拿大 D-Wave 公司率先推动量子计算机商业化，IBM、谷歌、微软等科技巨头也陆续开始布局量子计算。2018 年，谷歌发布了 72 量子位超导量子计算处理器芯片。2019 年，IBM 发布最新 IBM Q System One 量子计算机，提出衡量量子计算进展的专用性能指标——量子体积，并据此提出了“量子摩尔定律”，即量子计算机的量子体积每年增加一倍。**在量子优越性方面，**2019 年 10 月，谷歌基于 53 位的 Sycamore 量子处理器进行实验，成功证明量子计算机在随机电路采样任务的执行速度远超最快的经典超级计算机，宣布在量子计算领域实现“量子霸权”。

“量子霸权”是重要的里程碑，标志着量子计算领域的一个重大转折点，即量子计算机首次在特定任务上展现出超越传统超级计算机的能力，证明了量子计算机从原理走向应用的可行性与在并行计算方面的优越性。尽管目前量子计算机的应用还非常有限，但这一突破展示了量子计算技术的巨大潜力，并为未来的发展奠定了基础。

量子计算机的进一步发展可能会在材料科学、药物发现、优化问题等领域带来革命性的变化。2020 年 12 月 4 日，中国科学技术大学的潘建伟院士团队成功构建了 76 个光子的量子计算原型机“九章”。根据中科大钟瀚森、潘建伟等人发表的在 Science 期刊发表的《Quantum computational advantage using photons》论文，“九章”在处理高斯玻色取样的速度上比当时的超级计算机“富岳”快 100 万亿倍，使中国成为全球第二个实现“量子优越性”的国家。2021 年，在“九章”的基础上，中国科学技术大学团队又构建了“九章二号”和“祖冲之二号”量子计算机。这些机器在处理特定问题上的速度比当时的顶级超级计算机快得多，进一步巩固了中国在量子计算领域的国际领先地位。2023 年，中国科学技术大学团队成功构建了 255 个光子的量子计算原型机“九章三号”。根据邓宇皓、潘建伟等人发表的《Gaussian Boson Sampling with Pseudo-Photon-Number Resolving Detectors and Quantum Computational Advantage》论文，“九章三号”在处理高斯玻色取样的速度上比“九章二号”提升了 100 万倍，进一步刷新了光量子信息的技术水平和量子计算优越性的世界纪录。

图2. 量子计算机逐渐从理论走向实现



资料来源：信通院，赛迪智库，Science Physical Review Journals，量子物理与量子信息研究部，国投证券研究中心

1.2. 政策：全球积极布局，国内外政策齐发力

量子科技的战略重要性日趋显现，多国持续加大量子研发投入。鉴于量子信息科技重要的科学意义和巨大的应用价值，欧美发达国家的政府、科研机构和产业资本正在不断完善战略部署，稳步增加研发投入。全球主要国家在量子信息领域的战略规划和投资概况来看，**以 2018 年欧盟“量子旗舰计划”和美国《国家量子倡议（NQI）》法案为重要标志**，近五年来各国在量子信息领域的规划布局持续加速。根据信通院的统计报告，2023 年 6 个国家相继发布量子信息相关国家战略和投资规划，计划投资总规模达到 67 亿美元。**美国方面，**2018 年 12 月，美国启动了为期 10 年的“国家量子倡议法案（NQI）”，2019-2022 年间计划投资 12.75 亿，实际投资已达 37.38 亿，2023 年的预算请求为 8.44 亿美元，远超 NQI 法案最初计划的 5 年 13 亿美元。2022 年 8 月，美国总统拜登签署了《2022 年芯片和科学法案》，为多个量子信息相关项目拨款近 8 亿美元。

欧盟方面，2018 年 10 月，欧盟正式实施“量子技术旗舰项目”，连同各成员国的配套，总经费超过 40 亿欧元；2021 年，欧盟提出天基安全连接计划，计划将卫星星座和欧洲量子通信基础设施集成，以借助量子加密技术为欧洲政府和军事组织提供安全通信，预估经费总额为 60 亿欧元；2023 年，德国政府通过“量子技术行动计划”，将在 2023-2026 期间投入约 30 亿欧元。2021 年 1 月，法国启动量子技术国家行动计划，5 年投资 18 亿欧元。2023 年 3 月，英国发布《国家量子战略》，将在 2024-2034 年间提供 25 亿英镑的政府投资，并吸引至少 10 亿英镑的额外私人投资。

表1：全球主要国家量子信息领域战略规划与投资概况（截至 2023 年 10 月）

时间	战略规划/法案	国家/地区	投资规模（美元）
2014	国家量子技术计划	英国	10 年投资约 12.15 亿
2018	光量子跃迁期间计划	日本	投资约 1.2 亿/年
2018	量子旗舰计划	欧盟	10 年投资约 11 亿
2018	国家量子信息科学战略 国家量子倡议（NQI）法案	美国	计划 5 年投资 12.75 亿， 实际投资已达 37.38 亿
2018	量子技术从科研到市场	德国	投资约 7.1 亿
2019	量子技术发展国家计划	荷兰	7 年投资约 7.4 亿
2019	国家量子技术计划	以色列	5 年投资约 3.3 亿
2019	国家量子行动计划	俄罗斯	5 年投资约 5.3 亿
2020	国家量子技术投资计划	法国	投资约 19.6 亿
2021	量子系统研究计划	德国	5 年投资约 21.7 亿
2022	国家量子计算平台	法国	投资约 1.85 亿
2022	芯片与科学法案	美国	4 个量子项目 1.53 亿/年
2023	国家量子战略	加拿大	投资约 2.7 亿
2023	国家量子战略（NQS）	英国	10 年投资 31.8 亿
2023	国家量子战略	澳大利亚	投资约 6.4 亿
2023	国家量子技术战略	丹麦	5 年投资约 1 亿
2023	量子科技发展战略	韩国	2035 年前投资 17.9 亿
2023	国家量子任务	印度	2030 年前投资 7.2 亿

资料来源：信通院《量子信息技术发展与应用研究报告 2023》，国投证券研究中心

美国：发布《国家量子倡议法案（NQI）》与专项战略，推动量子科技发展。美国是较早开展量子信息科学研究的国家之一，特别注重通过政府顶层设计推动量子信息科学（QIS）发展，经过多年发展，已形成立法保障、制定专项战略和优先发展相互衔接配套的政策体系，多方位支撑 QIS 发展。一是颁布法案，2018 年，美国《国家量子倡议法案（NQI）》正式生效，该法案既是美国统筹国内力量推进 QIS 发展的法律基础，也是美国谋求 QIS 及其技术应用全球领导地位的战略规划。法案共有五大目标：1）支持 QIS 研发、示范和应用；2）加强联邦政府 QIS 研发的跨部门规划与协调；3）最大限度地发挥联邦政府 QIS 研发和示范项目的效能；4）促进联邦政府、联邦实验室、企业和大学之间的合作；5）促进 QIS 安全国际标准的制定。二是制定 QIS 专项战略。三是近期综合科技战略将 QIS 作为优先发展方向。无论联邦政府层面还是机构层面的科技发展战略，其优先发展事项中不乏 QIS 的身影。例如，2020 年 10 月美国政府发布的《关键与新型技术国家战略》将 QIS 列为 20 项关键与新兴技术之一。

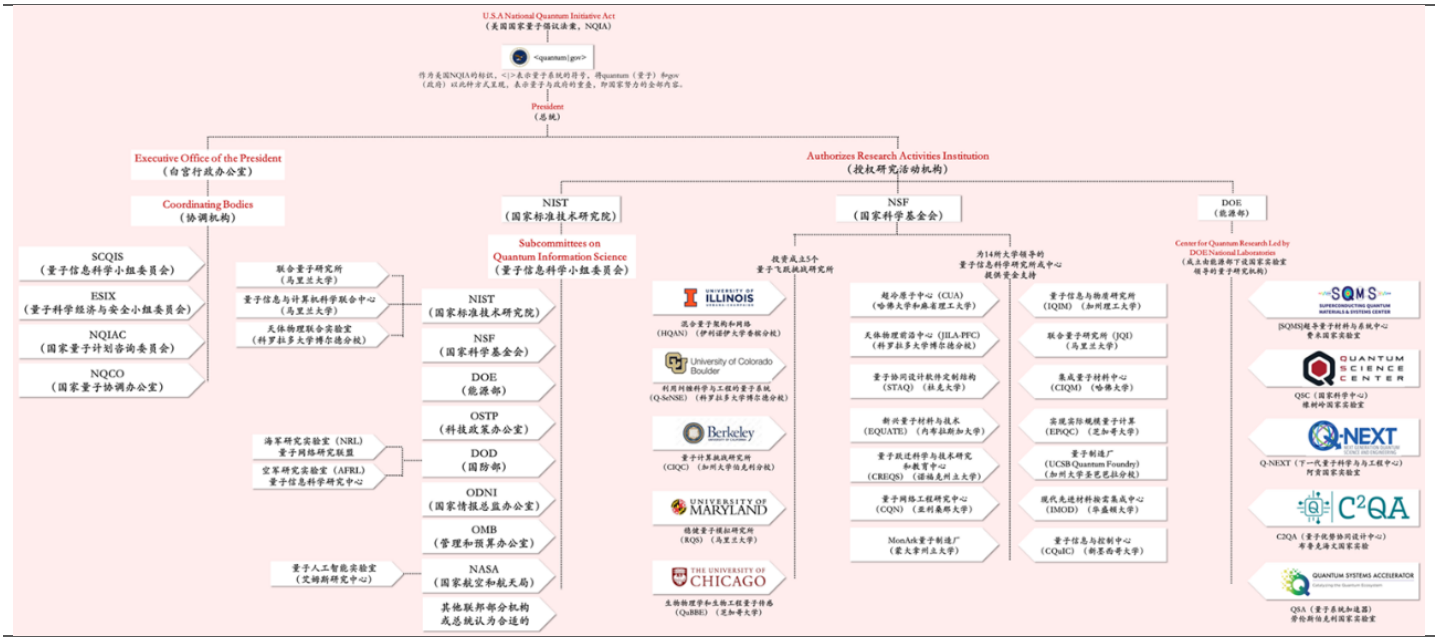
表2：美国量子战略和专项计划

时间	机构	战略规划名称	内容
2020 年 2 月	白宫国家量子协调办公室	《美国量子网络战略远景》	提出美国将开辟量子互联网，确保 QIS 惠及大众
2020 年 7 月	能源部（Department of Energy，DOE）	《从远距离纠缠到建设全国范围的量子互联网》	规划了美国第一个全国性量子互联网的战略发展蓝图，提出需要重点关注的 QIS 应用领域、优先研究方向，以及量子互联网建设的阶段性目标
2020 年 10 月	白宫国家量子协调办公室	《量子前沿报告》	确定八个方向为优先领域，指导后学量子研发投入：1）扩大量子技术造福社会的机会。2）建立 QIS 工程学科。3）QIS 靶向材料科学。4）通过 QIS 仿真探索量子力学。5）利用 QIS 技术进行精确测量。6）为新应用生成的分配量子纠缠。7）表征和缓解量子误差。8）通过 QIS 了解宇宙。
2020 年 10 月	白宫	《关键与新兴技术国家战略》	将 QIS 列为 20 项关键与新兴技术之一，认为 QIS 对军事、情报和经济等国家安全优势具有至关重要的作用。
2021 年 1 月	国家科学技术委员会	《量子网络研究的协调办法》	确定了《美国量子网络战略远景》中所提出的目标的实现途径，确定了联邦机构可以采取的行动，以增进国家的知识基础并准备使用量子网络。

资料来源：《世界科技研究与发展：量子科技创新战略研究》，国投证券研究中心

美国：NQI 计划提供总体框架，加强与协调量子研发活动。在立法方面，迄今为止与量子有关的最重要立法是《国家量子倡议法案》(NQI)，该法案于 2018 年 12 月签署成为联邦法律，旨在加速和推进美国的量子科学技术。从本质上讲，NQI 为量子研发创建了一个框架，并授权在 2019-2023 年提供略高于 12 亿美元的资金，用于各种量子研究和开发项目。这些资金主要分配给历来积极参与量子科学与技术研发的三个机构：美国国家标准与技术研究院(NIST)、美国国家科学基金会(NSF)和美国能源部(DOE)。NQI 法案授权这些机构加强 QIS 计划和研究中心；建立一个新的联邦机构，名为国家量子协调办公室(NQCO)；成立一个新的联邦咨询委员会，名为国家量子计划咨询委员会(NQIAC)，由来自学术界、工业界和政府的专家组成，其任务是为国家量子计划提供独立评估和建议。

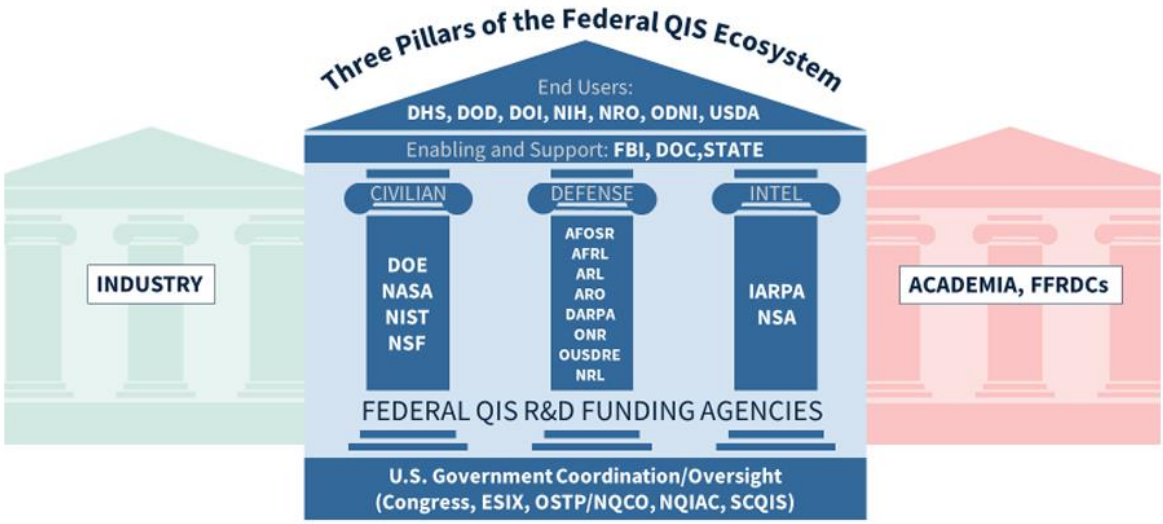
图3. 美国量子信息技术实施机构及组织架构



资料来源：ICV，国投证券研究中心

美国：打造量子生态三大支柱，共筑量子领域领导地位。量子信息科学(QIS)研发资助机构可被视为支持量子信息产业生态系统的三大支柱，民用科学机构、国防部科学机构和情报部科学机构共同支持量子信息产业的研发工作。**1）美国国家标准与技术研究院(NIST)：**通过扩展和连接量子系统、提高设备性能和稳定性、丰富人才库、制定技术标准等多种方式，推进测量科学标准，促进美国的创新与工业竞争力；开展在量子传感、计算、网络、风险缓解、基础科学等方面的核心技术项目；建立并支持量子经济发展联盟，致力于通过识别技术、供应链、标准、劳动力和通过合作解决各方面差距的方法，加速美国量子产业增长。**2）美国国家科学基金会(NSF)：**资助超过 2000 个学术机构的量子科学与工程研究；NQI 法案明确要求 NSF 支持量子信息科学研究与教育的多学科中心，协调量子计算核心项目。此外，NSF 在 2024 财年预算中向国会阐明两大投资目标：①量子计算、量子通信、量子测量、量子网络的先驱发展，提高信息处理、传输与测量效率；②开发具有明显量子优势的概念研制设备、工具、系统和应用程序。**3）美国能源部(DOE)：**通过基础和应用科学研究、新技术的发现和开发、同位素生产等多种方式推进量子技术发展；NQI 法案授权能源部建立 5 个国家量子信息科学研究中心，并在核心项目中继续加强和协调量子研究。**多个量子研究活动机构在量子信息科学基础研究、教育、培训和劳动力发展方面的投资相互促进、相辅相成，加快美国在量子信息服务领域的领导地位。**

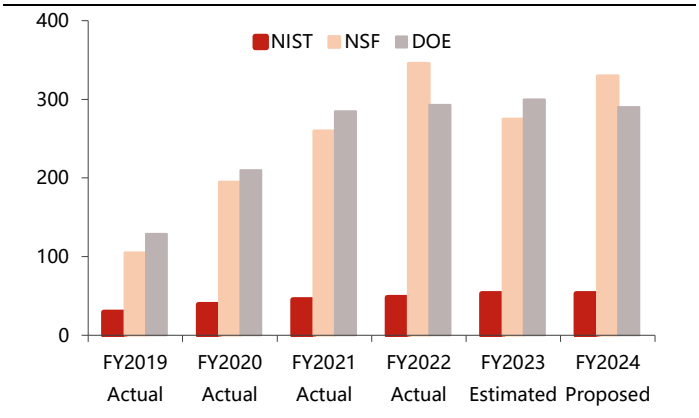
图4. 量子科学生态系统三大支柱



资料来源：《NQI Annual Report FY2024》，国投证券研究中心

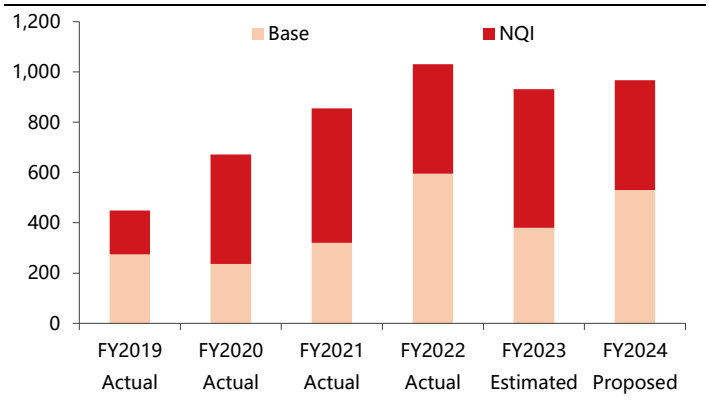
美国：量子科技研发资金大幅增加，推动量子科技快速发展。在 NQI 法案的推动下，用于 QIS 研发的联邦资金大幅增加。从 2019 财年到 2024 财年，联邦资金大约翻了一番。2023 年 12 月 1 日，《国家量子计划（NQI）总统 2024 财年预算补编》发布，这是《国家量子计划法案》（NQI）要求的第四份 NQI 计划年度报告，2019-2024 财年量子信息科学预算分别为 4.49/6.72/8.55/10.31/9.32/9.68 亿美元。此外，**分配给 NQI 法案授权活动的资金是在基线量子信息服务研发活动预算之外的额外资金。**然而，虽然《国家质量与创新法案》为各联邦机构的质量信息系统研发设定了资助目标和优先事项，但并不保证具体的资助金额。总统和国会通过年度财政年度预算确定各联邦机构的非国防量子研发优先事项和资金，国防开支则通过名为《国防授权法案》的单独法案确定。

图5. 三大研发机构资金规划情况



资料来源：《NQI Annual Report FY2024》，国投证券研究中心

图6. 美国 NQI 法案颁布后的 QIS 量子战略总体联邦预算（百万美元）



资料来源：《NQI Annual Report FY2024》，国投证券研究中心

NQI 法案修订后增加预算总规模，根据 ICV 计算显示，未来美国量子科技预算总额超过 36 亿美元，其中 NQI 法案拟议更新的资金规划共 22.33 亿美元，芯片与科学法案授权资金规划共 14.24 亿美元。

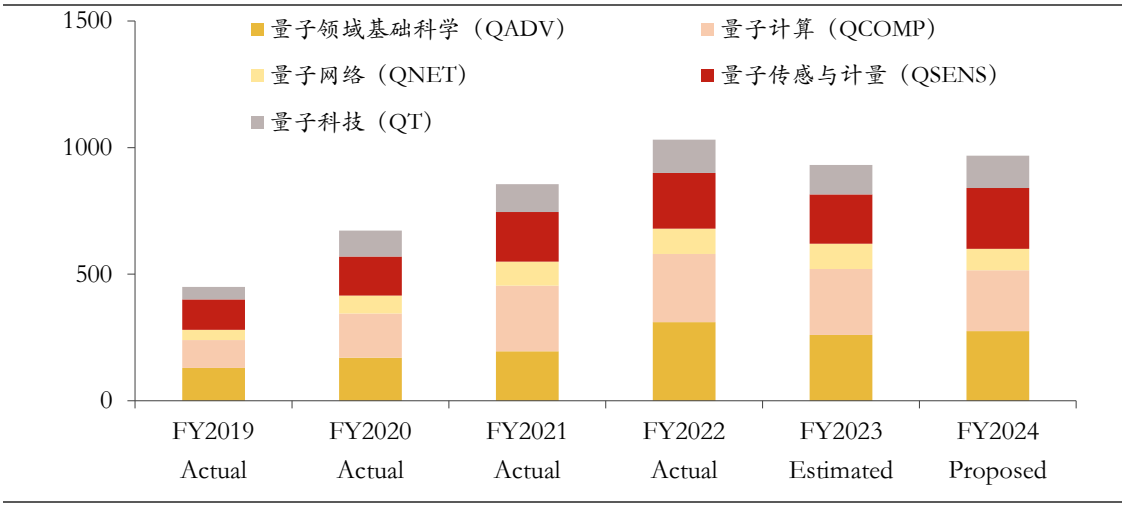
表3：NQI 法案拟议资金（2024-2028）

NQI 再授权法案参考章节	机构	年投资金额（百万美元）	投资周期（年）	投资总额（百万美元）	法案依据	目的
11	NIST（国家标准技术研究院）QED-C（量子经济发展联盟）	85	4	340	芯片与科学法案	开展研发和示范项目，促进量子应用的发展和标准化；支持量子技术可比性能相关研究；促进量子相关国际事务参与；建立必要的基础设施项目
12	NIST（国家标准技术研究院）	54	5	270	NQI 再授权法案	NIST 建立新的、目的驱动的量子中心，加速 NIST 研发、部署和标准化活动，并优先考虑量子测量和量子工程
13	NSF（国家科学基金会）	141	4	564	芯片与科学法案	量子信息科学研究与教育项目
14	NSF（国家科学基金会）	100	5	500	NQI 再授权法案	多学科量子研究和教育中心，
15	NSF（国家科学基金会）	10	5	50	NQI 再授权法案	建立量子再培训教育与劳动力协调中心（QREW）
15	NSF（国家科学基金会）	50	5	250	NQI 再授权法案	建立新的量子试验台
16	DOE（能源部）	130	4	520	芯片与科学法案	能源量子信息科学研究项目，指导制定十年战略计划，指导联邦设计、开发、商业化以量子为中心的高性能计算系统
17	DOE（能源部）	25	5	125	NQI 再授权法案	建立量子仪器和基础设施计划，以应对量子供应链特有的挑战和需求
18	DOE（能源部）	175	5	875	NQI 再授权法案	对能源部进行技术修正指导，并确保合作事务包括多样化的可行量子技术
20	DOE（能源部）	38	1	38	NQI 再授权法案	指导能源部与公共部门、私营部门多方合作开发基于云的量子计算机算法和应用，并探索教育与培训计划。
21	NASA（国家航空航天局）	25	5	125	NQI 再授权法案	授权 NASA 开展量子基础与应用研究，建立 NASA 专属量子研究所，专注于量子科技航空航天应用
NQI 法案修订后的资金规划				**2,233**		
芯片与科学法案授权资金规划				**1,424**		
资金规划总额				**3,657**		

资料来源：《世界科技研究与发展》，国投证券研究中心

美国：明确五大资金投入领域，增加资金投入。美国政府在《量子信息科学国家战略概述》中划分的所有五个计划组成领域，即量子传感与计量(QSENS)、量子计算(QCOMP)、量子网络(QNET)、量子发展(QADV)和量子技术(QT)，都增加并保持了资金投入。

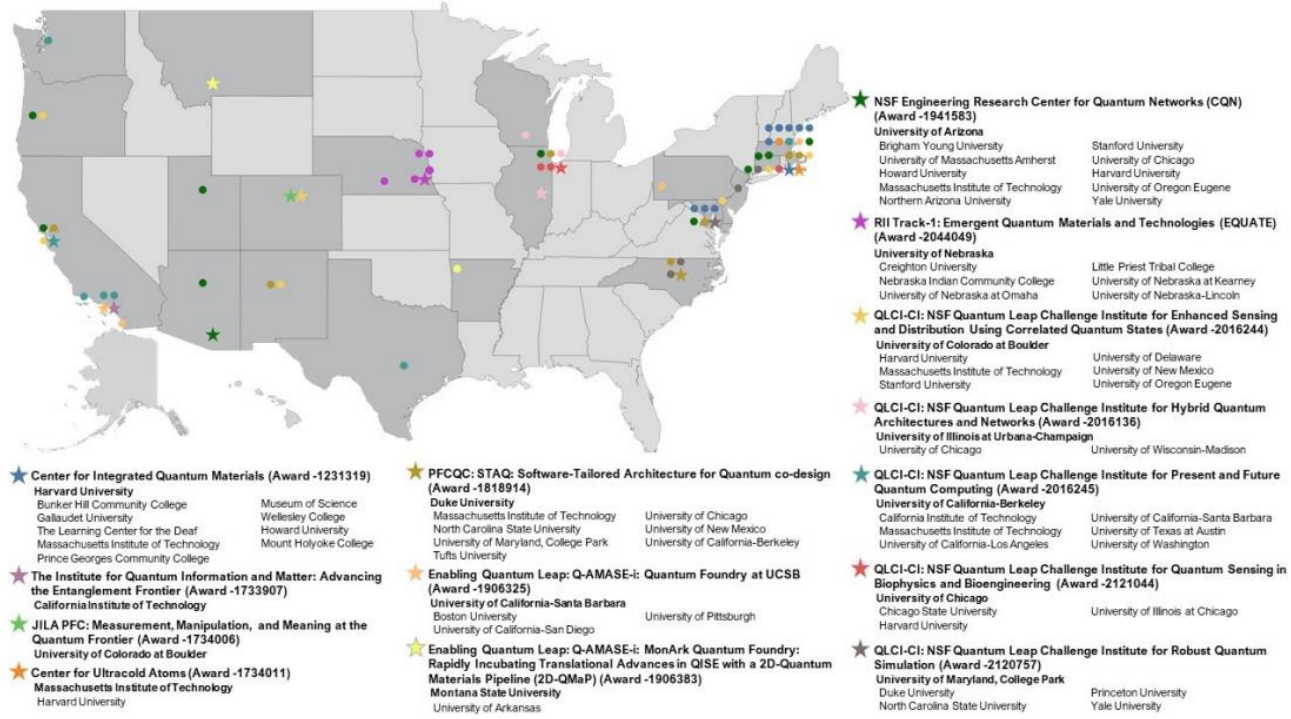
图7. 按项目组成领域划分的美国量子信息科学研发情况



资料来源：《NQI Annual Report FY2024》，国投证券研究中心

美国：促进量子跨学科研究，推进量子科技快速发展。美国国家科学基金会(NSF)和能源部(DOE)都在通过支持建立跨学科研究中心来克服这些机构障碍，采取不同的方法以反映其不同的使命和资助重点。国家科学基金会的重点是促进大学中心和研究所的教师开展跨学科合作，**截至 2023 年 3 月，该机构已资助了五个量子飞跃挑战研究所。**另一方面，能源部已在自己的国家实验室建立了跨学科量子研究中心。对此，负责国家量子计划评估工作的国家量子信息中心对量子合作的进展进行了评估，发现总体而言各中心之间的合作发展良好。

图8. 国家自然科学基金委员会对 QIS 研究中心的规模投资



资料来源：ICV，国投证券研究中心

欧盟：发布《量子宣言》和量子旗舰计划，多方位发展量子信息技术。2016 年 3 月，欧盟委员会发布《量子宣言（草案）》，呼吁欧盟成员国及欧盟委员会**发起资助额达 10 亿欧元的量子技术旗舰计划，并实现如下目标：**1）建立极具竞争性的欧洲量子产业，确保欧洲在未来全球产业蓝图中的领导地位；2）增强欧洲在量子研究方面的科学领导力和卓越性；3）面向量子技术的创新企业和投资，把欧洲打造为一个有活力和吸引力的区域；4）充分利用量子技术进展，更好地解决能源、健康、安全和环境等领域的重大挑战。宣言提出，欧洲旗舰计划应集合工程、科学、教育以及创新能力，充分释放量子技术的潜能。通过通信、模拟器、传感器和计算机这四方面的短中长期发展，实现原子量子时钟、量子传感器、城际量子链接、量子模拟器、量子互联网和泛在量子计算机等重大应用。

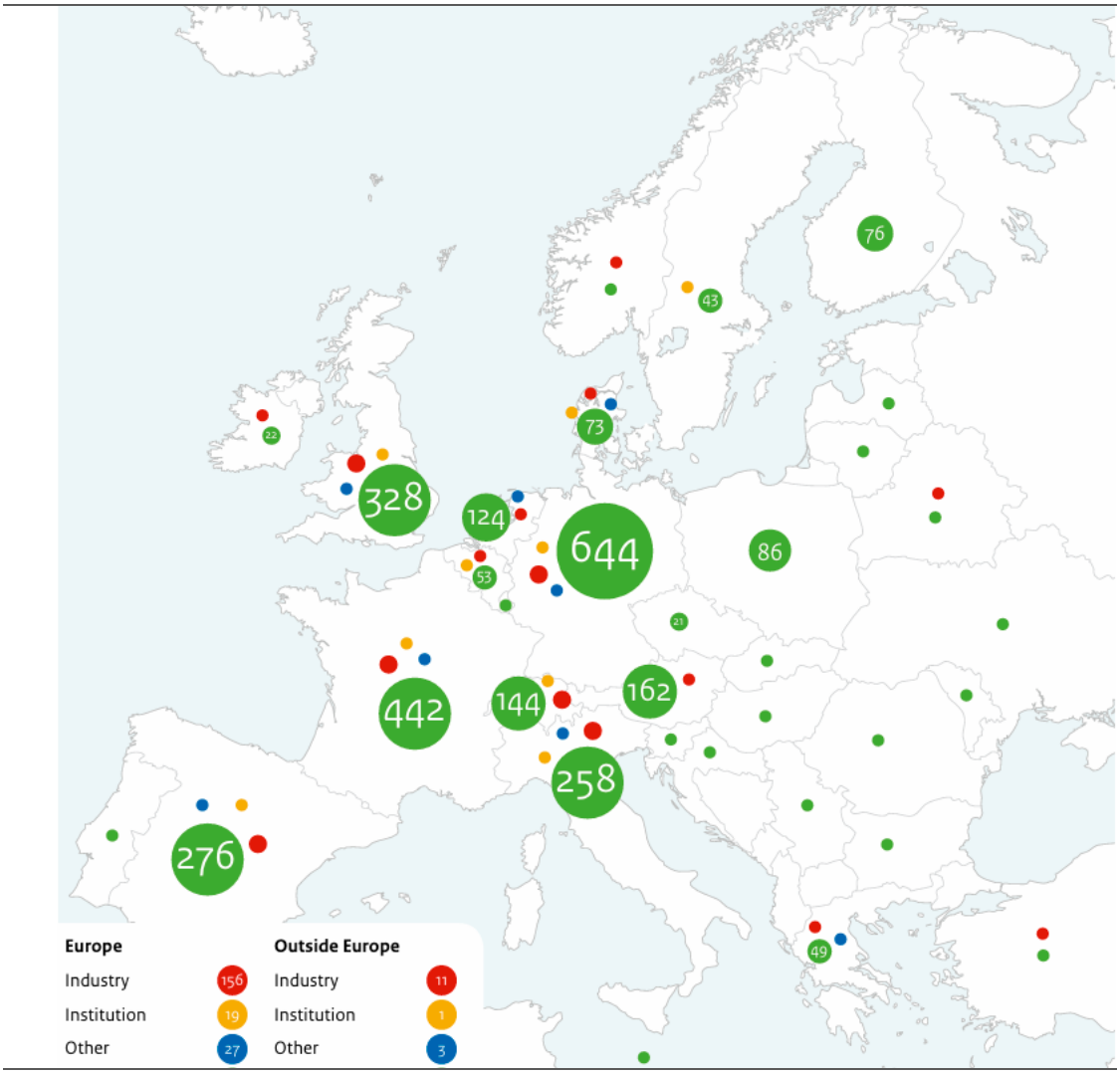
表4：欧盟量子技术的短中长期目标

量子技术及发展目标	通信（城际量子连接、量子互联网）	模拟器（量子模拟器）	传感器（原子量子时钟、量子传感器）	计算机（量子计算机）
短期（5 年内）	量子中继器核心技术； 安全的点到点量子链接。	材料中电子运动的模拟器； 针对量子模拟器和网络的新算法	针对医疗护理、地理调研和安全等新型应用的量子传感器； 针对高频金额交易的时戳打造更准确的原子时钟。	运行受纠错或拓扑学保护的逻辑量子位； 针对量子计算机的新算法； 能执行技术相关算法的小型量子处理器。
中期（5-10 年）	远距离城市间的量子网络； 量子信用卡	设计和开发新型复合材料； 有关量子磁性和电流的多样化模拟器。	针对汽车建筑等大规模应用的量子传感器； 手持量子导航设备。	利用专业型量子计算机解决化学和材料科学难题。
长期（10 年以上）	具有加密和监听检测功能的量子中继器； 结合量子与传统通信的泛欧安全互联网。	有关量子动力学和化学反应机制的模拟器，用以支持药物设计。	基于重力传感器的重力成像设备； 将量子传感器集成到消费者应用中（包括移动设备）。	结合量子路线和低温传统控制硬件； 超越传统计算机能力的通用量子计算机。

资料来源：《Quantum Manifesto》，国投证券研究中心

欧盟：组织和成员国双层发力，明确四大领域发展路线。近年来，为在全球量子科技竞争中赢得主动，欧盟和欧洲主要国家积极布局，在组织和成员国两个层面出台了一系列量子科技战略。**在组织层面，**欧盟牵头制定泛欧洲的量子技术发展战略。2020 年 3 月，量子旗舰战略咨询委员会发布的报告《战略研究议程》对量子技术旗舰计划进行了细化，提出量子通信、量子计算、量子模拟，以及量子计量和传感等领域的发展路线图。**在成员国层面，**法国和德国制定战略谋划未来量子科技发展。《量子宣言》得到 3400 多名学术界与工业界人士的支持。

图9. 欧盟《量子宣言》成员国和组织数量分布



资料来源：《Quantum Manifesto》国投证券研究中心

欧盟投入规模达 10 亿欧元，资助四大领域科研项目。欧洲量子技术旗舰计划是欧盟未来新兴技术旗舰计划（FET）的重要组成部分，FET 旨在为欧盟革命性、高风险、高回报的技术创新及商业开发提供长期稳定支持，量子技术旗舰计划是 FET 中执行期最长、资助强度最大的计划。量子技术旗舰计于在 2018 年正式启动，项目为期 10 年，总研发投入规模达 10 亿欧元。

旗舰计划实施分为两个阶段：1）导入期（2018-2021）：由地平线 2020 计划提供支持，投资总额预计为 1.32 亿欧元；2）发展期（2021-2027）：由“未来第九研发计划”（FP9）提供支持。**第一阶段，计划将资助量子基础科学、量子计算、量子互联网、量子模拟和量子传感领域的 24 个项目。**欧洲议会、欧洲理事会和欧盟委员会正在磋商，以确保量子研发将在欧盟 2021-2028 年的多年度财务框架中得到资助。受资助的项目中，超过三分之一为参与者是来自各行各业的工业公司，其中大部分是中小企业。

表5：欧盟“量子宣言”旗舰计划首批科研项目

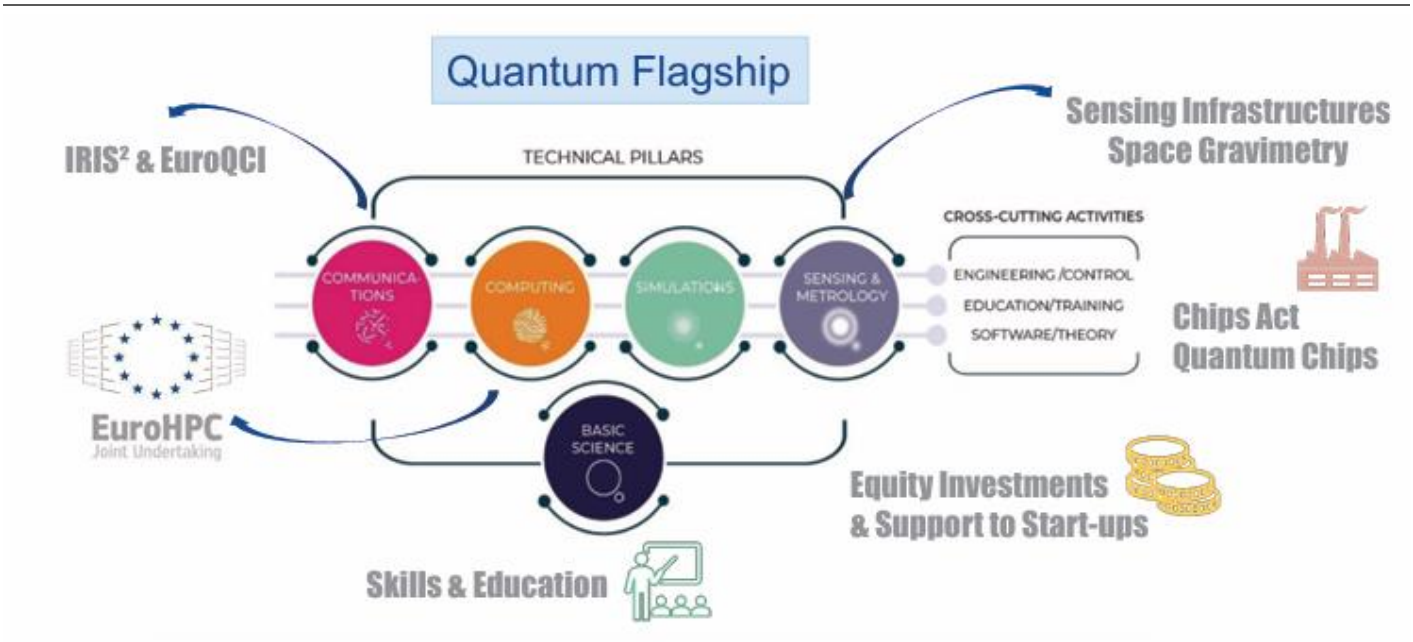
量子通信方向			
连续变量量子通信	CIVIQ	ICFO，西班牙	基于 PIC 的 CV-QKD 系统，面向电信运营商的网络部署和应用验证
量子互联网联盟	QIA	Delft，荷兰	基于量子中继器的量子隐形传态网络，连接量子计算平台物理比特
量子随机数生成器	QRANGE	Geneva，瑞士	集成化 CMOS 工艺 SPAD，随机数产生速率> 10Gbps 芯片化 QRNG
实用化量子通信	UNIQORN	AIT，奥地利	InP 平台量子片上系统，可用于量子隐形传态、单光子 QKD 和压缩态
量子计算+模拟方向			
离子阱量子计算	AQTION	Innsbruck，奥地利	可扩展离子阱量子计算物理平台及多激光器操作系统，全自动运行
开放超导量子计算机	OpenSuperQ	Saarlanders，德国	开放式超导量子计算机硬件+软件+优化工具，50 -100 量子比特
可编程原子大规模量子模拟	PASQuanS	Max-Planck，德国	500 位中性原子和离子平台离子模拟器，面向离子退火与优化问题
级联激光器频率梳量子模拟	Qombs	Consglio，意大利	光学晶格超冷原子离子模拟器，研究载波传输离子动态效应和传感
新一代量子计算应用	NEASQC	Leiden，荷兰	研究、开发量子应用，利用 NISQ 含噪声量子系统解决实际问题，如药物发现、二氧化碳捕获、智能能源管理、自然预研处理等，旨在通过提供通用工具集吸引工业用户。
硅中的量子大规模集成	QLSI	fraunhofer，德国	为量子计算开发一种可拓展的硅量子比特技术
量子测量方向			
金刚石色心量子测量	ATERIQS	Thales,法国	固态金刚石 NV 色心探针，高动态范围多用途量子传感器
集成化量子钟	IqClock	Amersterdam，荷兰	集成化光原子晶格钟，小型化锶原子钟，超辐射原子钟
微型原子气室量子测量	MACQSIMAL	CSEM，瑞士	基于 MEMS 原子蒸汽腔的量子陀螺、量子重力仪和气体传感器
金刚石动态量子多维成像	MetanoliQs	Fraunbofer，德国	基于金刚石 NV 色心偏振器的超极核磁共振（MRI）医学成像
量子基础科研			
二维量子 PIC 材料与器件	2D-SIPC	ICFO，西班牙	用于可扩展集成光子电路（PIC）的二维量子材料和器件集成
微波驱动离子阱量子计算	MicroQC	TCPA，保加利亚	微波控制微加热技术多比特离子阱逻辑门和量子处理器设计
亚泊松分布光子枪	PhoG	Andrews，英国	集成化高确定性非传统光源，如亚泊松分布光源和多模纠缠光源
基于光子的量子模拟	PhoQuS	Sorbonne，法国	基于多光子量子超流体和量子湍流转台的量子模拟新平台
量子微波计算和传感	QMICS	Bayorlsche，德国	微波频段单光子探测，数米距离的量子微波互联分布式量子计算
可扩展二维量子 PIC	S2QUIP	Kungliga，瑞典	小型通用化光源和集成光子电路，为量子通信提供信息载体
可扩展稀土离子量子计算	SQUARE	KIT，德国	基于稀土离子材料的离子物理比特高密度集成和光学互联

离子协调、合作与教育			
量子旗舰的协调和支持行动	Qflag	欧盟	核心任务是建立一个学术界与工业界的旗舰社区，以准备和实施欧洲量子技术战略研究议程，将确定用例，分析并提供关键的量子技术基础设施，并动员欧盟成员国将量子技术从实验室推向商业阶段。
量子技术国际合作	IncoQFlag	欧盟	旨在确定与美国、加拿大和日本等大量投资量子技术的国家合作的双赢局面
量子技术教育的协调和支持行动	QTEdu	欧盟	协助欧洲量子旗舰计划构建必要的量子学习生态，向社会教育普及量子科技

资料来源：《Quantum Manifesto》，国投证券研究中心

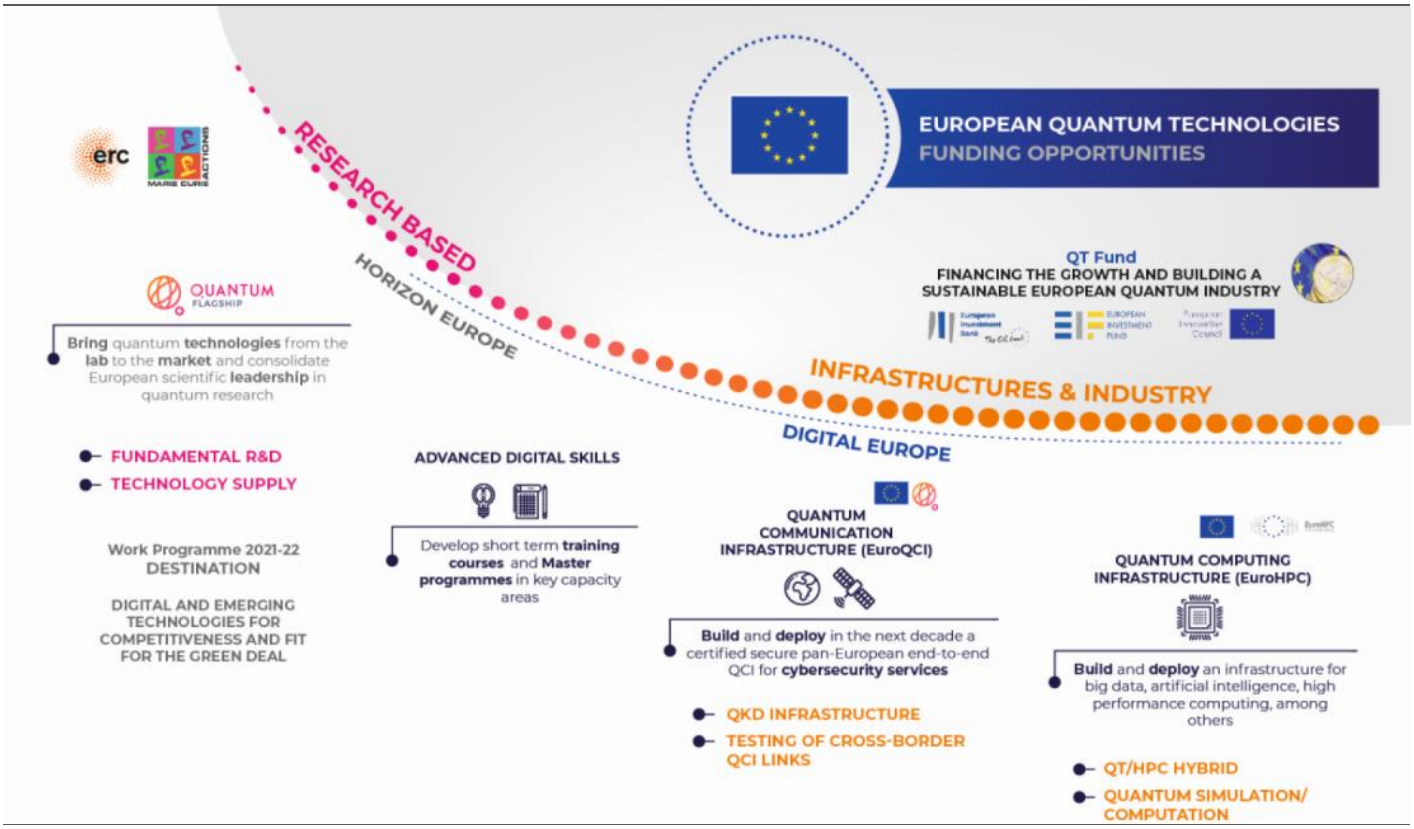
欧盟：大力投入基础设施，推进量子技术发展。在量子旗舰计划中，欧盟也通过在量子基础设施等关键领域进行专门的投资，展示量子技术部署，例如，EuroQCI 欧洲量子通信基础设施部署规划和 EuroQCS 欧洲量子计算和模拟基础设施部署规划。**量子通信方面，**通过 EuroQCI 进行量子通信基础设施建设，联合 27 欧盟成员国和欧洲航天局共同设计、开发和部署最先进的量子通信地面和空天的基础设施。地面部分依赖于光纤通信网络，连接国内外战略站点。同时，空天部分利用卫星形成欧盟新的天基安全通信系统 IRIS。EuroQCI 结合地面和空天能力，旨在建立高度安全可靠的量子通信网络，并在安全数据传输和量子密码学等领域取得突破。**量子计算方面，**EuroQCS 计划重点推进量子计算和模拟的基础设施，旨在将量子计算机和模拟器集成到欧洲的超级计算基础设施中，促进量子模拟和量子计算在各个领域的突破性研究。量子计算机被集成到选定主机上的现有超级计算机中。目前，欧盟的六个站点已被选中托管和运行首批 EuroHPC 量子计算机，包括捷克、德国、西班牙、法国、意大利和波兰。这些量子计算机将主要供欧洲用户用于研究和开发，惠及科学界、工业界和公共部门。

图10. 量子旗舰计划构建欧洲量子生态



资料来源：《Strategic Research and Industry Agenda》,国投证券研究中心

图11. 欧洲量子技术部署方向



资料来源：Quantum Flagship 官网,国投证券研究中心

欧盟：布局四大研发方向，规划明确发展路线。欧盟量子旗舰计划分别规划了量子通信、量子计算、量子模拟、量子传感与测量四大领域的短期、中期发展路线。**短期来看，在量子通信领域，**欧盟注重开发用例和业务模型，开发光纤、自由空间和卫星链路的可信节点网络功能和互操作性；开发基于卫星的离子密码术等。**在量子计算领域，**欧盟计划短期实现容错用用量子计算机的实用策略，确定具有优势的算法和用例，启动更深的算法，与芯片和软件提供商联络，实现量子器件物理、量子位和栅极控制，实现与材料科学、理论物理学等领域合作。**在量子模拟领域，**欧盟计划演示特定任务中的优势，利用量子模拟加快机器学习，提供控制水平和可伸缩性，扩大供应链，加强关键使能技术的开发等。**在量子测量领域，**欧盟计划短期建立可靠、高效的供应链，进行首次标准化，研发光电集成芯片，使用纳米加工等技术进行材料工程研发，建立新传感器技术的标准等。

中期来看，在量子通信领域，欧盟计划实现远距离量子中继器、至少 20 个量子位的量子网络节点、在独立于平台的软件中的量子网络应用程序、与设备无关的 QRNG 和 QKD 等。**在量子计算领域，**欧盟计划研发具有量子误差校正和强大量子位的量子处理器、优于传统计算机的通用门、具有量子优势的量子算法，建立能够制造所需技术的制造厂，研究材料、量子器件物理、量子位和栅极控制、量子存储器、光子学、RF、低温和超导体电子学、系统工程和器件封装等。**在量子模拟领域，**欧盟提出与最终用户建立紧密联系，开发更多实际应用，提供更高程度的控制和可编程性的量子模拟器；使用量子模拟器解决化学、复杂量子系统和材料科学中的问题，与企业密切联系保持投资；开发带有计算机科学概念的软件；建立量子模拟和计算相关研究机构与企业之间的合作。**在量子测量领域，**欧盟提出发展技术和材料工程，将量子传感器推向市场；集成用于仪器自校准的量子测量标准；建立关键技术制造厂等。

表6：量子旗舰四大研发领域的未来发展路线

领域	短期发展路线（2024-2026）	中期发展路线（2027-2030）
量子通信	1）开发用例和业务模型；2）开发光纤，自由空间和卫星链路的可信节点网络功能和互操作性；3）开发基于卫星的离子密码术；4）开发标准、量子随机数发生器（Quantum Random Number Generation,QRNG）和 QKD 的认证方法；5）开发测试套件；6）演示基于卫星通信的关键组件；7）标准化 QKD 卫星和地面站组件；8）改进了设备和组件的性能，解决与密码学和网络应用相关的参数基准；9）演示基本链接、应用程序协议等。	1）远距离量子中继器；2）至少 20 个量子位的量子网络节点；3）在独立于平台的软件中的量子网络应用程序；4）与设备无关的 QRNG 和 QKD；5）使用基于卫星的纠缠；6）开放式开发基于结构，用于教育和吸引未来劳动力；7）建立强大的量子通信供应链。
量子计算	1）容错用用量子计算机的实用策略；2）确定具有优势的算法和用例；3）启动更深的算法；4）与芯片和软件提供商联络；5）量子器件物理、量子位和栅极控制；6）与材料科学、理论物理学等领域合作；7）标准等。	1）具有量子误差校正和强大量子位的量子处理器，优于传统计算机的通用门；2）具有量子优势的量子算法；3）建立能够制造所需技术的制造厂，包括集成光子、低温和超导电子产品；4）支持仪器制造商和软件公司；5）研究材料、量子器件物理、量子位和栅极控制、量子存储器、光子学、RF、低温和超导体电子学、系统工程和器件封装；6）扩展量子算法套件；7）优化编译器和编译库；8）演示自动化系统控制和调优；9）开发集成工具链和模块库，集成光学器件、低温和超导体电子器件；10）协调材料科学、理论和低温物理学、电气工程、数学和计算机科学领域研究；11）整合中小企业、大型企业和制造厂；12）和欧盟的基础设施计划、大型实验室和 RTOs 协调开展。
量子模拟	1）特定任务中的优势；2）利用量子模拟加快机器学习；3）提供控制水平和可伸缩性；4）与产业互动在复杂研究中应用；5）扩大供应链，加强关键使能技术的开发；6）认证和基准测试等。	1）与最终用户建立紧密联系，开发更多实际应用；2）提供更高程度的控制和可编程性的量子模拟器；3）使用量子模拟器解决化学、复杂量子系统和材料科学中的问题，与企业密切联系保持投资；4）开发带有计算机科学概念的软件；5）建立量子模拟和计算相关研究机构与企业之间的合作。
量子传感和计量	1）建立可靠、高效的供应链，进行首次标准化；2）研发光电集成芯片；3）使用纳米加工等材料工程；4）建立新传感器技术的标准；5）量子电气标准雏形；6）可移动光学时钟原型；7）基于人造原子或量子光电系统的可移动电、磁、温度和压力传感器原型；8）量子增强型，超分辨型和/或亚散电噪声显微镜等。	1）发展技术和材料工程，将量子传感器推向市场；2）集成用于仪器自校准的量子测量标准；3)建立关键技术制造厂；4）基于生物医学应用的功能化材料、感应电场和磁场集成原子芯片，制造光电集成芯片实验平台；5）量子增强的测量和成像设备；6）商业产品，例如新型磁共振成像磁力计，高性能光学时钟和原子干涉仪；7）量子传感器网络以及增强型量子传感器网络。

资料来源：《Strategic Research and Industry Agenda》，Quantum Flagship，国投证券研究中心

欧盟：明确量子技术关键绩效指标。欧盟在量子旗舰计划中提出 2030 年计划实现的几大量子技术关键绩效指标，包括繁荣与就业、数字自治和技术领先、人民利益、凝聚力与多样性、量子通信、量子计算、量子模拟、量子传感与测量、教育和多样性九大方向。其中，**在量子通信领域，**欧盟提出创建跨领域的量子安全网络、具有卫星链路的互联光纤网络，以及利用纠缠性和量子中继器的远程量子通信网络；将欧洲所有国家连接到量子通信网络；结合后量子密码学，创建量子安全网络功能和密钥分发，用于 IoT、5G、SDN 和关键基础设施，以及利用远程量子处理器、时钟和传感器之间的远程纠错量子互联网应用。

在量子计算方面，欧盟提出构建至少 1000 个物理量子位的全栈、高度连接、高保真度量子计算机，展示可扩展性能，并能够在相关的实际用例中超越经典计算机；为科学和技术用户提供欧洲量子计算基础设施，以超越当前最好的超级计算机。

在量子模拟方面，欧盟提出构建可编程的欧洲量子模拟器，能够模拟远超经典的难以计算的量子或经典系统的可能性；能够访问欧洲量子模拟设施，并在相关的实际用例中超越最好的超级计算机。

在量子测量方面，欧盟提出广泛部署，使用量子传感器网络进行地面和天基的实际演示；可用性方面，工业界要开发量子产品生产和制造设施以及产学研试验线，以促进产品开发和快速创新；市场准备方面，面向高性能和大众市场的商业产品，以及基于全球公认的标准和可追溯的量子测量和校准服务，利用量子传感器扩展产品组合，以应对卫生、运输、导航和电信探索、科学和气候挑战。

表7：欧洲量子技术关键绩效指标梳理（2030）

领域	关键绩效指标
繁荣和就业	欧洲的量子产业在就业数量和质量/产量/市场份额方面属于世界前两大量子科技产业
数字自治和技术领先	不同领域价值链的完整性，在核心量子科技产业应用领域拥有领先的知识产权地位
人民利益	为欧洲公民在应用领域带来突破性的进步，使欧洲公民能够通过提高认识来充分利用了科技潜力
凝聚力和多样性	来自不同领域的量子科技跨成员国合作，包括工业、学术界和公共部门项目，以确保凝聚力和多样性
通信	创建跨领域的量子安全网络、具有卫星链路的互联光纤网络，以及利用纠缠性和量子中继器的远程量子通信网络；
	可访问性：将欧洲所有国家连接到量子通信网络；
	功能：结合后量子密码学，创建量子安全网络功能和密钥分发，用于 IoT、5G、SDN 和关键基础设施，以及利用远程量子处理器、时钟和传感器之间的远程纠错量子互联网应用。
计算	能力：构建至少 1000 个物理量子位的全栈、高度连接、高保真度量子计算机，展示可扩展性能，并能够在相关的实际用例中超越经典计算机。
	可用性：为科学和技术用户提供欧洲量子计算基础设施，以超越当前最好的超级计算机。
模拟	能力：构建可编程的欧洲量子模拟器，能够模拟远超经典的难以计算的量子或经典系统的可能性；
	可用性：能够访问欧洲量子模拟设施，并在相关的实际用例中超越最好的超级计算机。
传感和计量学	能力：广泛部署，使用量子传感器网络进行地面和天基的实际演示。
	可用性：工业界正在开发自己的量子产品生产和制造设施，以及产学研试验线，以促进产品开发和快速创新，特别是对初创企业和中小企业。
	市场准备：面向高性能和大众市场的商业产品，以及基于全球公认的标准和可追溯的量子测量和校准服务，利用量子传感器扩展产品组合，以应对卫生、运输、导航和电信探索、科学和气候挑战。
教育和多样性	教育和培训：在所有教育和技能水平上建立自我维持的泛欧量子技术教育计划。
	多样性和公平性：建立成熟和有效的计划，以解决、促进和实现泛欧范围内的包容性和公平性，涵盖量子技术的所有学术和工业相关层面。

资料来源：《Strategic Research Agenda & Key Performance Indicators》，European Quantum Flagship，国投证券研究中心

中国：多次强调量子科技关键技术前瞻战略布局，量子科技有望成为未来新质生产力。自 2006 年以来，我国国家相关部委制定了一系列推动量子科技产业发展下相关政策。其中，2021 年 12 月，国务院印发的《**“十四五”国家信息化规划**》中明确提到，加强人工智能、量子信息、集成电路、空天信息、类脑计算、神经芯片、DNA 存储、脑机接口、数字孪生、新型非易失性存储、硅基光电子、非硅基半导体等关键前沿领域的战略研究和技术融通创新。此外，《**“十四五”数字经济发展规划**》中亦明确提出增强关键技术创新能力，瞄准传感器、量子信息、网络通信、集成电路、关键软件、大数据、人工智能、区块链、新材料等战略性前瞻性领域，发挥我国社会主义制度优势、新型举国体制优势、超大规模市场优势，提高数字技术基础研发能力。**2024 年的政府工作报告中**，明确将量子技术列入未来产业，成为新质生产力的重要组成部分。3 月 29 日，**国务院国资委**遴选确定首批新质生产力的启航企业名单，重点布局了人工智能、量子信息和生物制药领域，量子科技再获重要关注。

表8：国内量子科技产业相关政策梳理

年份	机构	政策	具体内容
2006.2	国务院	《国家中长期科学和技术发展规划纲要（2006-2020 年）》	重点研究**量子通信**的载体和调控原理及方法，量子计算，电荷-自旋-相位-轨道等关联规律以及新的量子调控方法，受限小量子体系的新量子效应，人工带隙材料的宏观量子效应，量子调控表征和测量的新原理和新技术基础等。
2011.7	科技部	《国家“十二五”科技发展规划》	突破光子信息处理、**量子通信**、量子计算、太赫兹通信、新型计算系统体系、网构软件、大量数据处理、智能感知与交互等重点技术，攻克普适服务、人机物交互等核心关键技术。研发未来网络/未来互联网、下一代广播电视、卫星移动通信、绿色通道与融合接入、高性能计算与服务环境、高端服务器、大量存储与服务环境高可信如那件与服务、虚拟现实与智能表达等重大技术系统和战略产品。
2016.3	全国人大	《中华共和国国民经济和社会发展第十三个五年规划纲要》	着力构建量子通信和泛在安全物联网，加快发展合成生物和再生医学技术，加速开发新一代核电装备和小型核动力系统、民用核分析与成像，打造未来发展新趋势。
2016.5	国务院	《国家创新驱动发展战略纲要》	面向 2030 年……在**量子通信**、信息网络、智能制造和机器人、深空深海探测、重点新材料和新能源、脑科学、健康医疗等领域，充分论证，把准方向，明确重点，再部署一批体现国家战略意图的重大科技项目和工程。
2016.12	国务院	《“十三五”国家信息规划》	加强**量子通信**、未来网络、类脑计算、人工智能、全息显示、虚拟现实、大数据认知分析、新型非易失性存储、无人驾驶交通工具、区块链、基因编辑等新技术基础研发和前沿布局，构筑新赛道先发主导优势。加快构筑之智能穿戴设备、高级机器人、智能汽车等新兴智能终端产业体系和政策环境。
2016.12	信息部	《信息通信行业发展规划（2016-2020 年）》	发挥互联网企业创新主体地位和主导作用，以技术创新为突破，带动移动互联网、5G、云计算、大数据、物联网、虚拟现实、人工智能、3D 打印、量子通信等领域核心技术的研发和产业化。

2017.5	科技部、教育部、中国科学院、国家自然科学基金委员会	《“十三五”国家基础研究专项规划》	**量子通信研究面向多用户联网的量子通信关键技术和成套设备，率先突破量子保密通信技术，建设超远距离光纤量子通信网，开展星地量子通信系统研究，构建完整的空地一体广域量子通信网络体系，与经典通信网络实现无缝链接。**
2018.1	国务院	《国务院关于全面加强基础科学研究的若干意见》	拓展实施国家重大科技项目，加快实施量子通信与量子计算机、脑科学与类脑研究等“科技创新 2030——重大项目”，推动对其他重大基础前沿和占了必争领域的前瞻布局。
2018.7	中央办公厅、国务院办公厅	《金融和重要领域密码应用与创新发展工作规划（2018 年-2022 年）》	大力推动密码科技创新……促进**密码与量子技术**、云计算、大数据、物联网、人工智能、区块链等新兴技术融合创新。
2020.1	中央政治局	第二十四次集体学习	**量子科技**发展具有重大科学意义和战略价值，是意向对传统技术体系产生冲击，进行重构的重大颠覆性技术创新，将引领新一轮科技革命和产业变革方向。
2020.12	科技部	《长三角科技创新共同体建设发展规划》	聚焦**量子信息**、类脑芯片、物联网、第三代半导体、新一代人工智能、细胞与免疫治疗等领域，努力实现技术群体性突破，支撑相关新兴产业集群发展。
2021.3	全国人大	《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》	加快布局**量子通信**、神经芯片、DNA 存储等前沿技术，加强信息科学与生命科学、材料等基础学科的交叉创新，支持数字技术开源社区等创新联合体发展，完善开源知识产权和法律体系，鼓励企业开放软件源代码、硬件设计和应用程序。
2021.1	中共中央、国务院	《国家标准化发展纲要》	加强关键技术领域标准研究。在人工智能、**量子信息**、生物技术等领域，开展标准化研究。
2021.12	国务院	《“十四五”国家信息化规划》	加强人工智能、**量子信息**、集成电路、空天信息、类脑计算、神经芯片、DNA 存储、脑机接口、数字孪生、新型非易失性存储、硅基光电子、非硅基半导体等关键前沿领域的战略研究和技术融通创新。
2022.1	国务院	《“十四五”数字经济发展规划》	增强关键技术创新能力。瞄准传感器、**量子信息**、网络通信、集成电路、关键软件、大数据、人工智能、区块链、新材料等战略性前瞻性领域，发挥我国社会主义制度优势、新型举国体制优势、超大规模市场优势，提高数字技术基础研发能力。
2022.12	中共中央、国务院	《扩大内需战略规划纲要（2022-2035 年）》	以需求为导向，增强国家广域量子保密通信骨干网络服务能力。在人工智能、**量子信息**、脑科学等前沿领域实施一批前瞻性、战略性国家重大科技项目。
2023.3	国家发改委	《横琴鲁澳深度合作区鼓励类产业目录》	在科技研发与高端制造产业中，包括**量子通信**技术等新机理计算机系统开发等。
2024.1	工信部、教育部、科技部、交通运输部、文化和旅游局、国务院国资委、中国科学院	《关于推动未来产业创新发展的实施意见》	以实施意见为指南，围绕脑机接口、**量子信息**等专业领域制定专项政策文件，形成完备的未来产业政策体系，发挥行业协会等社会组织作用，推广先进的典型案例，营造推进未来产业发展的良好氛围。

资料来源：ICV《2024 量子通信与安全产业发展展望》，国投证券研究中心

1.3. 产业：四大研究领域共创新需求

量子信息技术通过对光子、电子和冷原子等微观粒子系统及其量子态进行精确的人工调控和观测，借助量子叠加和量子纠缠等独家物理现象，以经典理论无法实现的方式获取、传输和处理信息。**量子信息主要包括量子计算、量子通信、量子测量、抗量子密码四大研究领域**。

1）**量子计算：**基于量子力学的新型计算方式，利用量子叠加和纠缠等物理特性，以微观粒子构成的量子比特为基本单元，通过量子态的受控烟花实现计算处理。随着量子比特数量增加，量子计算算力可呈指数级规模拓展，理论上具有经典计算无法比拟的巨大信息携带和超强并行处理能力、以及攻克经典计算无解难题的巨大潜力。

2）**量子通信：**利用量子相干叠加、量子纠缠效应进行信息传输的一种新型通信技术，由量子论和信息论相结合而产生。从物理学角度看，量子通信是在物理极限原理下完成的高性能通信，从物理原理上确保通信的绝对安全，解决了通信技术无法解决的问题，是一种全新的通信方式。从信息学角度看，量子通信是利用量子不可克隆或者量子隐形传输等量子特性，借助量子测量的方法实现两地之间的信息数据传输。量子通信中传输的不是经典信息，而是量子态携带的量子信息，是未来通信技术的重要发展方向。

3）**量子测量：**以量子力学为基础理论的，采用粒子能级跃迁、量子纠缠、量子相干等技术原理对微观粒子，如原子、光子等量子态制备、测量和读取，实现对物理参数如磁场、频率、电场、时间、长度等物理参数的高准确度精密测量。量子精密测量能够消除宏观实物基准各种参数不稳定所产生的影响，在待测物理量上可以获得前所未有的测量准确度，可以获得比实物基准高几个数量级的稳定性和准确度。

4）**抗量子密码：**为了解决量子计算机对传统加密算法威胁的产物。其目标是设计新的密码学算法，能够在量子计算机的影响下依然保持高度安全性。这种新型密码学研究了在量子计算背景下仍然难解的数学难题，以及基于这些难题构建的新型加密算法。

图12. 量子科技产业分类

资料来源：Mckinsey《Quantum Technology Monitor》，国投证券研究中心

四大领域研究与应用探索发展迅速，前景可期。量子科技作为前沿科技领域，其研究与应用探索正以前所未有的速度发展，展现出广阔的前景。量子计算利用量子比特的叠加态和纠缠态进行计算，有望解决传统计算机难以处理的复杂问题，未来可能在药物发现、材料科学、优化问题等领域实现重大突破。量子通信利用量子纠缠和量子密钥分发实现安全、高效的信息传输，未来目标是构建全球性的量子互联网，实现绝对安全的信息传输。量子测量利用量子系统的超高灵敏度，能够进行精密测量，未来将在精密工程、时间标准、物理常数测定等方面发挥更加关键的作用。抗量子密码旨在开发新的加密算法，确保在量子计算机时代的信息安全，将成为网络安全的新基石。**总的来看，量子科技在多个细分领域都取得了显著进展，其发展速度和应用潜力表明，量子科技将成为未来科技革命和产业变革的重要驱动力。**

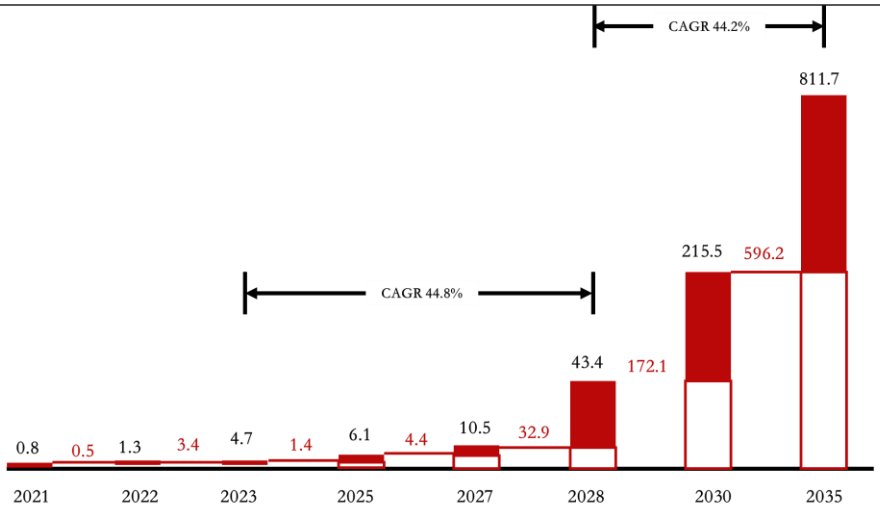
图13. 量子信息四大领域的原理特性，发展定位及应用场景

	量子计算	量子通信	量子测量	抗量子密码
原理特性	❑ **量子比特**为基本单元，利用量子叠加和干涉等原理实现并行计算，在某些计算困难问题上可能提供指数级加速。	❑ 利用量子**叠加态及纠缠效应**，在经典通信辅助下，进行量子态信息传输或密钥分配，具有无法被窃听的**信息论安全保证**。	❑ 基于对光子和冷原子等**微观粒子系统**的调控和观测，实现对时间、磁场、重力场等多种物理量信息的**超高精度测量**。	❑ 基于格基难题、多变量多项式难题和编码理论难题等复杂数学问题，构建加密算法，**确保加密信息在面对量子计算机的安全性。**
发展定位	➢ 为计算困难问题提供高效解决方案，实现突破经典计算极限的**算力飞跃**，量子计算与经典计算**长期并存，相辅相成**。	➢ 连接量子信息处理节点构成**量子信息网络**；量子密钥分发服务于**经典通信加密**，量子通信与经典通信**应用场景不同**。	➢ 实现物理量测量和信息获取的精度、分辨率、稳定度等性能指标**进一步提升**。经典测量到量子测量是**发展必然趋势**。	➢ 满足信息安全需求，确保在量子计算机成为通信威胁之前，能够拥有足够强大的加密工具保护数据安全。**传统加密算法到抗量子密码的发展是必然趋势。**
应用前景	• **~5年**：基于含噪声中等规模量子处理器（NISQ）和云平台探索具备实用化价值的应用算例。 • **远期**：大规模可编程容错量子计算机及其应用。	• **~5年**：量子信息网络关键技术突破，实验网络和标准体系建设；量子保密通信商用化探索。 • **远期**：量子通信与量子计算融合形成量子信息网络。	▪ **~5年**：新一代定位、导航和授时系统，微弱磁场和重力场测量系统，高灵敏度成像系统。 ▪ **远期**：小型化和商用化量子测量系统和量子传感器。	• **~5年**：政府机构和关键基础设施开始采用抗量子密码保护通信和数据。 • **远期**：结合量子密钥分发和其他量子技术，建立量子网络，提供绝对安全的通信渠道。

资料来源：信通院《量子信息技术发展与应用研究报告 2020》，国投证券研究中心

量子计算：2023 年产业规模达到 47 亿美元，预计 2035 年总市场规模有望达到 8117 亿美元。根据 ICV 的报告，2023 年全球量子计算产业规模达到 47 亿美元，2023 至 2028 年的年平均增长率（CAGR）达到 44.8%，有望实现高速增长。2027 年，专用量子计算机预计将实现性能突破，带动整体市场规模达到 105.4 亿美元。在 2028 年至 2035 年，市场规模将继续迅速扩大，受益于通用量子计算机的技术进步和专用量子计算机在特定领域的广泛应用，到 2035 年总市场规模有望达到 8117 亿美元。**我们认为量子计算作为新型的算力形态和模式，有望为社会带来颠覆式创新，创造出许多新的应用需求，从而打开新的广阔市场空间，是量子科技领域最值得关注的研发方向。**

图14. 全球量子计算产业规模（2021-2035）（单位：十亿美元）



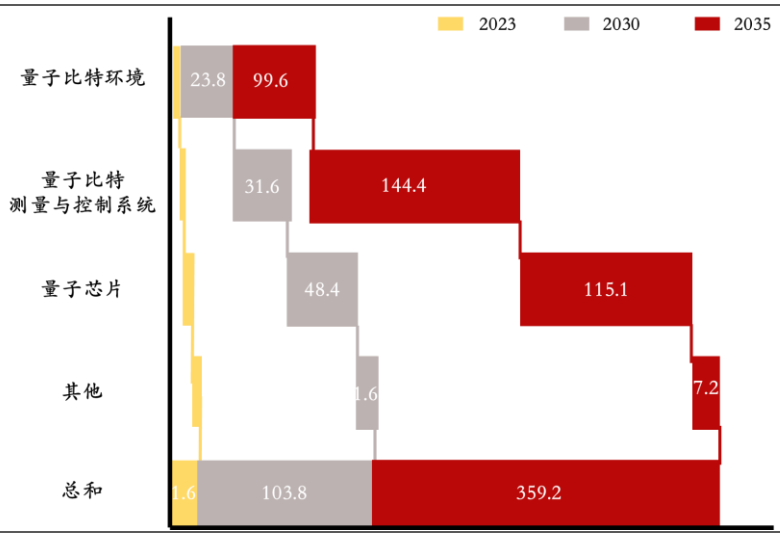
资料来源：ICV《2024 全球量子计算产业发展展望》，国投证券研究中心

量子计算：上游产业规模显著增长，预计 2035 年达千亿美元。从产业链来看，从 2023 年到 2035 年，上游市场规模呈现出显著的增长趋势，市场总规模由 2023 年不到 20 亿美元增长到 2035 年千亿美元。上游来看，**量子比特环境**市场规模的高速增长表明，在量子计算的演进中，提供稳定、可控的环境成为至关重要的因素。技术的不断进步推动了对量子比特环境的不断增加的需求，包括低温环境、低噪声等，因此投入在创造适宜的量子比特环境上不断增加。

与此同时，**量子比特测量与控制系统**市场规模增长有望实现较快增长，预计从 2023 年的几亿美元到 2030 年的 316 亿美元，最后增长到 2035 年的 1444 亿美元，跨越了 3 个数量级。测量和控制系统对于保持量子比特的相干性和实现量子计算任务至关重要，而技术的发展推动了对更为精密、高效的测量和控制系统的持续需求增加，带来庞大的市场需求。

同样，**量子芯片**市场规模到 2030 年以及 2035 年均有指数级别的增长。量子芯片作为量子计算的核心组件，对实现量子计算任务具有至关重要的作用。随着对量子计算性能要求的提高，对更先进、可扩展的量子芯片的需求持续上升，推动了市场规模的显著增长。

图15. 全球量子计算上游产业规模（2030&2035）（单位：十亿美元）

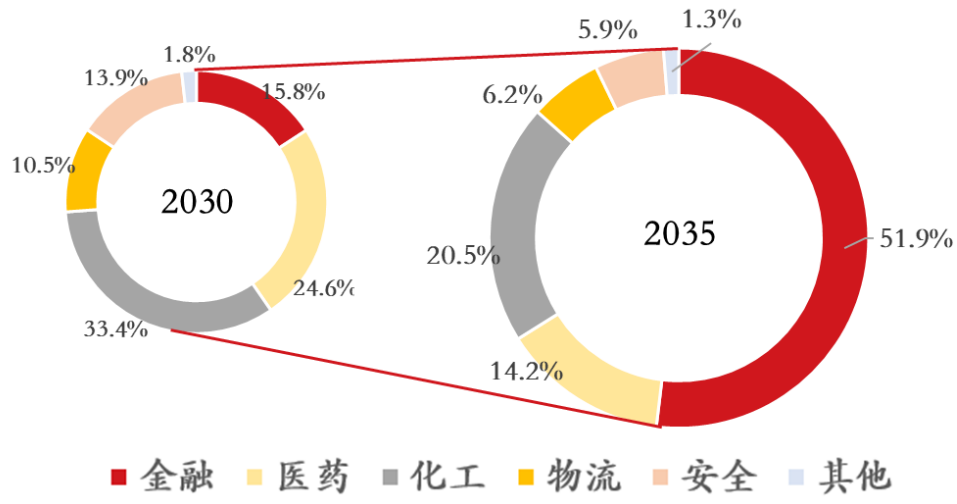


资料来源：ICV《2024 全球量子计算产业发展展望》，国投证券研究中心

量子计算：多种下游应用并驾齐驱，金融行业需求旺盛。从下游应用来看，根据 ICV 的报告，2035 年金融领域的应用市场份额有望达到 51.90%，主要源于金融行业对量子计算技术的深刻认可，特别是在风险管理、投资组合优化等方面的应用。量子计算的强大计算能力赋予其在解决金融难题上的优越性能，这使得金融领域有望对量子计算需求快速上升，市场份额得以快速扩大。

排名二至五的应用方向还包括医药、化工、物流和安全等。此外，**人工智能、量超融合、机群架构等因素同样对市场产生了深刻影响。**金融、医药等行业在人工智能算法的发展中寻求更强大的计算能力，而量子计算的崛起为其提供了更为强大的计算工具，有望部分替代传统的计算机方案，从而在市场格局中产生了深远的变革。这一多元因素的综合影响使得全球量子计算市场将在 2035 年呈现出多层次的发展格局。

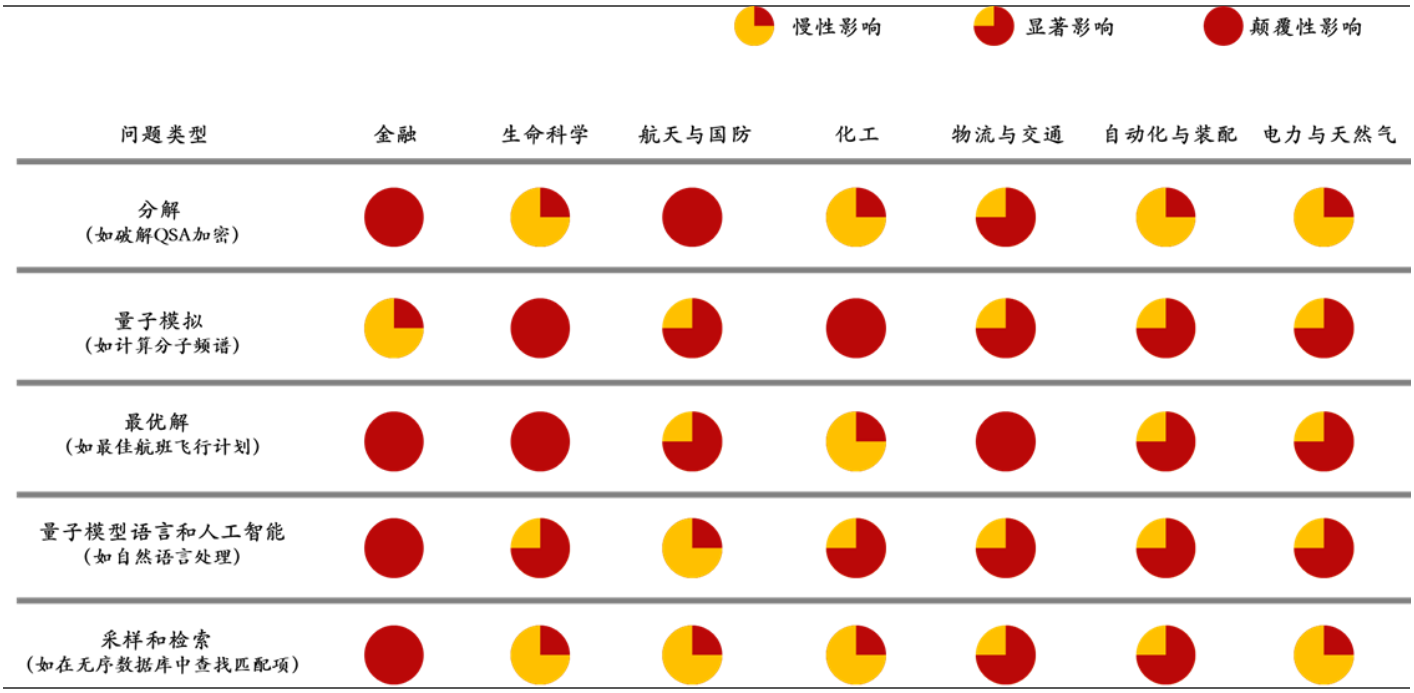
图16. 全球量子计算下游应用占比



资料来源：ICV《2024 全球量子计算产业发展展望》，国投证券研究中心

量子计算：对解决多种问题具颠覆式影响，金融与生命科学有望成为最具价值下游应用。从金融、生命科学、航天与国防、化工、交通物流、自动化与装配、电气与天然气这七大潜在的量子计算下游应用场景来看，量子计算技术对金融行业在分解问题、最优求解问题、量子模拟语言和人工智能、采样与检索等多个问题类型表现出了颠覆性的影响，同时量子计算技术对生命科学领域的量子模拟和最优求解问题上也表现出了颠覆性的影响。因此，从长远来看，金融和生命科学领域有望成为最具价值的量子计算领域下游应用场景。

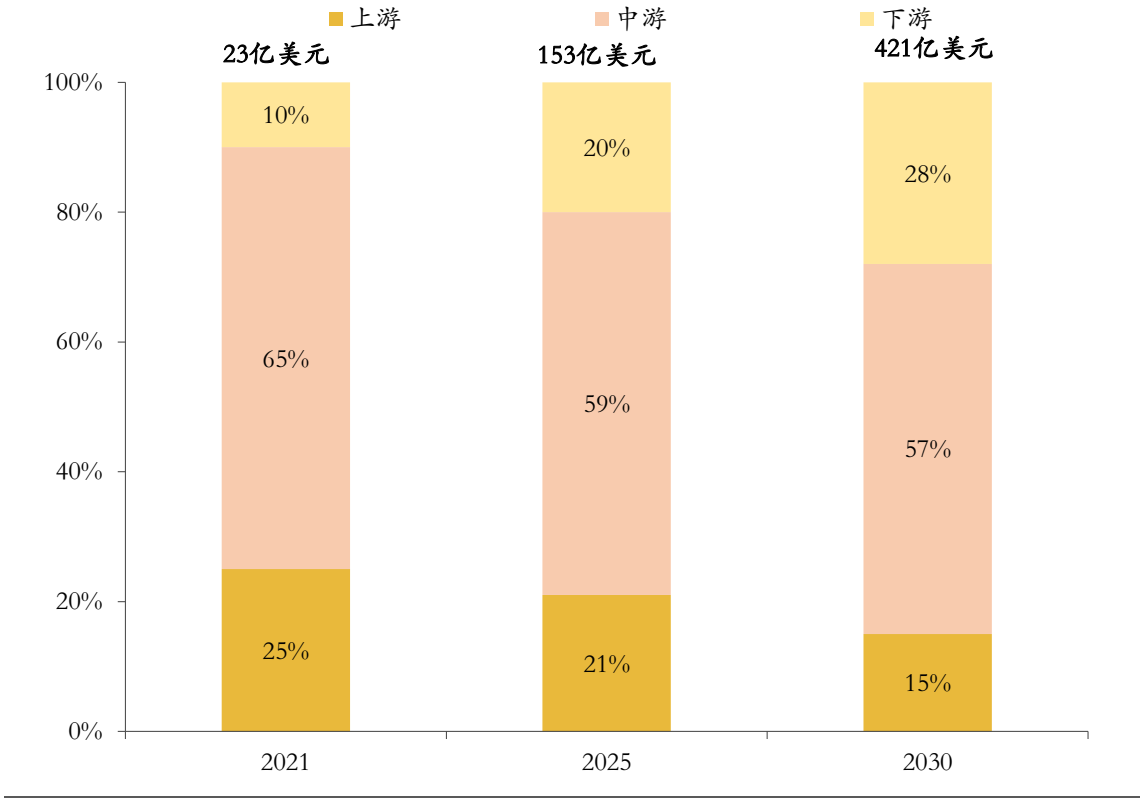
图17. 全球量子计算下游应用未来价值展望



资料来源：Mckinsey《Quantum Technology Monitor 2023》，国投证券研究中心

量子通信：产业规模预计超百亿，主要聚焦于中游设备。根据 ICV 预测，2021 年，全球量子通信市场规模约为 23 亿美元，预计到 2025 年增长到 153 亿美元，到 2030 年，增长到 421 亿美元。从产业链来看，量子通信市场规模集中度主要聚焦于中游。

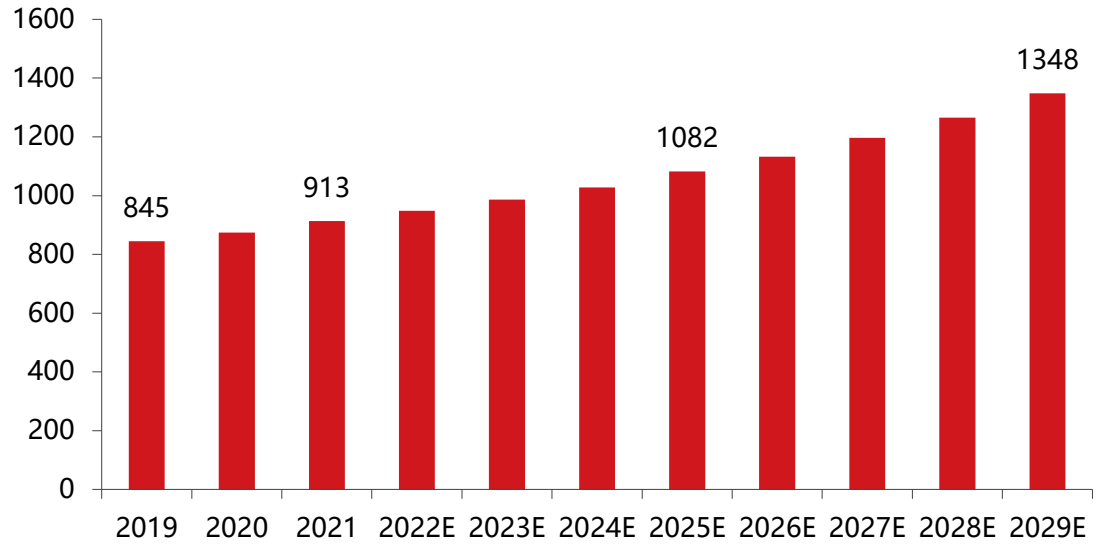
图18. 全球量子通信市场规模预测（2021-2030）



资料来源：ICV《2022 年全球量子通信产业发展报告》，国投证券研究中心

量子测量：市场规模稳步增长，未来规模有望超十亿美元。根据 ICV 预测，2022 年全球量子精密测量市场规模约为 9.5 亿美元，预计到 2029 年，市场规模增长到 13.48 亿美元，2022-2029 年复合增长率约为 5.1%。

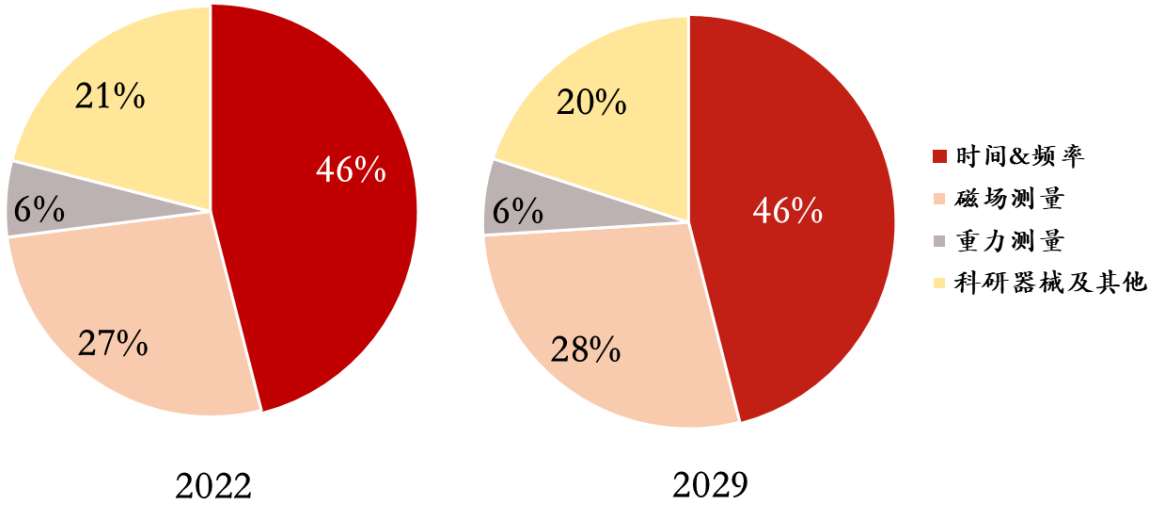
图19. 全球量子精密测量市场规模预测（2019-2029E）（单位：百万美元）



资料来源：ICV《2022 年全球量子通信产业发展报告》，国投证券研究中心

量子测量：重点应用聚焦四大领域，近半为时间与频率的测量需求。根据 ICV 报告，2022 年，量子时钟市场规模约为 4.4 亿美元，占比最高（46.3%），2022-2029 年复合增长率约为 4.9%；其次为量子磁测量，市场规模约为 2.5 亿美元，2022-2029 年复合增长率为 6.2%；然后为量子科研和工业仪器，市场规模约为 2 亿美元，2022-2029 年复合增长率约为 4.4%；最后为量子重力测量，市场规模约为 0.6 亿美元，2022-2029 年复合增长率约为 5.4%。

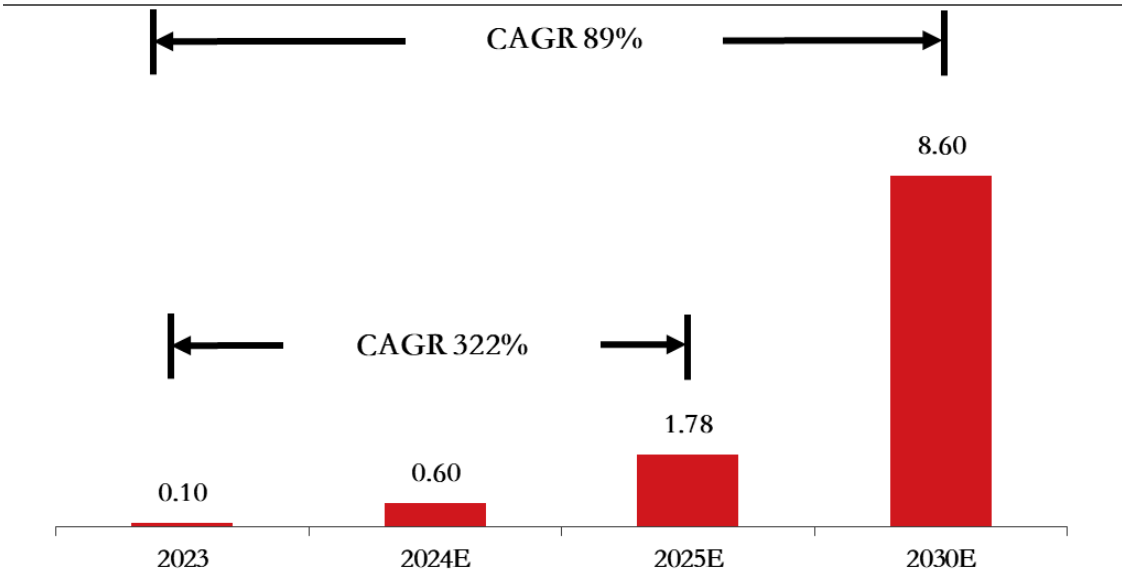
图20. 全球量子精密测量市场份额预测（按产品技术领域划分）



资料来源：ICV《2022 年量子测量产业发展报告》，国投证券研究中心

抗量子密码：产业处于初期阶段，未来有望加速发展。PQC 市场增长与 PQC 标准化进程及量子计算机的实用化有较大关联。2023 年，PQC 产业规模仍处在初期成长阶段，约为 1 亿美元。根据 NIST 的 PQC 标准化工作预计完成的时间点来估计，预计 2024 年后，行业将加速发展，到 2030 年，全球 PQC 产业规模将达到 86 亿美元。

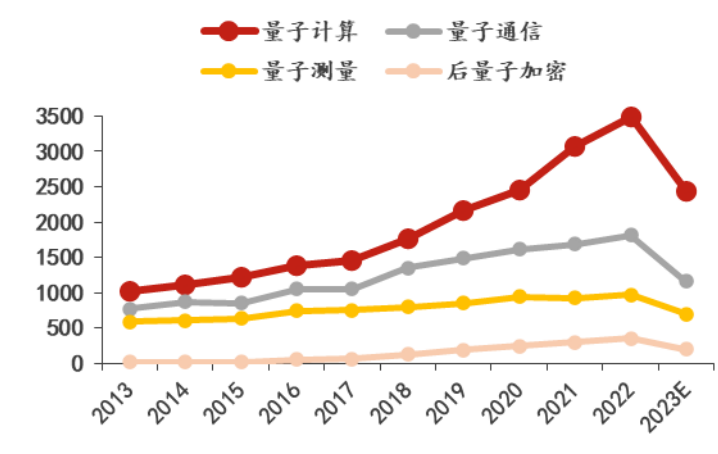
图21. 全球抗量子密码产业规模预测（2023-2030E，单位：十亿美元）



资料来源：ICV《2024 量子通信与安全产业发展展望》，国投证券研究中心

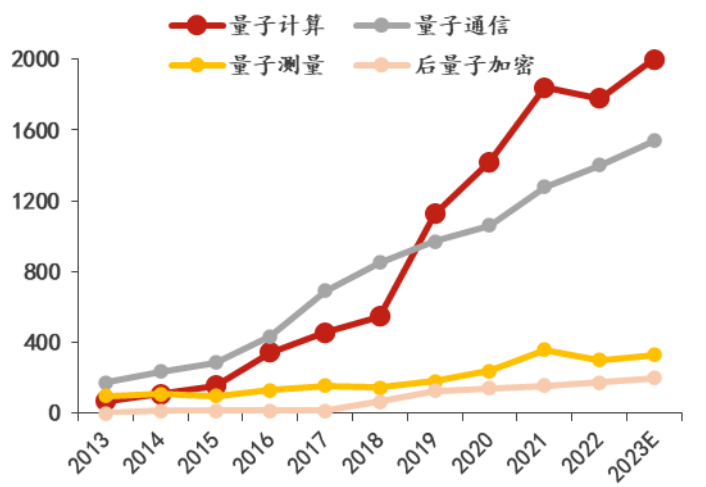
论文和专利分析：量子信息四大领域科研技术创新持续活跃。近十年，量子信息科学研究和技术创新保持快速发展趋势，量子计算、量子通信、量子测量、后量子加密等领域科研论文和专利申请数量逐年递增。论文方面，量子计算是最大热点，论文数量增速明显加快，近年来超过其他领域总和，量子通信和量子测量保持平稳增长，PQC 从 2016 年起逐步成为研究热点，2023 年有 340 余篇相关论文。专利方面，量子通信专利的增长趋势较为稳定，量子计算专利申请在 2019 年超过量子通信并持续保持快速增长，PQC 专利近年来快速增长，2023 年数量预计将达到 200 项。

图22. 全球量子信息科研论文数量年度变化趋势



资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

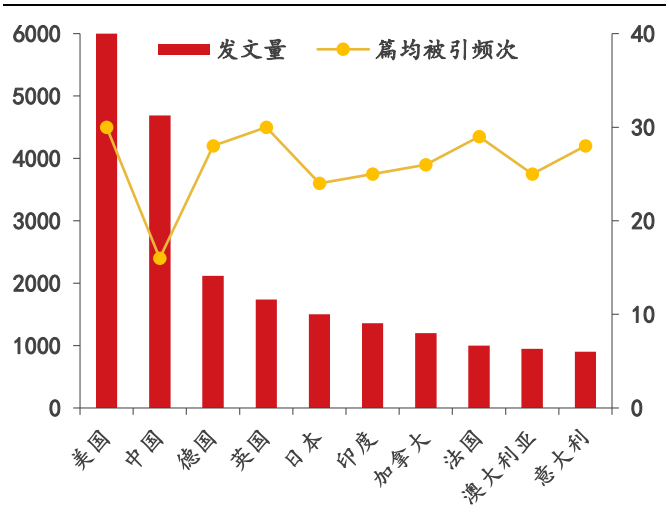
图23. 全球量子信息专利申请数量年度变化趋势



资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

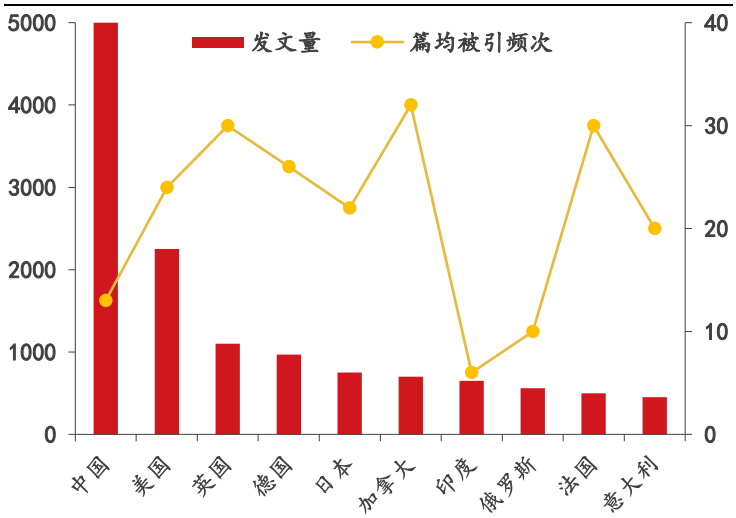
论文和专利分析：中美位于技术研发前列，我国量子通信领域研发实力领先。分国家来看，在量子信息各领域科研论文数量前十位中，中美占据前两位，在科研输出方面表现突出，量子通信我国论文数量远超其他国家；但从论文被引频次来看，我国与欧美相比仍有一定差距，高水平论文数量有待提升。

图24. 量子计算领域科研论文数量前十位国家情况



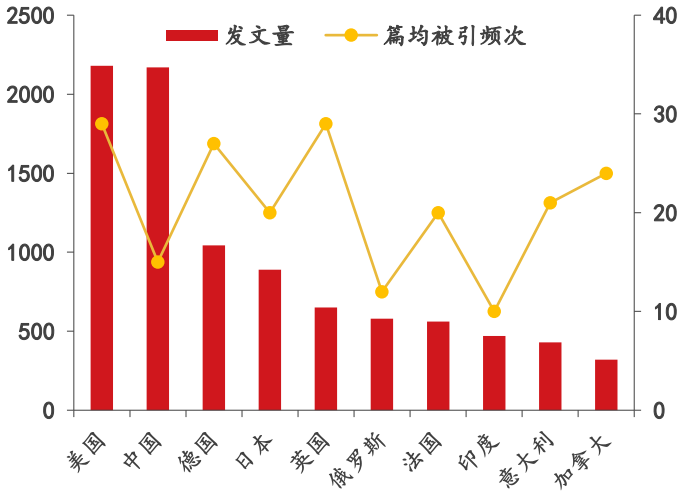
资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

图25. 量子通信领域科研论文数量前十位国家情况



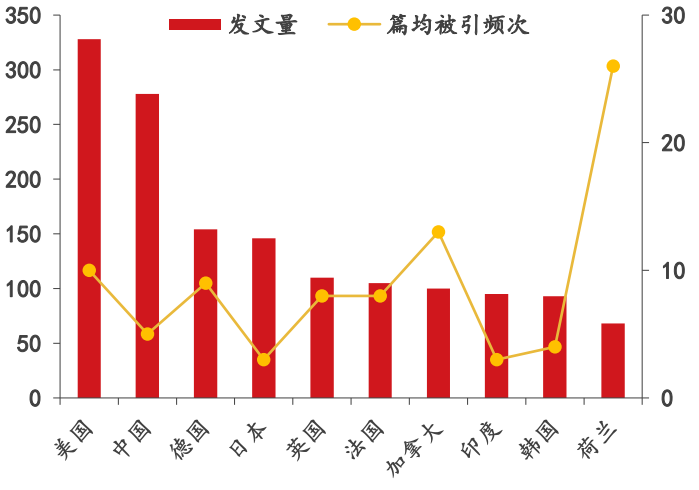
资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

图26. 量子测量领域科研论文数量前十位国家情况



资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

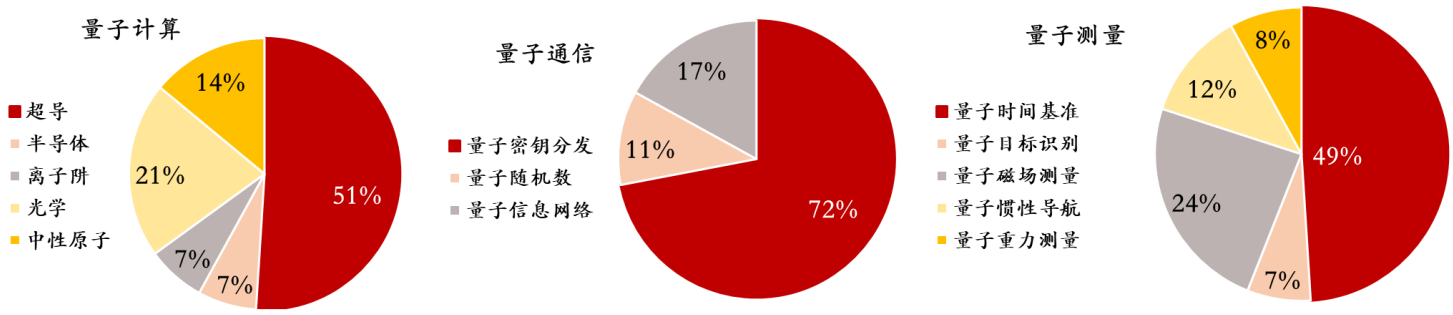
图27. 后量子加密领域科研论文数量前十位国家情况



资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

论文和专利分析：超导路线为量子计算主流方案，量子密钥分发为目前量子通信主流方案。从技术方向上看，在量子计算硬件技术路线中，超导路线专利数量占比超过 50%，光量子和中性原子路线技术创新热度高于离子阱和硅半导体；量子通信领域中，量子密钥分发技术专利占比超过 70%，器件、设备等系统研发类专利数量众多，量子信息网络技术成熟度不足，相关专利尚未大量涌现；量子测量领域中，以原子钟为代表的时频基准方向专利占比接近 50%，是技术创新与应用主力，磁场测量和惯性测量方向也有较多创新成果积累。

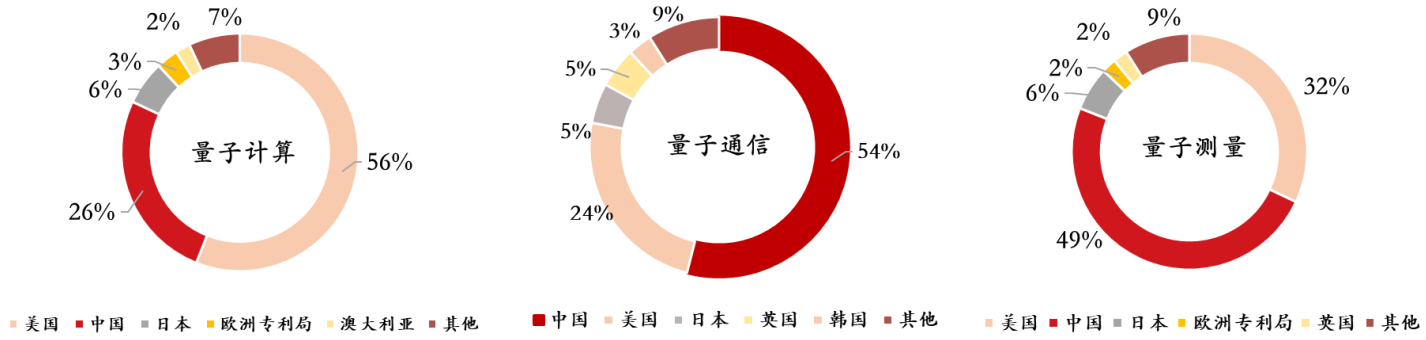
图28. 量子信息领域不同技术方向专利数量对比



资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

论文和专利分析：中美均处于量子科技领先水平，在不同领域各具优势。全球各国量子信息领域的专利申请占比情况来看，**量子计算领域，**美国技术创新活跃，专利申请占比达到 56%，中国位居第二，专利申请数量占比达到 26%；**在量子通信和量子测量领域，**中国专利申请数量均处于全球领先，占比分别为 24%和 32%。

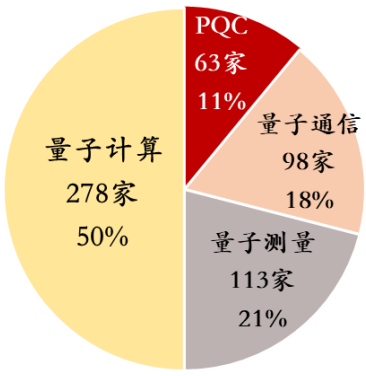
图29. 量子信息三大领域各国专利申请占比情况（截至 2022 年 9 月）



资料来源：信通院《量子信息技术发展与应用 2022》，国投证券研究中心

企业分析：量子科技企业数量持续增多，支撑未来产业化落地。根据信通院的报告，截至 2023 年 9 月，四大研发领域的全球相关科技企业、初创公司、行业应用企业等共 552 家，其中量子计算相关企业 278 家，占比超过 50%，凸显出量子计算是全球技术产业竞争的关注焦点。全球量子测量和量子通信企业数量均在百家左右，占比约为 20%。随着 PQC 算法评选和标准制定进程的逐步明朗，PQC 相关企业数量达到 63 家。

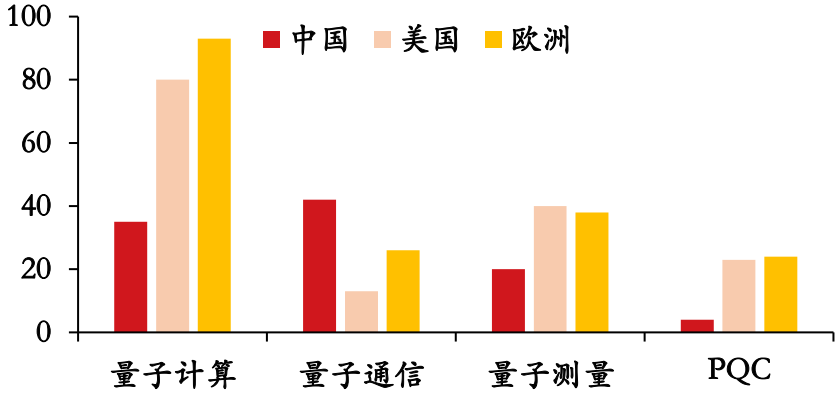
图30. 量子信息全球企业



资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

企业分析：量子计算企业聚集欧美，量子通信企业国内占优。从不同领域看，**量子计算领域，**欧美地区企业聚集度最高，共有 175 家，全球占比超过 60%，反映出美国和欧洲是量子计算产业生态活跃地区，中国量子计算领域相关企业共有 35 家，不及美国一半。**量子通信领域，**中国企业数量最多，共有 42 家，美国仅有 13 家，欧洲有 27 家，侧面反映出不同国家和地区在量子通信领域，主要是进入初步实用化阶段的量子密钥分发和量子保密通信的投资和推动力度差异。**量子测量领域，**欧美企业数量最多，共有 80 家，全球占比超过 60%，中国量子测量相关企业共 22 家，约为美国的一半。PQC 领域欧美平分秋色，共有相关企业 47 家，中国 PQC 企业数量仅 4 家，数量差距明显，未来 PQC 产业中国仍有待进一步发力。

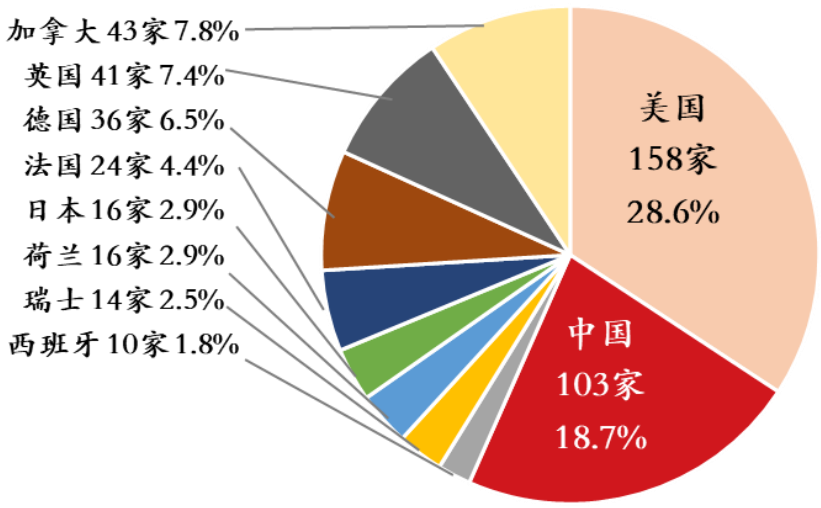
图31. 量子信息各领域企业数量



资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

企业分析：从具体企业的国籍分布来看，美国共有 158 家量子信息相关企业，全球占比超过四分之一。其中，谷歌、IBM、英特尔等科技企业已经成为量子计算领域业界标杆，IonQ、Quantinuum、PsiQ、AOSense 等初创企业创新驱动能力突出，在量子信息技术产业中拥有较为明显的先发优势。中国量子信息相关企业共 103 家。全球量子信息领域企业数量较多的国家还有加拿大、英国、德国、法国、日本、荷兰等，在未来技术产业发展中也拥有较强竞争力。

图32. 量子信息企业国家分布情况



资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

企业分析：产业链逐渐成型，依托产业联盟推动发展。量子计算目前仍处于应用和产业探索的初期，但气象、金融、石油化工、材料科学、生物医学、航空航天、汽车交通、图像识别等众多行业已开始关注和重视到其中的巨大发展潜力，开始于科技企业和初创企业合作探索，生态链不断壮大。其中，不同类型的产业联盟在量子计算生态建设中起到了巨大的推动作用。IBM 发起 Q Network 联盟，全球超过 100 家组织、160 个国家、20 万名用户使用其量子计算云服务，探索在人工智能、金融、智慧交通、生物医药、航天航空等的应用。微软成立“微软量子网络”和“西北量子联盟”，成员包括数十家企业及研究机构。加拿大成立了量子产业部（QIC），聚集了量子领域的 24 家公司，向全球的量子技术生态系统、人才和投资者宣传加拿大的量子准备，同时在省政府和联邦政府合作，从战略上支持量子技术之一新兴产业的发展。在产业配套设施设备供应链方面，精密机械、低温平台、真空室、微波器件、光学组件及系统等产业基础配套不断完善，既有 Janis Research 等老牌企业提供已有工业基础平台的共享，也有 ColdQuanta、Qblox 和 Quantum Microwave 当新兴企业推动助力发展。**目前，全球已有百余家量子计算初创企业，地域分布以美国、欧洲和加拿大最为密集，覆盖量子计算技术栈的各个层级。**

国际方面，国际科技巨头在量子计算领域竞争激烈，是推动量子计算技术与应用加速发展的主要动力。IBM、Google、Microsoft、Intel、Honeywell、Amazon 等美国科技巨头均已进军量子计算领域，具备资金投入雄厚、工程技术成熟、软件能力突出、云计算资源丰富等优势，开展包括量子计算硬件、软件算法、云服务及应用服务在内的全套研发。

国内方面，中国量子科技企业的发展格局主要由运营商、国盾量子、本源量子、研究院所和高校构成。其中，运营商在量子通信领域发挥着重要作用，积极推动量子密钥分发等技术的应用和发展；国盾量子作为国内量子通信领域的领军企业，不断突破关键技术，为我国量子通信产业提供有力支撑；本源量子则在量子计算机领域进行前瞻布局，在量子处理器硬件、开源软件平台和量子计算云服务等方面进行探索。此外，各大研究院所和高校在量子科技研究方面取得了一系列重要进展，为我国量子科技的发展提供了源源不断的创新动力。**总体来看，我国量子科技企业格局呈现出多元化、协同发展的良好态势。**

图33. 量子计算领域科技公司和初创企业分布

资料来源：GQI 量子计算报告，国投证券研究中心

投融资：事件及金额双增长，量子信息产业厂商不断孵化。从投融资事件数量来看，根据信通院的报告，2017 年起企业投融资事件数量开始出现明显增长，与企业数量爆发式增长的时间趋势吻合。大量初创企业获得政府的赠与投资(Grant)和不同轮次的股权融资等风险投资。美国 DOE、NSF 和国防部（DOD）等政府部门的合同赠予投资占比较高，从 2018 年开始，每年都有约 20 笔赠予，占全部投融资数量 20%左右。风险投资中，种子轮和 A 轮占比最高，合计每年约占整体投融资事件数量的 40%~50%，孵化器数量也在逐渐增加。可以看出，资本市场对量子信息领域关注度持续提升，但大多数企业仍处于早期投资阶段。

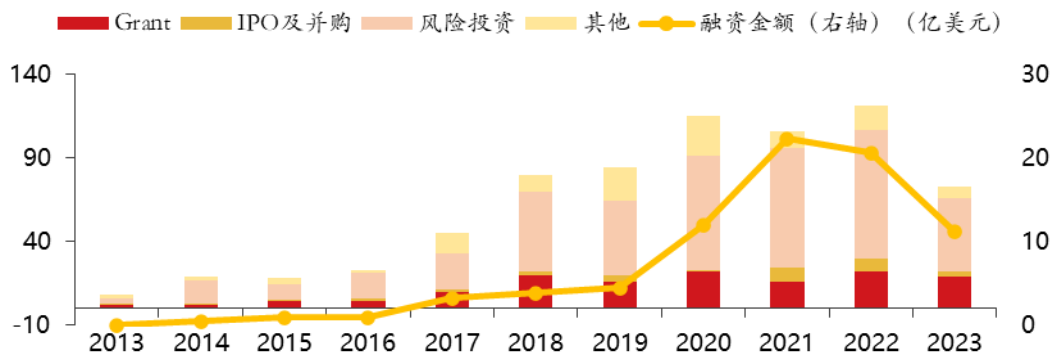
表9：全球量子信息初创企业十大融资事件（金额降序）

公司	国家	技术领域	融资额（亿美元）	时间
SandboxAQ	美国	量子软件/PQC	5.00	2022
PsiQuantum	美国	量子计算	4.50	2021
IonQ	美国	量子计算	3.50	2021
Regetti Computing	美国	量子计算	3.45	2022
Arqit	英国	量子通信	3.45	2021
IonQ	美国	量子计算	3.00	2021
Quantinuum	英国	量子计算	3.00	2021
D-Wave Systems	加拿大	量子计算	3.00	2022
PsiQuantum	美国	量子计算	2.30	2020
本源量子	中国	量子计算	1.45	2022

资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

从投融资金额规模看，过去 5 年资本市场对量子信息领域企业的投资同样经历了一轮爆发式增长，2021 年和 2022 年均超过 20 亿元量级，超过过去十年总和。近两年来，量子信息初创企业获得的投融资数量和金额开始出现一定回落，一方面是全球疫情、经济衰退和美元加息等宏观层面影响，另一方面也有量子计算等初创企业技术产品和投资收益未达市场预期等具体原因。

图34. 量子信息领域企业投融资事件数量与金额变化趋势



资料来源：信通院《量子信息技术发展与应用 2023》，国投证券研究中心

2. 量子计算：算力产业的颠覆式创新，未来科技的锋利之矛

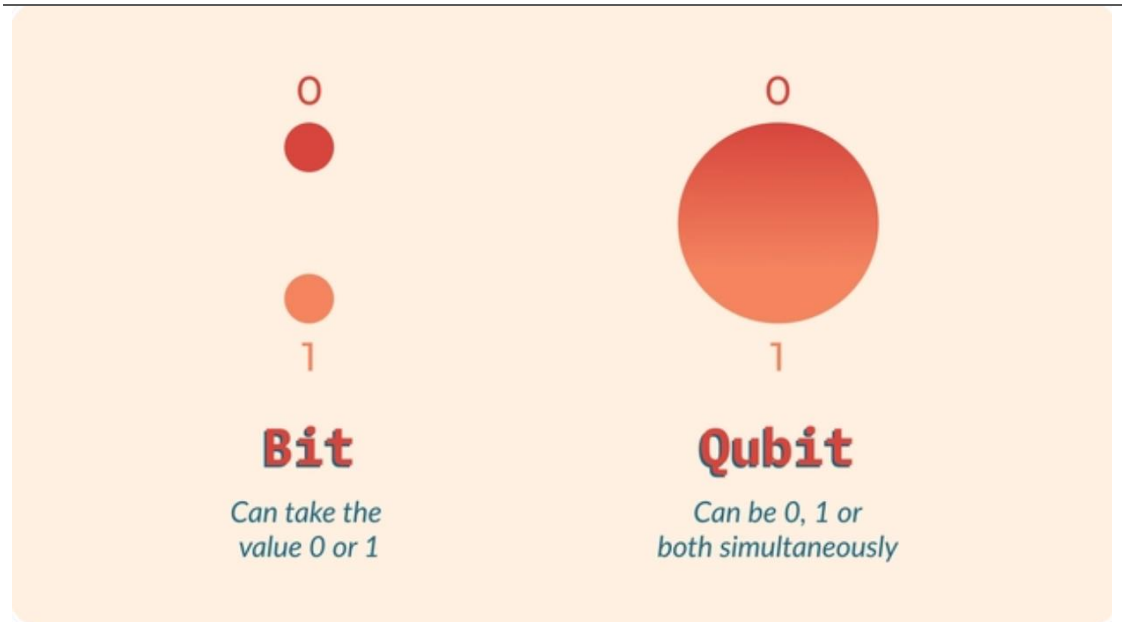
2.1. 量子计算原理：量子比特实现量子优越性

量子比特利用量子叠加态原理实现处理信息量的指数级增长。经典计算机中最基本的单位被称为经典比特，经典比特拥有两种互斥状态“0”，“1”，在任意时刻只能处于其中任一状态。与之对应的量子计算机中基本单位被称为量子比特（quantum bit），它可以处于由两个基态|0>，|1>线性组合的任意叠加态。量子计算利用量子叠加与纠缠性质，其优势体现在量子并行性与本身的可逆过程中。

量子并行性提供了量子计算巨大的计算潜力。当 N 个比特参与运算时，经典计算机参与运算的信息为 2^N 个信息中的一个，量子计算时由于量子叠加性原理,其参与运算的态可以为 2^N 个。即经典计算处理信息的能力随着 N 的增加是线性增长的，量子计算随着 N 的增加处理能力是指数增长的。

量子计算可逆过程代表量子计算过程随着比特数目和门数目的增加不会产生像经典计算发热的问题。逻辑不可逆的过程对应着物理态自由度减少的过程，必然导致能量耗散。经典计算的很多门操作是逻辑不可逆过程，比如与非门，异或门等。在计算过程中必然带来计算信息自由度的减小，也就带来发热问题。随着计算力的增加，散热问题也是现在经典计算机不得不面对的问题。因为量子计算的门操作都是量子力学中的厄密操作其都是可逆的，所以理论上计算的过程不会产生发热问题。

图35. 经典比特和量子比特的区别



资料来源：《Quantum computation and quantum information. Cambridge University Press》，国投证券研究中心

单个量子比特可以直观的由布洛赫球面上的一个向量来表征。布洛赫球模型最初是由德国理论物理学家费里·布洛赫（Felix Bloch）在 1929 年提出来的。布洛赫球是一种用于描述量子比特（quantum bit，或简称 qubit）状态的图形化工具。在布洛赫球上，两个计算基态分别位于球面的北极点和南极点，而一个单量子比特的状态可以用一个点表示，这个点的位置和方向对应着量子比特的状态。

图36. 用布洛赫球表示的量子比特

单量子态:

$$|\psi\rangle = \cos(\theta)|0\rangle + \sin(\theta)\, e^{i\varphi}\,|1\rangle$$

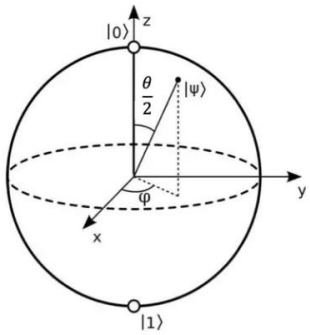
由于半角问题，上述单量子态公式调整为：

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right) e^{i\varphi}\,|1\rangle$$

其中：

$$0 \le \theta \le \pi\ ,\ 0 \le \varphi \le 2\pi$$

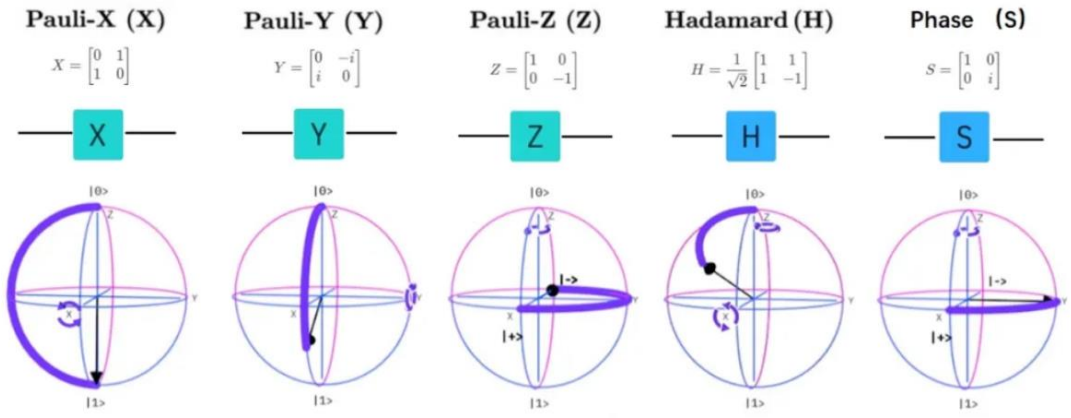
$$x = \sin\frac{\theta}{2}\cos\varphi$$
$$y = \sin\frac{\theta}{2}\sin\varphi$$
$$z = \cos\frac{\theta}{2}$$



资料来源：Qubits.top，国投证券研究中心

量子逻辑门通过操控量子比特的状态，实现通用逻辑门运算。经典计算中有许多逻辑门：例如与门、或门、非门、与非门、或非门等等。每一种逻辑门完成一项简单的逻辑运算，但是它们的各种组合，便能够完成各种复杂的计算。量子计算中也有各种“量子逻辑门”，与经典逻辑门相对应。量子逻辑门的作用是将 Qubit 从一个状态变成另一个状态。可以用 2 维矩阵代数的语言来描述叠加态（Qubit）的变化。量子比特是布洛赫球面上一个矢量，Qubit 状态的演化，就是布洛赫球面上矢量的旋转。旋转是由用幺正（酉）矩阵表示的“量子逻辑门”引起的。矩阵（量子门）作用在矢量上，将 Qubit 的状态变成新的状态。许多量子门连在一起，量子计算便如此一步一步进行下去。所有 Qubit 的最后状态，便是计算得到的最后结果。

图37. 几种量子逻辑门的矩阵和布洛赫球表示

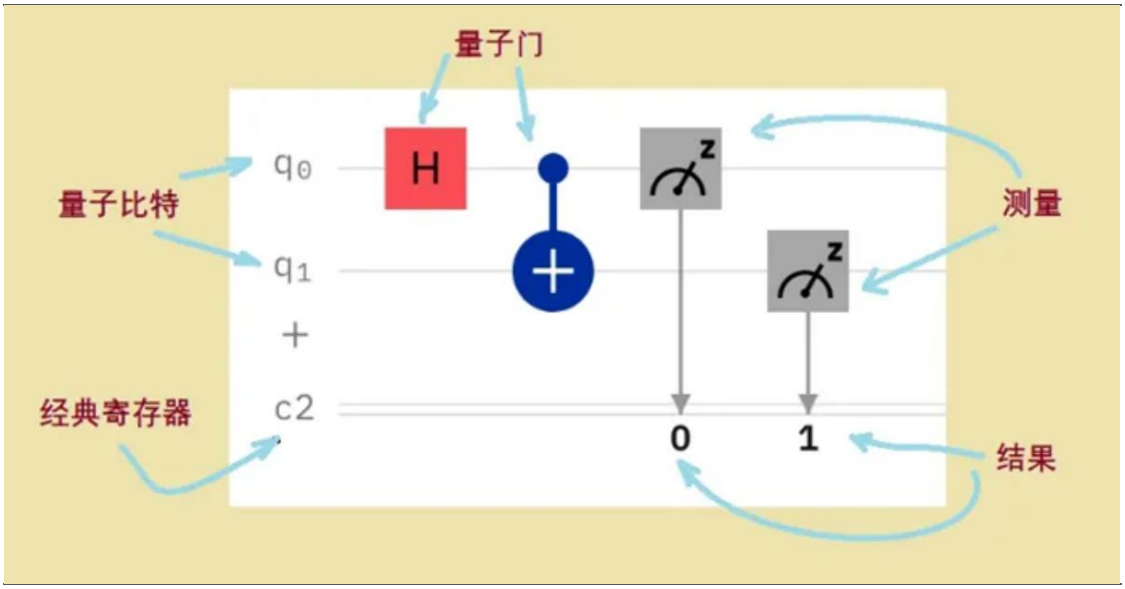


资料来源：墨子沙龙，国投证券研究中心

例如，最简单的量子门是量子非门（上图最左边的 X 门），类似于经典非门，实现 0、1 互换，量子非门实现$|0\rangle \rightarrow |1\rangle$或$|1\rangle \rightarrow |0\rangle$，另一个重要的量子门是 H 门（Hadamard 门），它的作用是使基态变成叠加态：$|0\rangle \rightarrow \alpha|0\rangle + \beta|1\rangle$，这样才有可能进行量子计算。除此之外，还有双比特的逻辑门如受控非门（CNOT 门）、三比特的逻辑门如托佛利门（CCNOT 门）等等。

量子比特和量子逻辑门组成量子逻辑电路。量子电路是用于量子计算的模型，是执行量子位状态的传送之路，但量子电路图只是貌似经典的电路图，实际上完全不同于传统电路，例如：实线并不一定是物理电缆。量子电路的目的只是定义事件的时间顺序：水平轴是时间，左边开始右边结束。量子门的时间顺序会对量子位的最终状态产生重大影响。类似经典电路，计算是一系列的量子门，但测量是经典电路没有的量子操作。多个量子电路结合，就构成了量子计算机，可以实现通用计算。

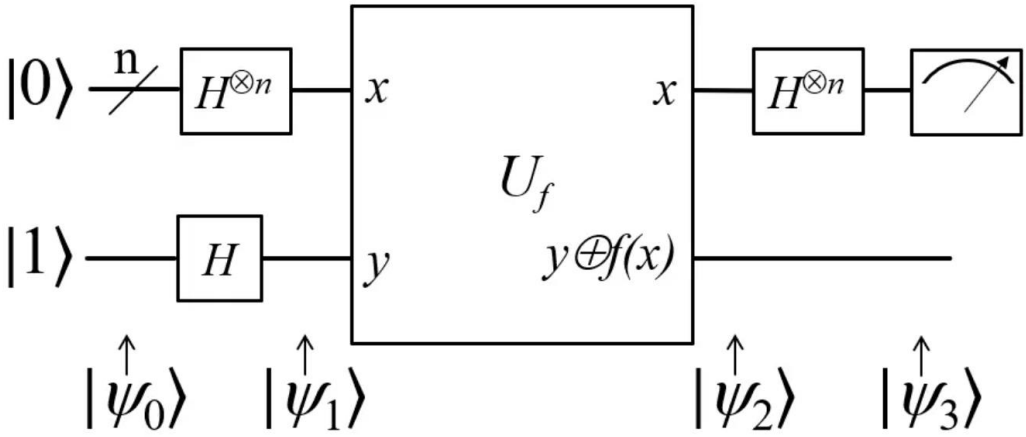
图38. 简单的量子电路实例



资料来源：墨子沙龙，国投证券研究中心

接下来我们以 Deutsch-Jozsa 算法为例，来看一下量子计算在特定算法场景下的优越性。Deutsch 算法主要想解决以下的数学问题：x 是由 0 或 1 组成的任意 n 位二进制数（例如 n=3 的 011，n=7 的 1010011 等），f(x)是一个常值函数（f(x)=0 或者 f(x)=1）或者是一个平衡函数（50%情况 f(x)=0，50%情况 f(x)=1），如何进行最少次数的计算，来确定 f(x)是常值函数还是平衡函数。**经典计算机情况下**，n 位二进制最多表示 2^n 个数字，因为需要尝试(2^n)/2+1 次计算，才能在比 50%多一次的情况下，判断函数 f(x) 是常值函数还是平衡函数。而**量子计算机下**，只需要做一次尝试，就可以做出准确判断，为此我们需要构建以下的量子逻辑门电路：

图39. Deutsch-Jozsa 算法的量子电路



资料来源：《Deutsch-Jozsa algorithm's quantum circuit》，国投证券研究中心

在这个量子线路中，H 门先把低位的 n 个量子比特 $|0\rangle^{\otimes n}$ 演化为了 $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n}=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$，这样所有可能的态 $|x\rangle, x=0\ldots0,0\ldots1,\ldots1\ldots1$ 就叠加在一起了。

最高位量子比特把|1>演化为 $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$，和低位的 n 个量子比特一起，得到：

$$|\psi_1\rangle=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

将其进入 U_f 矩阵进行运算。按照 U_f 矩阵的运算规则，如果 $f(x)=0$，则高位量子态不变，如果 $f(x)=1$，则高位量子态取反，演化为 $\frac{|1\rangle-|0\rangle}{\sqrt{2}}$。综合而言，最高位量子态在经过 U_f 之后会演化为 $(-1)^{f(x)}\frac{|0\rangle-|1\rangle}{\sqrt{2}}$，而低位的 n 个量子比特保持不变，因此得到：

$$|\psi_2\rangle=(-1)^{f(x)}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\otimes\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\frac{|0\rangle-|1\rangle}{\sqrt{2}}|x\rangle$$

对该量子态低处的 n 位做 H 门操作，也就是除了最高位以外，其他位的|0>要演化为 $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$，|1>要演化为 $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$。对于任意|0>和|1>张成的|x>，每一位都经过 H 门之后，会变成 $\frac{|0\rangle\pm|1\rangle}{\sqrt{2}}\otimes\frac{|0\rangle\pm|1\rangle}{\sqrt{2}}\otimes\ldots\frac{|0\rangle\pm|1\rangle}{\sqrt{2}}=\frac{1}{\sqrt{2^n}}\sum_{z=0}^{2^n-1}(-1)^{x\cdot z}|z\rangle$，其中 $x\cdot z$ 代表两个二进制数按位与。从上式可以看出，只有当 x,z 同时取 1 的时候，才会有一个-1 的系数。因此，最后 n+1 个量子比特的量子态表示为：

$$|\psi_3\rangle=\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{z=0}^{2^n-1}(-1)^{x\cdot z+f(x)}\frac{|0\rangle-|1\rangle}{\sqrt{2}}|z\rangle$$

接下来只要对低位的 n 个量子比特进行测量，如果 $f(x)=a,(a=0,1)$ 是常值函数，则全 0 量子态|00…0>的系数为 $\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{0\ldots0+f(x)}=(-1)^a$，无论 a 取 0 还是 1，系数的平方为 1，即对 n 为量子比特的测量，最后会坍缩为 100%的测出量子态|00…0>。如果 $f(x)$ 是平衡函数，量子态|00…0>的系数会由于 $f(x)$ 取 0 和 1 的等可能性而互相抵消，从而振幅平方为 0，即不可能测出|00…0>这个量子态。

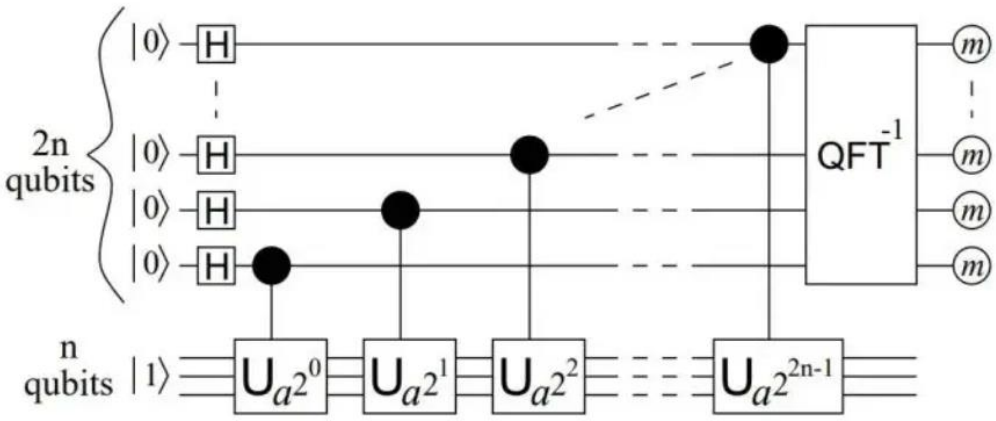
因此，我们只需要测量低位量子态是否为全 0 的|00…0>，若是则为常值函数，若不是则为平衡函数，从而**通过 1 次函数运算，实现经典计算机 2^n 运算，实现量子计算机指数级加速**。

Shor 算力利用量子纠缠和干涉的原理，实现对密码破解的指数级加速。另一种具备量子计算优越性的算法，就是 1994 年由 Peter Shor 提出的 Shor 算法。Shor 算法主要用于解决找出一个给定整数 N 的质因数的问题即整数分解问题，通过量子计算机实现 Shor 算法，可以将整数的质因数分解问题计算复杂度，从经典计算机的$O(n^n)$下降到$O(n)$，实现指数级加速。

Shor 算法所解决的问题为设一个很大的奇数 N，N 为两个质数 n1 和 n2 的乘积，现在已知 N 求 n1 和 n2。**主要计算步骤如下**：1）选择任意数字 a；2）计算 a 和 N 的最大公约数 gcd(a, N)。3）若 gcd(a, N) ≠1 程序结束；4）否则，利用量子计算来周期查找函数 f(x)= ax mod N 的周期 r，也就是能够使得 f(x+r) = f(x)；5）若 r 是奇数，回到第一步；6.）若 ar/2= -1 (mod N)，回到第一步。7）否则，计算 gcd(ar/2+1,N) 与 gcd(ar/2-1, N) ，他们至少有一个是 N 的因数。

Shor 算法将求解质因数分解问题，转换为求解余数周期的问题，而这一问题又可以通过量子计算机来实现加速。如下是查找函数 f(x)= ax mod N 的周期所构建的量子电路，首先我们构造两个量子寄存器 1 和 2，对寄存器 1 利用 H 门来形成叠加态的量子比特，然后利用量子的并行性，对所有的 f(x)同时进行求余数的计算，再利用量子的纠缠态，对寄存器 2 进行一次投影测量。此时由于纠缠的特性，周期信息被包含在了寄存器 1 的量子比特中。我们利用量子相干性，对寄存器 1 中的量子比特再做一次量子傅里叶逆变换（QFT），变换后量子比特中包含的周期信息转移到比特前的系数上，从而使得我们需要获取的量子比特值前的系数（即测量概率）会变大，而不需要的量子比特前的值会变小（甚至为 0）。对于变换后的寄存器 1 再做一次测量，将测得的量子比特值通过连分数的计算，就可以得出函数的周期 r。

图40. Shor 算法的量子电路

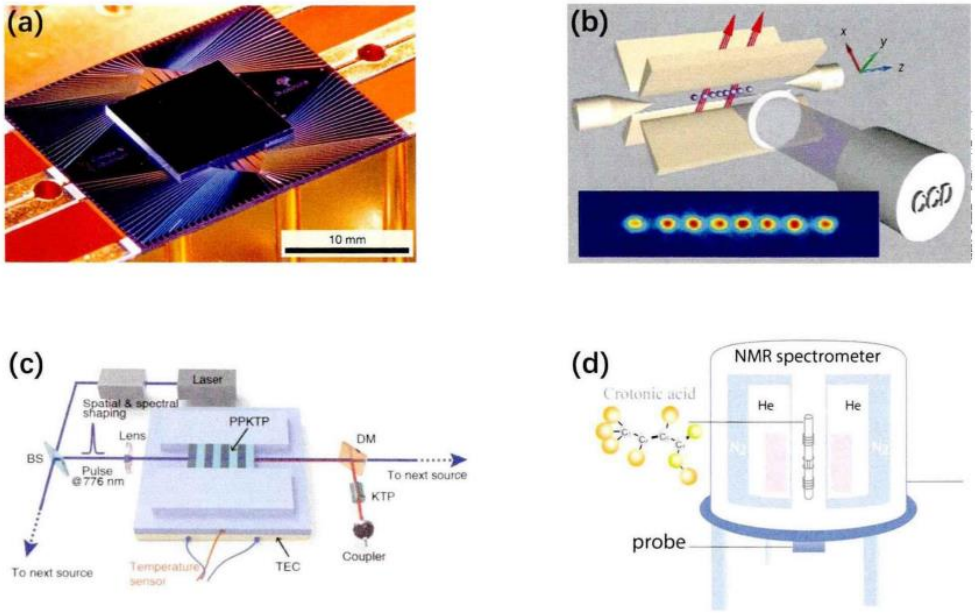


资料来源：《Algorithms for quantum computation: discrete logarithms and factoring》，国投证券研究中心

Shor 算法实现密码破解的指数级加速，为量子计算机打开了应用空间。2019 年 Craig Gidney 等发表论文《How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits》，提出用表面码编码形成的容错量子计算，结合 Shor 算法以及近些年再此基础上的优化方法，可以在 20 万个错误率在 0.1%的量子物理比特上在 8 个小时内破解 2048 位的 RSA 密码。随着评估解决算法的持续进步，也有人提出了可以优化实现的方法可以进一步减小物理量子比特的数量。因此我们认为 Shor 算法的落地已经在未来可见的时间内，为量子计算的商用典型了算法基础。**量子比特的物理实现依赖于一个服从量子力学基本原理的二能级系统，技术路径仍未收敛。**类似于经典计算机中使用二进制编码处理和保存信息，其中比特是信息的最小单元，量子计算机中，量子比特替代比特作为存储信息的最小单元。

但不同于经典计算机中，物理实现路径已收敛至，通过外端输入的电压信号对晶体管进行开关控制从而实现 0 和 1 的转变，量子计算机目前仍处于早期发展阶段，物理实现方案众多，包括但不限于离子阱、光量子、核磁共振、超导电路等，但其本质均旨在构建一个服从量子力学基本原理的二能级系统，例如离子的能级、光子的偏振、原子核的自旋、超导电路的电磁场能量等。

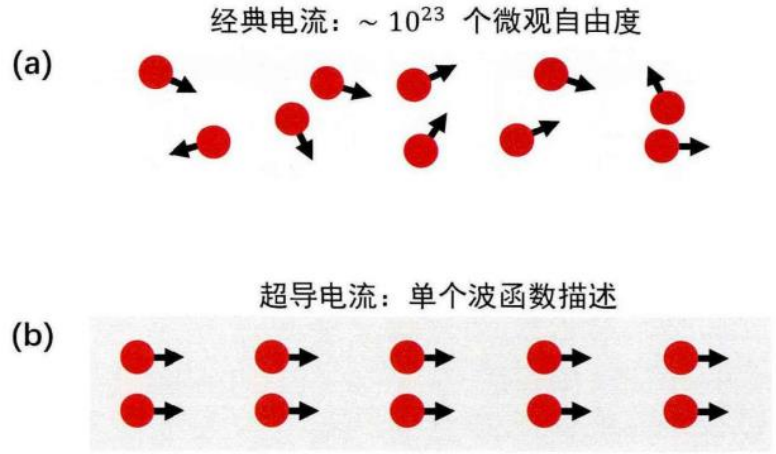
图41. 量子计算机的不同物理实现方案



资料来源：《超导多比特电路的量子操控和量子多体物理研究》郭秋江，国投证券研究中心

超导量子计算成为主流物理实现方案，理论基础是宏观量子现象。尽管学界对最终哪一种物理体系能够率先实现通用量子计算尚未形成统一意见，但是超导量子计算长期被寄予厚望，因此我们以超导量子计算为例，看量子比特的物理实现。对于 BCS 超导体，当温度低于超导临界温度时，电子之间通过电声子相互作用形成库伯对，此时在外加电场的作用下，尽管存在大量的库珀对电子的运动，但与经典过程不同的是，他们运动的“步调一致”、相位相干。因此，这种大量库珀对电子的集体运动行为可以用单个波函数来描述，呈现出宏观量子现象，即该电路可以用量子电动力学来描述。

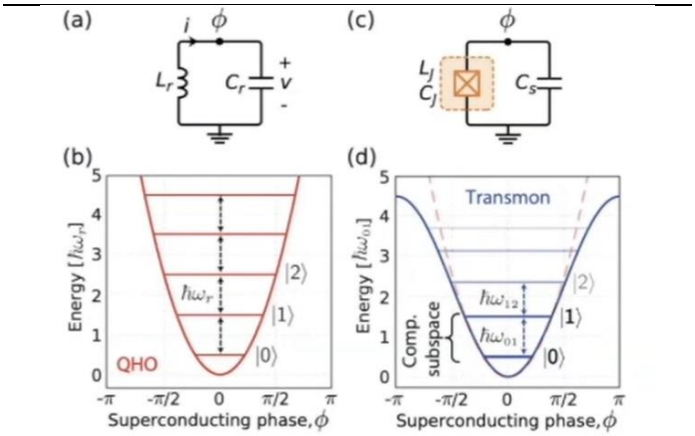
图42. 经典电流示意图和超导电流示意图



资料来源：《超导多比特电路的量子操控和量子多体物理研究》郭秋江，国投证券研究中心

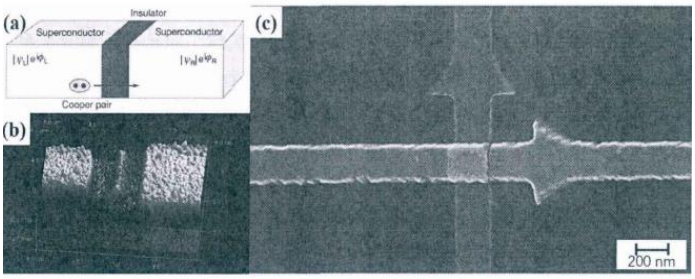
超导量子比特是一个利用约瑟夫森结非线性电路特性所构成的二能级系统。结合上文，一个处在超导状态下的 LC 振荡电路会表现出谐振子的物理特性，但由于其能级间的间距是无差别的，即系统可能被激发到各个高激发态，因此不能直接用来做量子比特。此时我们引入约瑟夫森结，其类似三明治结构（在两个超导层中间夹一层很薄的绝缘层），具有宏观量子遂穿效应，可以作为非线性器件来使用。通过非线性器件的引入，我们得以构建不同能级间距的能级态，并选择其基态和第一激发态构成二能级系统。因此，超导量子比特本质上是一种，利用约瑟夫森结在极低温环境下的非线性电路特性，由人工构建二能级系统。

图43. 振荡电路及能级图



资料来源：《基于超导量子比特芯片的测控与量子模拟》王战，国投证券研究中心

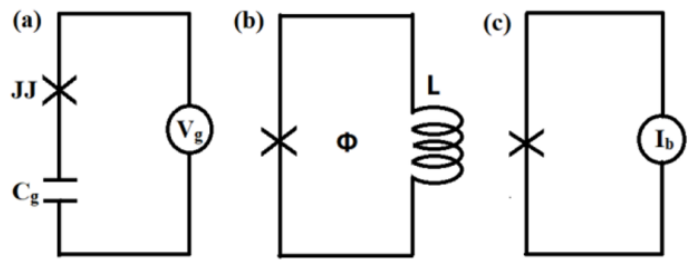
图44. 约瑟夫森结示意图与 SEM 扫描图



资料来源：《基于 transmon qubit 的量子芯片工作环境的研究与优化》孔伟成，国投证券研究中心

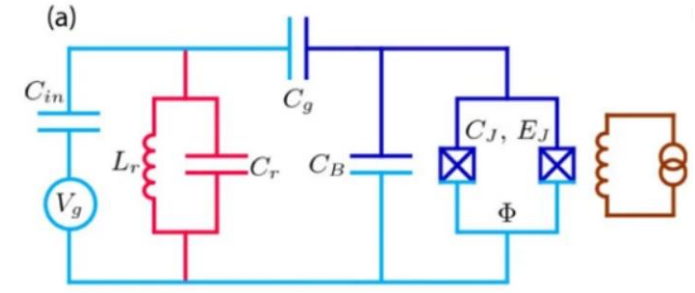
Transmon 型量子比特是目前最流行的超导量子比特。尽管理论上超导电路是无耗散的，但是由于电路尺寸太大，材料特性也不可能完美，导致现有工艺制备的超导量子比特与环境的耦合还是很强烈，退相干时间较短。因此在电荷、通量、相位三种超导量子比特原型的基础上，衍生出许多新的超导量子比特：如 Transmon 型量子比特、Fluxonium、0-π 量子比特、混合量子比特等。这其中，Transmon 型量子比特是目前最流行的超导量子比特，主要系结构简单、可扩展性好，并通过增大电容的方式降低了对电荷噪音的敏感度，从而提升了相干性，但代价是非线性比较弱。

图45. 电荷、通量、相位三种超导量子比特



资料来源：光子盒公众号，国投证券研究中心

图46. Transmon 量子比特及其电路示意图



资料来源：光子盒公众号，国投证券研究中心

超导量子比特具有设计可控性强、可扩展性好、易耦合和易操控等优势。超导量子比特的优点是在于制备工艺接近传统的半导体工艺，因此带来的好处包括：1）可以利用成熟的微加工技术完成芯片级的设计，使得超导体系的量子计算拥有接近经典计算机的高集成度潜力；2）一旦完成芯片线路设计就能快速利用成熟微加工产线加工出相应的芯片，试错时间成本低；3）与现有的微波电子技术结合紧密，工作频段在标准射频范围内，诸如电容、电感和传输线之类的电子元器件可以用来读出超导量子比特的状态，或者用来控制。

2.2. 量子计算机：从 NISQ 向 FTQC 迈进，技术路线较为多元

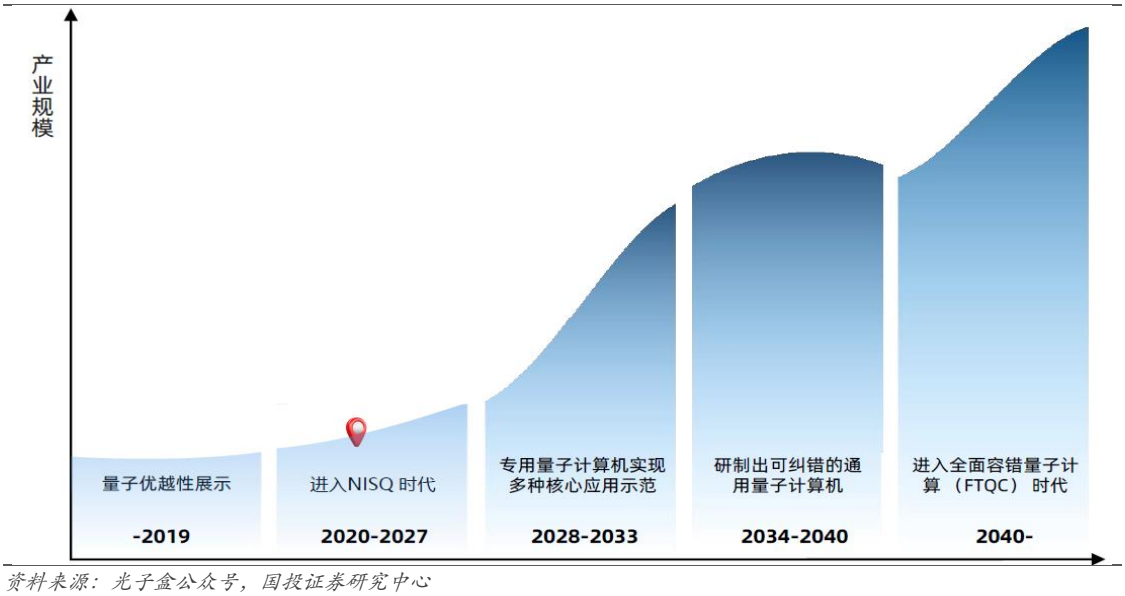
从量子计算机的演进来看，主要分为 5 个阶段。1）量子优越性展示：由计算领域成熟企业引导，完成初步的概念验证。IBM 早在 1990 年代就建立了专门的量子计算研究团队；Google 团队首次证明了量子优越性等；**2）进入中等规模含噪声（NISQ）时代：**初创企业以及大部分科研机构开始加入硬件研发以及纠错的行列，全面推进各个技术路线发展；**3）专用量子计算机实现多种核心应用示范：**各技术路线的专用量子计算机不断涌现，并且中下游的量子软件企业，将在这一阶段迅速增长。将优先在金融、医药、化工、汽车、机器学习等领域替代经典计算机，产生多种核心应用范例；**4）研制出可纠错的通用量子计算机：**各技术路线间的优劣势开始逐渐被放大，或将收敛到单一或几条特定路线，纠错成本大幅降低。由下游新应用场景的需求驱动产业链进一步细化，产业链上游话语权增加，产线扩张直至供需平衡；**5）进入全面容错量子计算（FTQC）时代：**运算错误率接近或小于经典计算机，量子比特数量将达百万量级。但即使计算机产业进入全面容错的量子计算时代，量子计算机和经典计算机依旧将并存，各自发挥优势，二者并非完全替代关系。

当前我们正处于 NISQ 阶段，而从 NISQ 向 FTQC 的跨越，是量子计算机从技术探索向规模商用迈进的重要过程。我们将这两者分别定义如下：

NISQ 时代（Noisy Intermediate-Scale Quantum，**中等规模含噪声**）：一些参与者强调使用更适度、嘈杂、中等规模的量子设备可能会更快实现。这避免了量子纠错所需的巨大开销，而是寻求在少量步骤（浅电路深度）完中成计算，以便每个物理量子比特门引入的错误不会变得难以处理。门模型量子计算机要在实际应用中获得广泛的量子优势，可能需要 99.99%+的 2Q 保真度。增强的甚至是针对特定问题的量子比特连接也可能非常重要。将需要与经典处理进行低延迟集成。

FTQC 时代（Fault Tolerant Quantum Computation，**大规模纠错容错量子计算机**）：对于某些应用，我们只需要“几个量子比特”。此类应用的早期示例通常位于量子计算、网络安全和量子通信的交叉点；这种重叠有望最终发展成为量子互联网，并通过传感器发展成为量子物联网。这里的不同权衡最终可能适合不同的量子比特平台。能够在更高、更容易部署的温度下提供一些相干寿命可能是一个有用的优势。

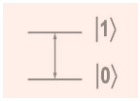
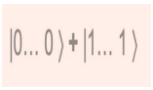
图47. 量子计算发展生命周期图



资料来源：光子盒公众号，国投证券研究中心

通用量子计算机的实现需要满足 DiVincenzo 的 5+2 技术准则。2000 年，IBM 研究员 David P. DiVincenzo 提出了构建可行的量子计算机的 5 条技术准则和量子通信的两条准则，只有满足准则的物理体系,才有望构建出可行的量子计算机。这 7 条准则分别为:(1)表征量子比特(2)量子比特有足够的相干时间（3）量子比特可以初始化（4）可以实现通用的量子门集合（5）量子比特可以被读出（6）静止量子比特和飞行量子比特相互转换的能力（7）在指定位置之间忠实地传输飞行量子比特的能力。

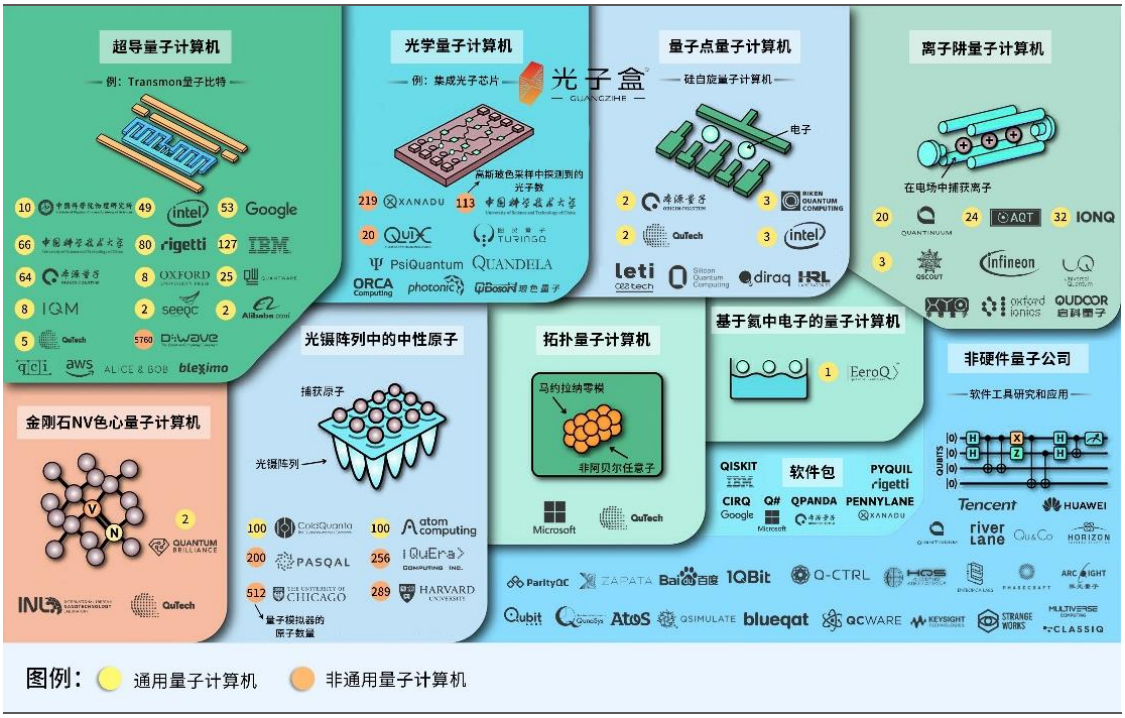
表10：DiVincenzo 关于量子计算机五条技术准则的解释

标准	示意	含义
表征量子比特		在可扩展物理体系中，要能很好的表征（定义）量子比特。需要一个由多比特组成的，用来存储信息的量子寄存器。在量子体系中，一种能够物理上实现量子比特的最简单的方式，莫过于利用二能级物理体系。例如：电子自旋、自旋为 1/2 的原子核等。同时使用几种类型的量子比特可能是实现可行的量子计算机最有前景的方式。
量子比特有足够的相干时间		当经典计算机无法重置时，即使其处理过程非常正确，所得的计算结果也不会令人信服。因此初始化对于经典计算机和量子计算机来说都是一个重要的部分。
量子比特可以初始化		对于一台内存比较大的经典计算机，需要通过一系列的逻辑门操作，把数据编码到内存上去。对于量子计算来说需要在内存上应用任意的逻辑操作门，去完成有用的量子信息处理过程。
可以实现通用的量子门集合		对于量子计算，需要测量运算量子算法之后的状态以提取计算结果，测量过程在很大程度上取决于所考虑的物理系统。由于退相干（量子比特非常脆弱，它对外界的微扰极其敏感，量子比特的计算状态如果由于外界影响发生变化称为退相干），量子门操作误差等原因，测量通常没有 100%的准确性。如果是这种情况，必须重复多次相同计算，以达到合理且比较高的置信度。
量子比特可以被读出		建造一个可实用的量子计算机，退相干的问题可能是一个最大的障碍。由于系统会和环境有相互作用，退相干也就意味着量子态的诸多方面都会退化，同时也会限制量子计算的最大有效时长。

资料来源：光子盒公众号，量子客公众号，国投证券研究中心

当前量子计算机在物理实现上，分为多种技术路线，其中超导和离子阱路线相对领先。围绕量子计算的一大热点问题是哪种硬件技术将最终胜出，目前主要有五个资格充足且经过充分论证的候选方案正在竞争，分别为超导、离子、光量子、半导体量子点和冷原子(或称为中性原子)。这些方案都是在 20 世纪 90 年代开创性的物理实验和实现中开发的。**目前，以超导电路和离子阱技术搭建的量子计算系统基本满足 DiVincenzo 标准的 5 个条件，而光量子系统在第（3）条的受控非门方面较难实现。**从量子计算的物理实现要求和现今技术发展情况来看，超导和离子阱的量子计算实现系统当前比较成熟。此外，国际上正在尝试的量子计算系统的物理实现还有中性原子、硅自旋、拓扑、NV 色心和量子点等约十种方式。

图48. 量子计算机主要技术路线和参与公司



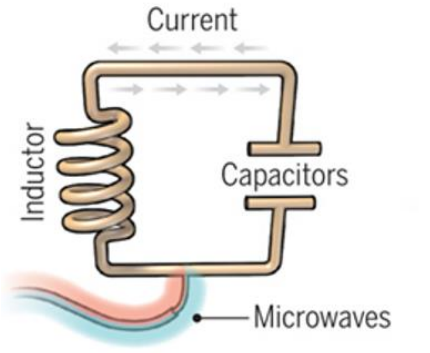
资料来源：光子盒公众号，国投证券研究中心

超导量子计算机方案是目前国际上进展最快的方案。原理上，超导量子计算技术使用电荷量子比特、磁通量子比特和相位量子比特这三种方式来形成量子比特。目前普遍采用的 Transmon 量子比特，是一种基于电荷量子比特的改良的设计，该设计可以减小量子比特对于电荷噪声的敏感度，从而提高退相干时间，使得测量操纵变得更加容易。

图49. 超导量子计算机示意图

资料来源：国盾量子官网，国投证券研究中心

图50. 超导量子计算技术



资料来源：Science，国投证券研究中心

超导量子比特是人造原子，在操控、耦合、测量、扩展等方面具有独特的优势。目前超导量子技术路线的难点在于易受环境噪音影响，而导致退相干时间短。但该技术路线的发展并无原则性障碍。当前的发展主要侧重于可控耦合量子比特的数目与可以连续进行的高保真度多量子比特逻辑操作次数的继续提高。长远来看，该条技术路线在未来比较容易实现规模化。

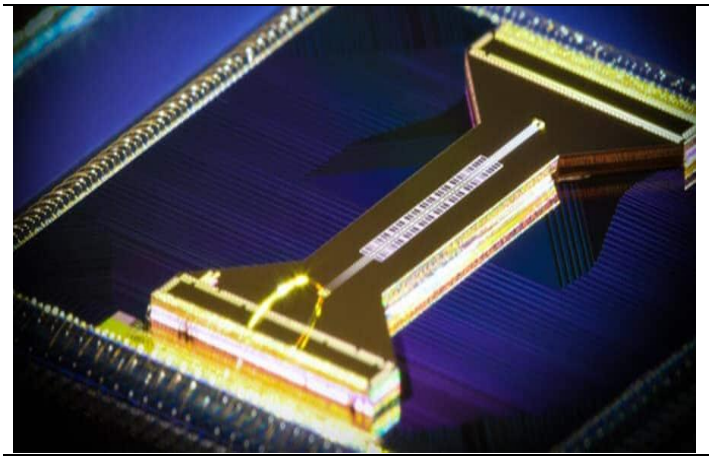
表11：中美超导量子计算机进展

中国		美国	
时间	进展	时间	进展
2018 年	中科大、浙江大学等联合实现 11 位超导量子比特纠缠	2019 年	谷歌报道 53 位比特处理器“悬铃木”，量子随机路线采样问题中首次实验验证量子计算优越性。
2019 年	中科大实现 24 位超导量子比特处理器，并进行多体量子系统模拟；同时，清华大学利用单量子比特实现精度 98.8%的量子生成对抗网络，未来可应用于图像生成等领域。	2019 年	1 月，IBM 展示具有 20 位量子比特的超导量子计算机，并在 9 月将量子比特数量更新为 53 位。
2019 年	本源量子研发了适用于 20 位量子比特的量子测控一体机，用于提供量子处理器芯片运行所需要的关键信号，实现量子芯片操控。	2020 年	IBM 推出 65 位比特样机“蜂鸟”，在德、日、英等国开展部署，通过云平台向部分用户开放
2021 年 5 月	中科大报道 62 位“祖冲之”处理器实验演示二位量子随机行走	2021 年	谷歌发布路线图预测 2029 年实现百万位量子比特和可纠错量子计算
2021 年 10 月	中科大报道 66 位处理器在与 Google 相同问题中，以更大优势验证量子计算优越性。	2021 年 11 月	IBM 推出 127 位量子比特 Eagle 处理器
2021 年	本源量子发布超导样机研发计划，预计 2025 年达 1024 位比特。	2022 年 2 月	Regetti 上线 Aspen-M80 量子比特系统，预计明年初发布 84 个量子比特单芯片处理器 Ankaa。
2022 年 7 月	阿里报道实现 Fluxonium 系统中双比特门的 99.72%保真度。	2022 年 5 月	IBM 发布 433 量子比特 Osprey 处理器
2022 年 8 月	百度发布超导量子计算机乾始。	2023 年	IBM 推出 1121 位量子处理器 Condor
2023 年	中科大在 66 位超导量子处理器“祖冲之二号”基础上新增 110 个耦合比特控制接口，使可操纵比特数达到 176 位	2023 年	Regetti 推出 84 位量子比特单芯片量子处理器 Ankaa-1。
2023 年	中科院物理所利用 41 位超导量子芯片“庄子”模拟“侯世达蝴蝶”拓扑物态。	2023 年	谷歌使用超导量子处理器模拟操控非阿贝尔任意子，并通过编码创新新型量子纠缠态

资料来源：信通院，国投证券研究中心

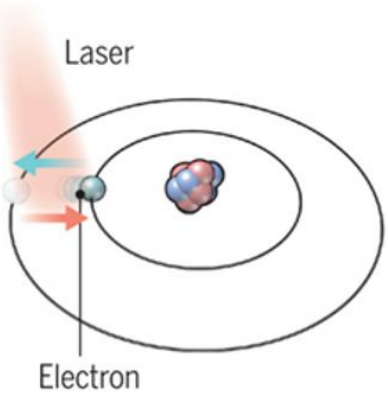
离子阱量子计算机至今已经发展 20 余年，与超导量子计算的发展旗鼓相当。原理上，其利用电荷与电磁场间的交互作用力牵制带电粒子运动，并利用受限离子的基态和激发态组成的两个能级作为量子比特，利用微波激光照射操纵量子态，通过连续泵浦光和态相关荧光实现量子比特的初始化和探测。

图51. 离子阱芯片



资料来源：霍尼韦尔官网，国投证券研究中心

图52. 离子阱技术示意图



资料来源：《How small startups are vying with corporate behemoths for quantum supremacy》，国投证券研究中心

离子阱技术的优势在于相干性好，可纠缠量子比特数目多，逻辑门保真度高。离子阱的劣势表现为量子比特操纵速度相对较慢，并且随着量子比特数量的增加，其操纵仍有技术困难。离子阱技术在应用方面，除量子计算机外，还广泛应用于量子化学、相对论量子力学、量子热力学等领域的量子模拟研究。

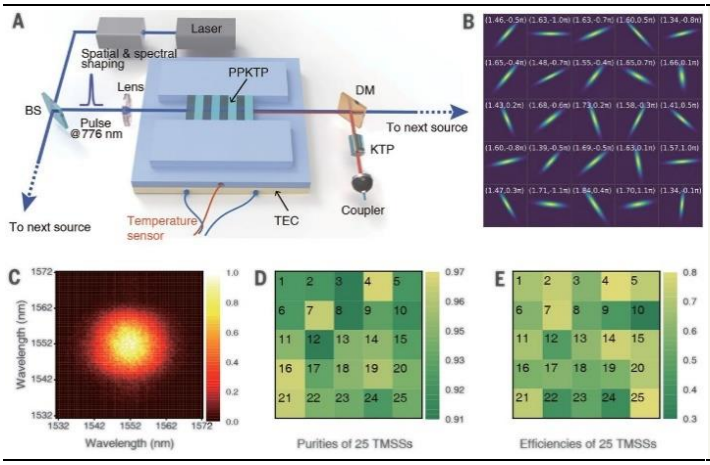
表12：国内外离子阱量子计算机进展

中国		海外	
时间	进展	时间	进展
2018 年	中科大分别实现相干时间最长的离子阱体系量子储存	2019 年	IonQ 已实现 79 位光量子比特和 160 位存储量子比特。
2020 年	清华大学、中山大学和启科量子等研究机构和公司在离子阱路线有所布局和研究。	2019 年	霍尼韦尔的离子阱量子比特装置已进入测试阶段
2021 年 1 月	清华大学交叉信息院金奇奂研究组在离子阱系统中首次将单量子比特相干时间提升至 1 小时以上，即 5500 秒。	2020 年	IonQ 发布 32 位数比特离子阱样机，预计在 2025 年比特数达到 64 位。
2021 年 9 月	中山大学物理与天文学院罗乐教授研究团队实现了离子阱中量子比特微运动抑制的自动化处理，这是国际上首次把神经网络技术应用于囚禁离子量子比特的微运动控制。	2020 年 10 月	IonQ 公司报道仅依靠 32 位高质量全连接的量子物理比特即可实现四百万量子体积性能指标，将该指标直接推向指数增长区间。
2022 年 1 月	清华大学交叉信息研究院段路明研究组在离子阱量子信息处理领域取得重要进展，首次实现对长离子链的高效协同冷却，获得接近全局激光冷却的极限温度，为多离子比特量子计算准备了技术基础。	2020 年 11 月	MIT 林肯实验室报道实现基于集成光学的离子阱处理芯片
		2021 年	Honeywell 报道基于电荷耦合器架构的 10 位高保真比特原型机“H1”，预计在 2023 年实现 40 位量子比特原型机“H2”，2030 年实现基于集成光学栅格的模块化百位量子比特样机。
2023 年 2 月	启科量子发布了国内首台模块化离子阱量子计算工程机 1.0“天算 1 号”，综合工程化水平进入国际先进行列。	2022 年	6 月，Quantinuum 的 Model-H1 离子阱量子计算机扩展到 20 全连接量子比特，9 月实现量子体积指标 8192 新纪录。
2023 年 4 月	华翊量子发布 37 位量子比特离子阱原型机 HYQ-A37。	2022 年 3 月	3 月 29 日，IonQ 报道钡基离子阱处理器的保真度达到 99.96%
2023 年 12 月	启科量子在离子阱量子计算工程机上成功实现量子速度极限测试	2023 年	Quantinuum 宣布其 32 位全连接量子比特离子阱原型机 Model H2 的单比特和双比特量子逻辑门保真度达到 99.997%和 99.8%，量子体积指标达到 524288，成为业界最新纪录。

资料来源：信通院，国投证券研究中心

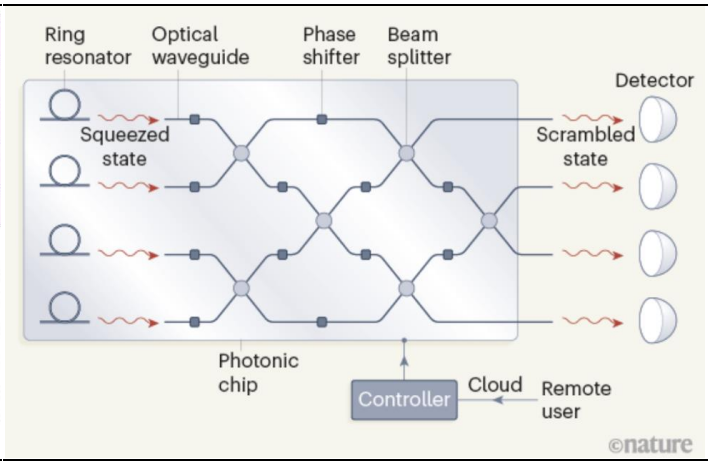
光量子是除超导量子和离子阱之外研究进展较快的技术路线。原理上，光量子计算机利用光子的偏振、路径、轨道角动量、时隙等自由度，将其编码量子比特的技术路线实现。根据是否支持逻辑门和量子纠错等操作，光量子可进一步分为逻辑门型和非逻辑门型两类：(1) 逻辑门型光量子计算是未来实现通用量子计算的发展方向（2）非逻辑门型光量子计算，如玻色采样和相干伊辛系统等，可用于组合优化和图论问题求解等专用计算问题。

图53. 光量子光学装置



资料来源：《Quantum computational advantage using photons》，国投证券研究中心

图54. 光量子技术



资料来源：《Quantum circuits with many photons on a programmable nanophotonic chip》，国投证券研究中心

光量子的技术优势主要体现在，光子不易于受到外界环境影响，所以由光子编码成的量子比特抗退相干能力强。同时，由于光子具有多个自由度的特性，可以用更少的光子数实现更多的物理量子比特。由于光子之间相互作用非常微弱,传统的光量子计算机技术只能实现光子的概率性逻辑门(对应确定性逻辑门)，这也是光量子技术路线实现通用量子计算道路上目前最大的阻碍。不过目前已有一些光量子方案实现了确定性和可重构性。

表13：国内外光量子计算机进展

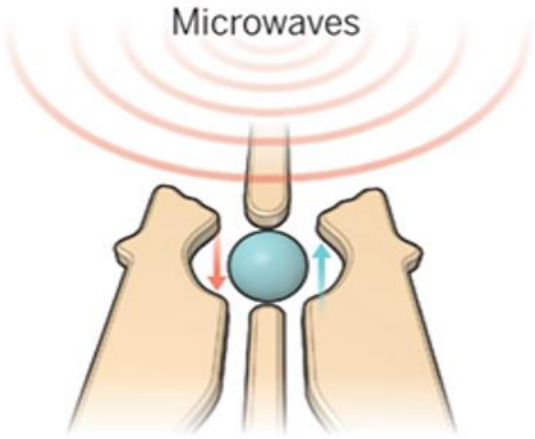
中国		海外	
时间	进展	时间	国家/地区
2019 年	中科大已实现 18 位光量子纠缠操控，处于国际领先地位。		
2019 年	中科大实现了高保真的单比特逻辑门		
2020 年	中科大在量子计算研究探索方面处于领先，实现 50 位光量子物理比特纠错操控和玻色取样实验。	2022 年 6 月	加拿大：Xanadu 报道 Borealis 光量子计算机完成 216 压缩高斯玻色采样实验，在此验证光量子计算优越性。
2020 年	上海交大在基于光子集成的光量子芯片领域开展了布局研究。		
2020 年 12 月	76 光子单模压缩光学实验系统九章，在高斯玻色采样问题中实验验证量子计算优越性，2021 年报道进一步提升为 113 光子，在相同问题中更大优势验证量子计算优越性。		
2023 年	中科大联合团队发布 255 光子的“九章三号”光量子计算原型机，进一步提升了高斯玻色采样速度和量子优越性。		
2023 年	玻色量子发布了 100 量子比特相干光量子相干伊辛机“天工量子大脑”，并与中国移动合作开展图像渲染算力调度优化等任务的可行性验证。	2022 年 8 月	德国：马克思-普朗克研究所报道实现 14 个光子纠错操控新纪录
2023 年	中科大联合团队发布 255 光子的“九章三号”光量子计算原型机，进一步提升了高斯玻色采样速度和量子优越性。		
2023 年	玻色量子发布了 100 量子比特相干光量子相干伊辛机“天工量子大脑”，并与中国移动合作开展图像渲染算力调度优化等任务的可行性验证。		

资料来源：信通院，国投证券研究中心

量子点技术利用半导体工艺，更容易实现芯片化，但相干性和比特数仍需提升。半导体量子点可以作为量子比特，也叫自旋量子比特。量子点是一种纳米大小的半导体粒子，一般为球形或类球形。由于这种纳米半导体粒子拥有限制电子和电子空穴的特性，这一特性类似于自然界中的原子或分子，因而被称为量子点。常见的量子点有硅量子点、锗量子点、硫化镉量子点和砷化铟量子点等。其中，半导体量子点或量子自旋技术路线是利用半导体量子点中的电子制造量子比特，将其电子的自旋方向编码为量子态用来存储量子信息。半导体量子点计算机结合了当前的半导体工业技术，未来可以快速实现产业化，同时由于半导体量子比特体积较小，较超导技术路线和光量子技术路线而言更容易实现芯片化。但是，当前半导体量子比特的数量较少，且相干性较弱。

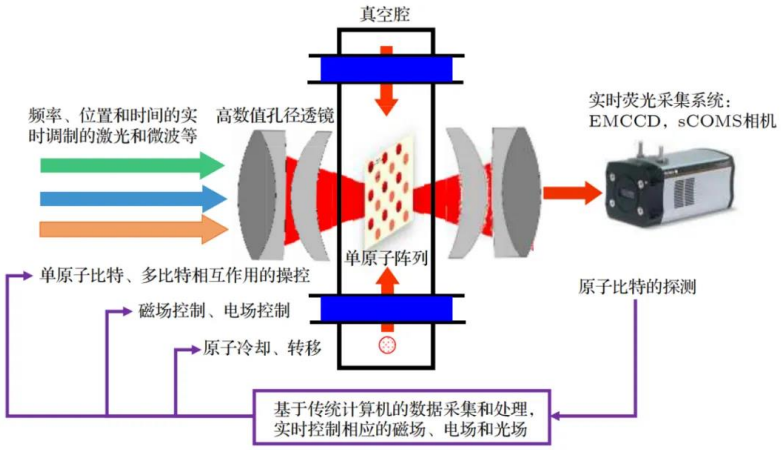
中性原子技术/冷原子技术，实现长相干时间，但比特之间的相互作用较难。中性原子是指核外电子等于核内质子数的原子，具有全同性且处于低能态的特点。原理上，中性原子量子计算机利用光镊或光晶格囚禁原子，激光激发原子里德堡态进行逻辑门操作或量子模拟演化。该技术在时间和操控精度等特性与离子阱路线相似，而在规模化扩展方面更具优势。当前中心原子技术路线尚不成熟，包括需要特定技术来实现量子比特之间的相互作用，从而制备纠缠态的比特对，以及在操作精度和设备成熟度方面的挑战。

图55. 硅半导体技术示意图



资料来源：《How small startups are vying with corporate behemoths for quantum supremacy》，国投证券研究中心

图56. 中性原子技术原理



资料来源：光子盒公众号，国投证券研究中心

针对不同的技术路线，可以用量子体积这一指标来衡量不同量子计算机的性能。由于当今量子计算机使用了不同的技术路线和指标，很难对比机器的整体性能。不同技术路线的量子计算机不能只从量子比特的数量来衡量，而忽略了影响计算能力的其他重要因素。为了衡量不同技术路线下的量子计算机性能，需要建立一套指标体系。2017 年，IBM 的研究人员引入了量子体积 Quantum Volume (QV)这一与硬件无关的指标进行简单的量子计算机性能衡量。量子计算机的 QV 越大，它可以解决的问题就越复杂。

从量子体积的衡量指标来看，**量子比特的数量和可以执行的操作数量称为量子电路的宽度和深度。**量子电路越深，计算机可以运行的算法就越复杂。量子电路深度受诸如量子比特数量、量子比特互连方式、门和测量错误、设备串扰、电路编译器效率等因素的影响。**相干性是另一个影响量子体积的重要因素。**相干时间 T1 表示量子比特自然弛豫的时间，即处于高能状态的量子比特自然会衰减到低能状态，与这种衰减相关的时间称为相干时间 T1。相干时间

T2 表示量子比特受环境影响的时间，即量子比特也有可能与环境相互作用并在弛豫到|0>状态之前遇到相位错误，与这种衰减相关的时间常数称为相干时间 T2。

此外，**保真度对量子体积也有重要影响。**量子计算机通过操纵比特的状态来执行计算--将比特从 0 更改为 1，将 1 更改为 0。保真度是衡量尝试翻转导致正确量子比特状态两个量子态“接近程度”的度量。由于环境噪声及量子处理器自身品质的影响，实际量子处理器执行结果往往与理想情况下经过量子门操作得到的结果有一定的偏差。这种偏差可以用理想量子态和实际量子态之间的保真度来衡量。保真度数值越大，代表偏差越小，系统的计算结果就越好。计算的准确性取决于以非常高的成功率或“保真度”执行这些“比特翻转”的能力。霍尼韦尔量子计算系统 99.997%的单个量子比特操作保真度是目前所有可寻址量子比特技术中报告的最佳性能。

图57. 影响量子体积的因素

资料来源：光子盒公众号，国投证券研究中心

表14：量子计算机性能对比

	超导	离子阱	光量子	硅半导体	中性原子
量子比特规模（光子/原子/量子点）	433 (IBM)	37 (华翊量子)	255 (中科大)	16 (TUDelft)	1180 (Chicago)
单比特逻辑门保真度	99.99% (Maryland)	99.9999% (Oxford)	99.84% (华中科大)	99.96% (SQC)	99.9953% (精测院)
双比特逻辑门保真度	99.92% (MIT)	99.92% (NIST)	99.69% (华中科大)	99.65% (TUDelft)	99.5% (Harvard)
SPAM 读取保真度	99.2% (ETH Zurich)	99.9904% (Quantinuum)	98% (赋同科技)	97% (Princeton)	99% (QuEra)
T1 时间	1.2 ms (Maryland)	数百 s 量级	数百μs 量级	数百 ms 量级	数百 s 量级
T2 时间	1.48 ms (Maryland)	5500s (清华)	数百μs 量级	0.23 ms (UNSW)	40±7s (Atom Computing)
门速度	24 ns (中科大)	μs~ms 量级	ns~μs 量级	ns~μs 量级	数百 ns 量

资料来源：信通院，国投证券研究中心

当前量子计算机参与者主体较为多元，主要参与者可分为四大类：第一类是国际科技巨头，例如 IBM、谷歌、霍尼韦尔等；第二类是量子计算初创公司，例如 Rigetti、IonQ 等；第三类是国家科研院所，例如美国费米国家实验室(Fermilab)、美国阿贡国家实验室(Argonne National Laboratory)、中科院量子信息与量子科技创新研究院；第四类是高水平研究型大学，例如剑桥大学、中国科学技术大学、哈佛大学等。其中我们看到，超导和离子阱技术参与的企业和科研机构最多，也反映了这两种技术路线的成熟度较高。

表15：量子计算机主要参与者

技术路线	机构类型	采用机构
超导	学术团队	加州大学圣巴巴拉分校(UCSB)、耶鲁大学、麻省理工学院(MIT)、美国国家标准与技术研究院(NIST)、加州大学伯克利分校、马里兰大学、芝加哥大学、荷兰代尔夫特大学(TU Delft)、瑞士苏黎世联邦理工学院(ETH)、**中科大**、清华大学、**浙江大学**、南京大学、南方科技大学、日本理化学研究所(RIKEN)、北京量子院、中国科学院量子信息与量子科技创新研究院、中国科学院物理研究所、法国 CEA 研究中心、IBM 苏黎世研究所
	公司	**IBM、谷歌、Rigetti、D-Wave**、英特尔、NEC、OCI、Oxford Quantum、**本源量子、国盾量子、量旋科技**、亚马逊
离子阱	学术团队	**哈佛大学**、MIT、马里兰大学、杜克大学、牛津大学、**清华大学**、国防科技大学、中科大、中国人民大学、中山大学、中科院量子信息重点实验室、因斯布鲁克大学、苏塞克斯大学(Sussex)、**NIST、Sandia 国家实验室**、中国科学院量子信息与量子科技创新研究院、北京量子院
	公司	**霍尼韦尔、IonQ**、Alpine Quantum Technologies(AQT)、Unversal Quantum、**启科量子**
光量子	学术团队	**牛津大学**、MIT 电子研究实验室、维也纳大学量子科学与技术研究中心、布里斯托大学量子光学研究中心、昆士兰大学量子计算与量子通信技术研究中心、**中科大**、南京大学、山西大学量子光学与光量子器件国家重点实验室、RIKEN 日本国立研究开发法人量子科学技术研究开发机构、中国科学院量子信息与量子科技创新研究院
	公司	**Xanadu、PsiQuantum、惠普、图灵量子、玻色量子**、法国 Quandela、英国 Tundrasystems
量子点	学术团队	普林斯顿大学、TU Delft、东京大学、北京大学、中科大量子信息重点实验室、新南威尔士大学(UNSW)、澳大利亚国家量子计算与通信技术研究中心(COCT)、中国科学院量子信息与量子科技创新研究院、RIKEN、法国 CEA-CNRS Grenoble 研究中心、比利时 IMEC 研究中心、美国 HRLLaboratories 美国 Sandia 国家实验室、日本 NIT、威斯康辛量子研究所(WOI)
	公司	**英特尔、本源量子**、Silicon Quantum Computing(SQC)
冷原子	学术团队	哈佛大学、香港科技大学、中科大、中科院量子信息重点实验室、清华大学、山西大学、中国科学院量子信息与量子科技创新研究院、中国科学院武汉物理与数学研究所
	公司	ColdQuanta、Atom Computing、QuEra Computing、PASQAL

资料来源：光子盒公众号，国投证券研究中心

2.3. 量子计算机结构：量子芯片、稀释制冷机和测控系统是核心

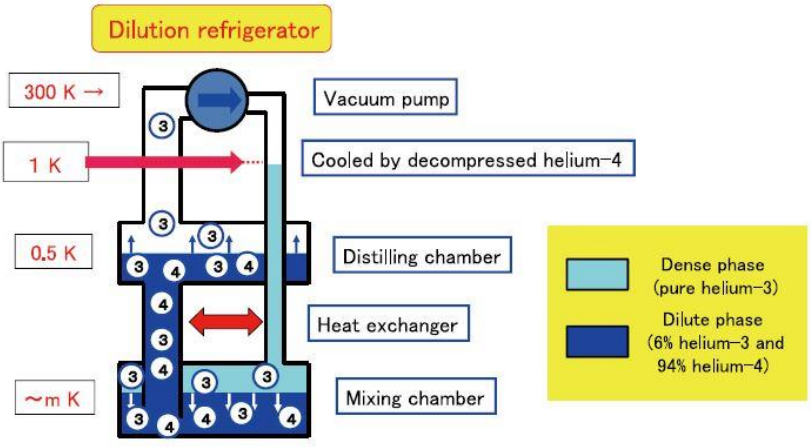
我们以超导量子计算机为例，来分析量子计算机的主要结构。超导量子计算机由量子芯片、稀释制冷机、测控系统三大核心部件构成。具体来看，1）**稀释制冷机**外形呈桶状，用于产生极低温、低噪声的环境，是超导量子计算机正常运行的必要基础；2）**量子芯片**是量子比特和外围电路的物理载体，其沿用了现有的半导体生产工艺，主要由超导量子计算机厂商自研；3）**室温测控系统**用于量子比特状态的控制和读取，其由 AWG、微波源等电子测量仪器构成，产业成熟度相对较高。此外，超导量子计算机还包括了软件系统、低温线缆、低温器件等。价值量方面，根据合肥超量融合计算中心项目招标文件，一台 200 量子比特的超导量子计算机单价约为 4500 万元。

图58. 超导量子计算机及核心系统

资料来源：国盾量子、Bluefors、《基于超导量子比特芯片的测控与量子模拟》王战、国投证券研究中心

稀释制冷机是生成低温环境的核心设备。超导量子计算机需要运行在超低噪声的环境中，稀释制冷机是实现该环境的核心设备。超导量子计算机是基于超导电路的量子比特体系，对于工作环境的最基本要求就是温度低于其超导临界温度（约 1.18K），同时为了提高相干时间、降低噪声，温度需要降低到 10mK 左右。从原理上来看，稀释制冷机利用了氦-3 和氦-4 的混合液体在 0.8K 左右发生的相分离现象，随着氦-3 从浓缩相向稀释相扩散，这一扩散过程会吸热，从而达到制冷的目的。

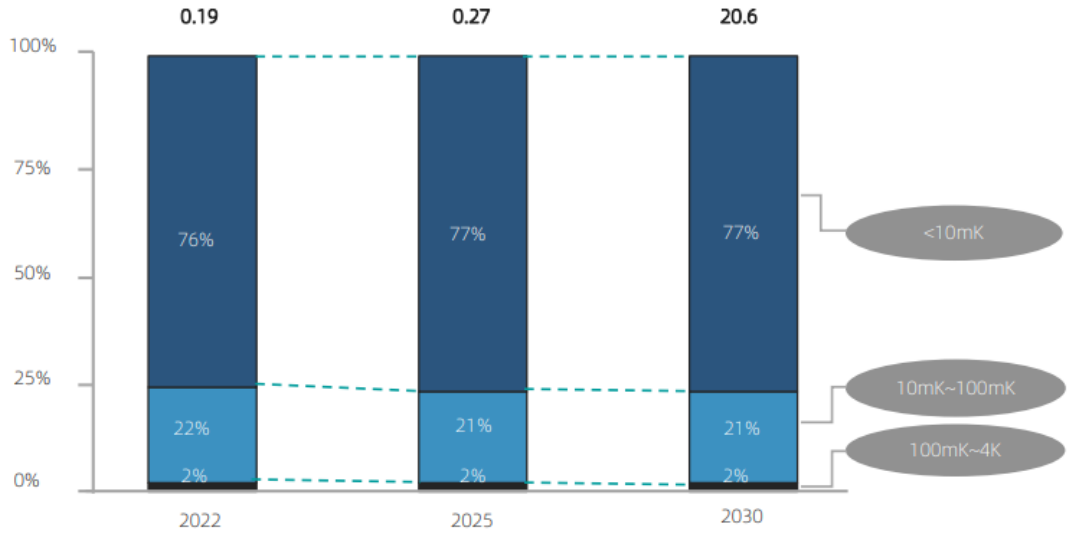
图59. 稀释制冷机原理示意图



资料来源：ULVAC，国投证券研究中心

稀释制冷机全球市场约 2 亿美元，行业呈现加速增长趋势。根据 ICV，2019-2015 稀释制冷机的年均增长率达到 8.59%以上，且增长率逐年上升。2022 年全球稀释制冷机市场规模将为 1.93 亿美元，到 2025 年预计达到 2.66 亿美元，并呈现加速增长的趋势。从单台价格来看，稀释制冷机的单价从百万到千万元不等，其价格与制冷功率相关性较大。根据招标网信息，本源量子于 2024 年中标的一台稀释制冷机 SL400 的单价为 450.7 万元。此外，自 2023 年起，10mK 以下温区的稀释制冷机已对我国禁运，且由于 10mk 以下温区的稀释制冷机占据了大部分市场，我国的稀释制冷机进口规模自 2023 年以来有所下滑。

图60. 2022-2030 年全球稀释制冷机市场规模（10 亿美元）



资料来源：2023 全球量子计算产业发展报告-ICV&光子盒，国投证券研究中心

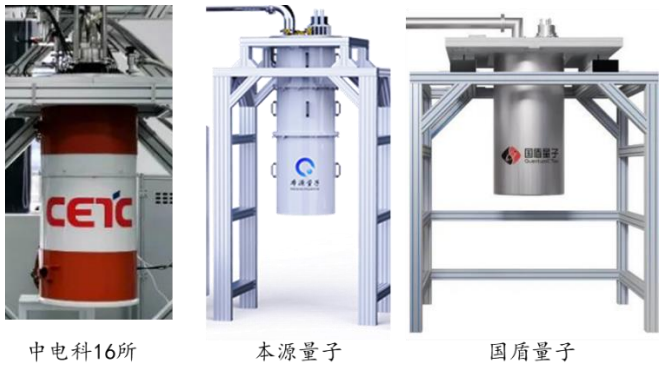
芬兰的 Bluefors 和英国的牛津仪器是全球主要供应商，国产已实现突破。全球来看，量子计算专用稀释制冷机市场主要由 Bluefors 和牛津仪器两家公司占据，其中 Bluefors 由于在量子计算领域起步较早，市场份额长期占据第一，且与量子计算领域头部公司 IBM 保持着深度合作。牛津仪器则在近年来推出了一系列新品，发展较快。根据北京量子信息科学研究院的中标公告，该单位 2021 年购入 Bluefors 和牛津仪器稀释制冷机分别为 8 台和 5 台。**国产方面，**中科院物理所在 2021 年取得了国产稀释制冷机的突破，自主研发的无液氦稀释制冷机原型机率先实现 10mK 以下极低温环境，此外电科 16 所也于 2023 年取得突破。目前，包括国盾量子、本源量子等企业已向市场推出国产稀释制冷机。

图61. 全球稀释制冷机主要供应商

BLUEFORS
Leiden Cryogenics
Leader in Low Temperature Techniques
FORMFACTOR™
OXFORD INSTRUMENTS

资料来源：Bluefors、牛津仪器、Leiden Cryogenics、formfactor,国投证券研究中心

图62. 国产稀释制冷机

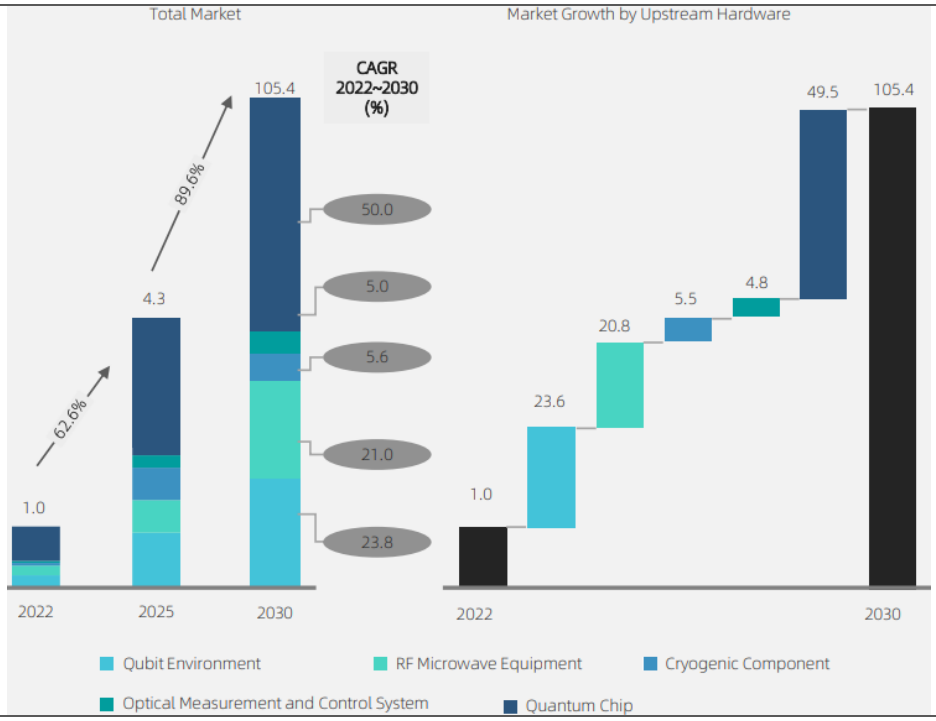


中电科16所　本源量子　国盾量子

资料来源：中电科 16 所、本源量子、国盾量子，国投证券研究中心

量子芯片是量子比特和外围电路的物理载体，是量子计算机厂商的研发重点。超导量子计算机的硬件性能主要取决于量子比特的数量和质量，而量子芯片则是量子比特的物理载体，因此目前绝大多数参与量子计算机的厂商均把研发重心放在了量子芯片上，即大多数量子芯片均是实验室或科研机构自研的产品。根据 ICV，2022 年量子芯片的市场规模约为 5.45 亿美元，预计 2030 年量子芯片的市场规模将达到 500 亿美元。

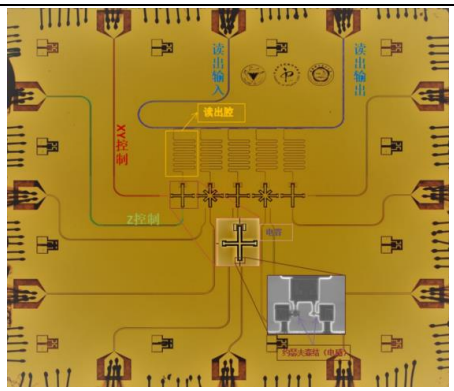
图63. 2022-2030 年全球量子计算上游产业规模（10 亿美元）



资料来源：2023 全球量子计算产业发展报告-ICV&光子盒，国投证券研究中心

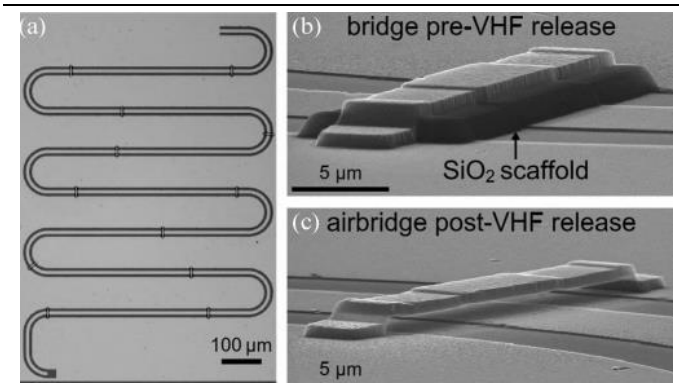
量子芯片结构从一维向三维演进，集成度持续提升。由于稀释制冷机内部空间极为有限，量子芯片的尺寸一般为 100mm²量级，而量子芯片中包含了约瑟夫森结（尺寸在 100-1000nm），控制线、谐振器、电容电感、读出线等结构（尺寸在 100-1000μm），且考虑到电磁场的串扰影响，各结构间都要保留足够的间隔，因此早期量子芯片中的比特数大都在 10 以下，例如 IBM 于 2016 年发布的 5 比特处理器 Tenerife。随着比特数量的增长，2 维的空桥方案被广泛采用，即利用架空的超导传输线相互接地，以降低线路间的干扰并节省线路排布空间。当比特数接近 100 后，量子芯片开始向 3 维发展，目前常见的是将量子比特和读出控制分成 2 个单独的平面，并用倒装焊模式进行连接，从而提升集成度。

图64. 一个具有 5 比特的超导量子芯片



资料来源：《基于超导量子比特芯片的测控与量子模拟》王战，国投证券研究中心

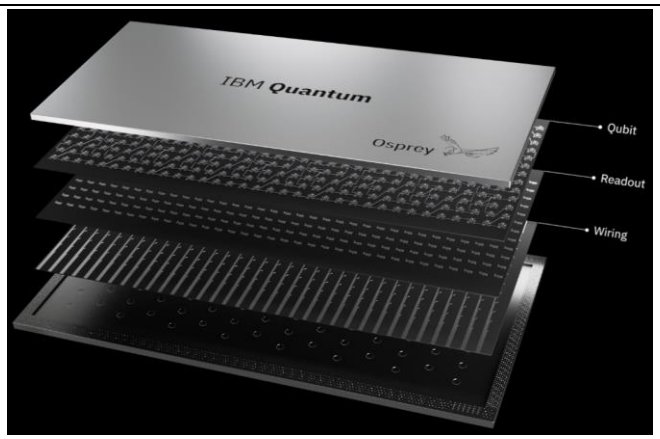
图65. 空桥结构示意图



资料来源：《超导量子芯片集成技术概述》郑伟文，李晓伟，熊康林等，国投证券研究中心

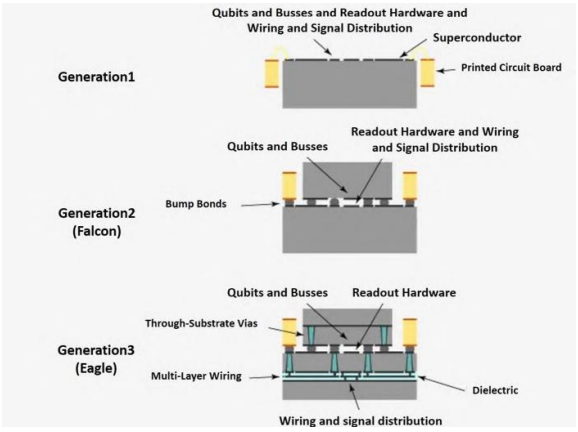
TSV 多层堆叠是量子芯片比特数进一步提升的关键技术。当比特数量进一步提升，上下 2 层结构也无法满足排线的空间需求时，此时需要更多的平面进行比特的扩展，TSV（硅通孔）开始被引入。其将两面的图形结构线路通过 TSV 内的导线进行连通，再利用倒装焊模式与第 2 个芯片进行连接，不仅充分利用了晶圆的正反面空间，同时解决了排线密集占空间的问题。例如 IBM 433 量子比特处理器 Ospery 便采用了 TSV 和多层布线技术，将量子比特、读出谐振器和测控线分成 3 个部分，再利用倒装焊进行多层互联。

图66. IBM 433 量子比特处理器 Ospery



资料来源：IBM 官网，国投证券研究中心

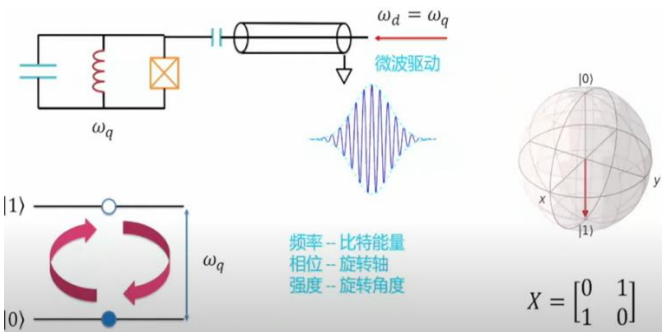
图67. IBM 超导量子计算机技术迭代图



资料来源：IBM 官网，国投证券研究中心

测控系统用于量子比特的实时控制、测量、反馈，是量子计算机的重要组成部分。由于超导量子比特本质上是一个由超导电路形成的二能级系统，因此我们可以使用微波信号对其进行控制，而测控系统便是生成和读取各类微波信号的设备，是量子计算机的重要组成部分。已有的量子测控系统可分为两代，第一代主要由可直接生成和接收模拟微波信号的设备组成，即波形发生器、模拟信号源、IQ 混频器、高精度电源等一系列通用电子测量仪器，其易于实现，但因缺乏反馈控制而使可扩展性和编程能力受限。二代测控系统则兼具可灵活编程的反馈控制能力和更好的可扩展性，例如本源量子于 2020 年推出第二代量子测控一体机，支持 216 通道，具备 200 皮秒同步稳定性，能够测控 32 个量子比特。

图68. 微波信号可以对量子比特进行控制



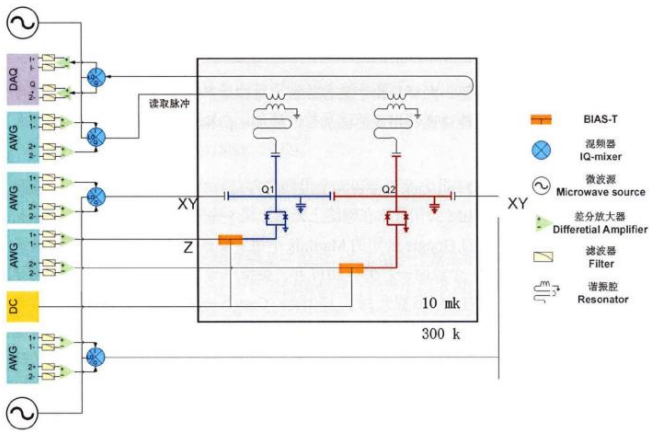
资料来源：达摩院量子实验室系列公开课，国投证券研究中心

图69. 本源量子 32 位测控一体机

资料来源：本源量子官网，国投证券研究中心

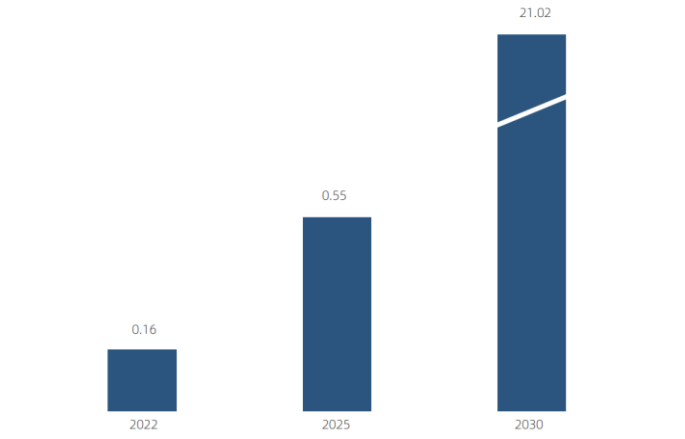
测控系统的价值量随着量子比特数的增加而增长。通常而言，一个 qubit 的 XY-control 操控和读取各需要用到 2 通道的 AWG 以及微波源，同时在读取侧还额外需要一台波形采集器用于读取谐振电路中输出的信号。因此测控设备市场规模的提升来自两大驱动力，首先是量子计算机台数的增长，其次是随着量子比特数量的增加，理论上测控设备的测控线路数也会相应增加。根据 ICV，2022 年全球量子计算测控系统市场规模为 1.60 亿美元，预计到 2025 年该市场总规模将达到 5.45 亿美元，2030 年达到 210 亿美元。

图70. 两比特超导量子计算操控系统电路模型简视图



资料来源：《超导量子计算室温电子学读出系统研究》徐昱，国投证券研究中心

图71. 2022-2030 年全球量子计算测控系统市场规模（10 亿美元）



资料来源：2023 全球量子计算产业发展报告-ICV&光子盒，国投证券研究中心

量子测控系统的主要供应商可分为测量仪器公司和量子计算机公司两大类。1）测量仪器厂商：全球的典型代表为罗德与施瓦茨（苏黎世仪器）、Keysight 等，国内厂商包括普源精电（耐数电子）、中电科 41 所、中微达信等。2）**量子计算机厂商：**典型代表包括了 Google、IBM、国盾量子、本源量子、国仪量子等。竞争格局方面，由于起步较早，罗德施瓦茨旗下的苏黎世仪器以及 Keysight 占据全球测控系统的绝大部分市场份额，但技术上看国内外公司基本处于同一起跑线。

图72. 布局测控系统的测量仪器公司

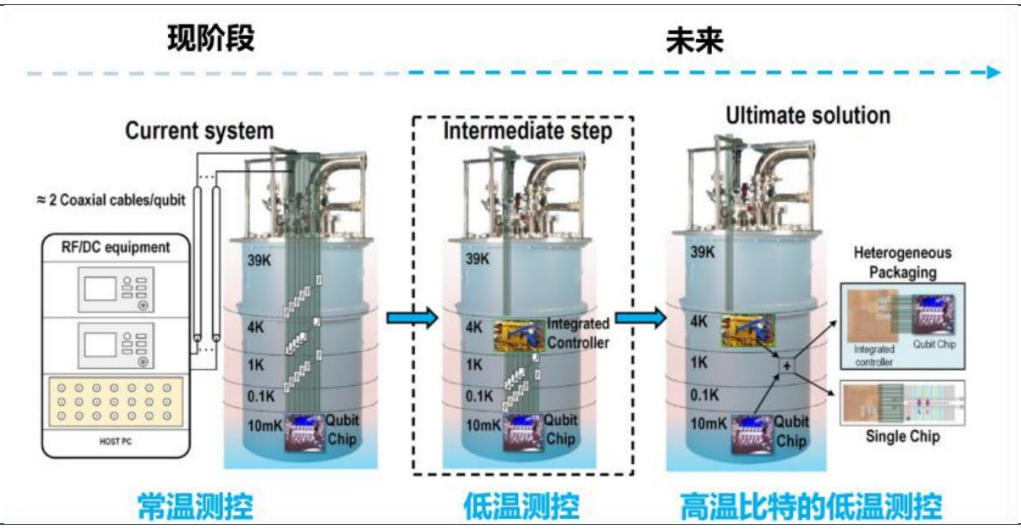
资料来源：Keysight、苏黎世仪器、思仪科技、中微达信、普源精电，国投证券研究中心

图73. 布局测控系统的量子计算机厂商

资料来源：国盾量子、本源量子、国仪量子，IBM、Google，国投证券研究中心

低温化和芯片化是测控系统未来的发展方向。由于处在室温环境中，现有的量子测控系统存在两大问题，其一是大量的线缆需要从室温连接到 10mK 的量子芯片，会带来热噪声，并影响量子门操作的保真度；其二是随着比特数的增长，控制线的数量会触及到稀释制冷机的功率与体积的天花板。为了解决这些问题，低温化和芯片化成为测控系统未来的发展方向，即把 DAC、RF、信号采集和处理电路均集成在一个芯片上，并将芯片置于低温环境中，从而提升性能。近年来，国际上有多款具备低温超导量子测控特征的测控芯片发布，相关厂商包括了英特尔、谷歌等。

图74. 量子计算测控系统发展趋势



资料来源：2022 全球量子计算产业发展报告-ICV&光子盒，国投证券研究中心

2.4. 量子计算应用：产业百花齐放，量子云平台构筑量超融合算力网

随着量子计算技术的飞速发展，其在多个领域的应用探索逐渐成为研究的热点。近年来，量子计算应用探索主要集中在量子模拟、组合优化和线性代数求解等领域。量子计算机在原子尺度直接模拟微观系统相互作用，可为物理化学、材料、医药等领域带来全新探索工具，近年来已成为研究热点。在涉及复杂多变量组合优化的量化金融、交通规划、气象预测等领域，量子计算应用探索也在广泛开展。量子机器学习通过构建新型数据处理模型，有望提升目前机器学习算法处理大数据的计算效率。

图75. 量子计算应用各场景评分等级（评分采用 5 分制，1 为最差，5 为最优）

	量子模拟			量子组合优化				量子线性代数		
行业领域	物理模拟	化学模拟	能源研究	金融	交通物流	航空	气象	密码学	金融	人工智能
应用场景	高能物理 核动力学 粒子物理	催化剂设计 材料研发 药物发现 靶向治疗	电池设计 固氮方法 碳捕获 太阳能转换	组合优化 模拟定价 风险预测	路线优化 货物装配	流体动力学 路线优化	气象预测 灾害预警	大数分解 密码破译	信用评分 欺诈检测	自动驾驶 机器学习 机器视觉
业界关注度	★★★★★	★★★★☆	★★★☆☆	★★★★☆	★★★☆☆	★★★☆☆	★★☆☆☆	★★★★★	★★★★☆	★★★☆☆
技术成熟度	★★★★☆	★★★☆☆	★★☆☆☆	★★★☆☆	★★★☆☆	★★☆☆☆	★★★☆☆	★★☆☆☆	★★★☆☆	★★☆☆☆
应用影响力	★★★★☆	★★★★☆	★★★☆☆	★★★★☆	★★★☆☆	★★★☆☆	★★☆☆☆	★★★★★	★★★☆☆	★★★☆☆

资料来源：中国信息通讯研究院，国投证券研究中心

从技术研发和成果落地看，量子计算技术在金融领域的应用已经取得实质性进展。2021 年 2 月，本源量子与建信金科联合推出国内首批量子金融应用——量子期权定价应用与量子 VaR 值计算应用，是国内金融领域对量子计算指数级加速能力的首次尝试，实现了国内量子金融算法 0 的突破。2021 年 3 月，英国剑桥量子计算公司（现已和霍尼韦尔 HQS 部门合并成 Quantinuum 公司）推出多个量子机器学习推理方法，在 IBM 量子计算机上实现贝叶斯网络的随机实例推理，在模拟金融时间序列的隐马尔可夫模型中推断市场条件波动。

量子机器学习逐渐成为研究和应用的热点，为解决复杂的人工智能问题提供了新的计算方案和思路。2023 年，各公司都在积极探索量子机器学习的新思路和新应用。量子计算和机器学习相结合，能够充分利用量子计算的优势解决传统计算无法处理的复杂问题。例如利用 VQNet 2.0 框架、CUDAQuantum 和 H100 NVL 等技术，研究人员实现了量子和经典计算资源的同时调度和优化，提高了机器学习的效率和性能，为解决复杂的 AI 问题提供了混合计算方案。

另一方面，当前量子计算与 AI 大模型的融合在当前阶段仍然面临着诸多的挑战和问题，如如何克服量子系统的噪声和不稳定性、如何适应不同类型的 AI 任务和数据、如何评估和验证量子计算在 AI 领域的优越性等。通过自然语言与 AI 进行交互，在解决问题和开发应用方面或许将有更多的可能性。目前的量子计算机仍然面临着错误率和噪声的问题，需要更稳定和可控的量子比特来支持大规模的机器学习任务。量子机器学习需要针对量子计算的特殊性质进行算法设计和优化，同时也需要简化和统一的编程框架来加速开发和应用。

表16：各公司量子计算机与人工智能结合进展

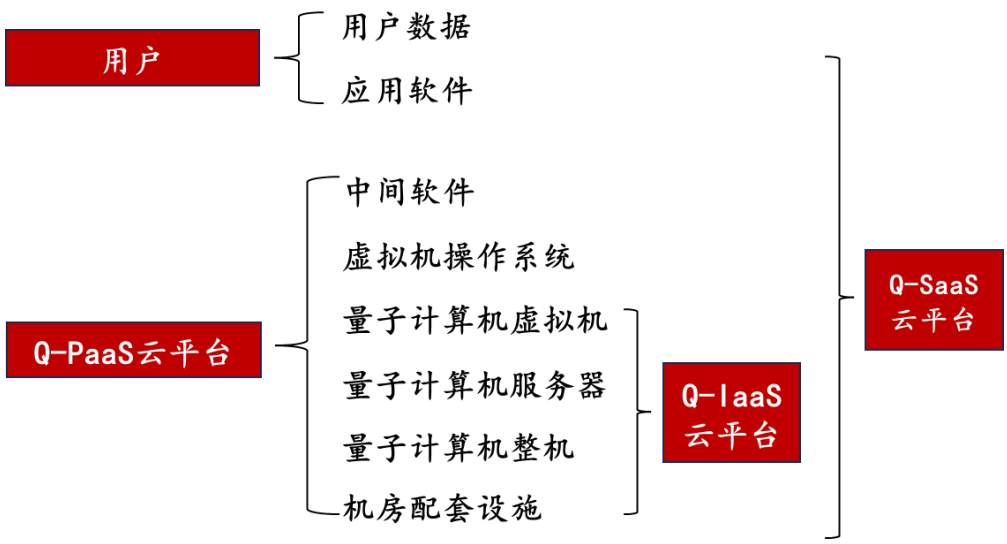
公司	量子计算机与人工智能结合进展
Google Quantum AI	谷歌与卢森堡大学以及 BIFOLD 合作，共同开发机器学习算法以处理复杂的量子系统。
rigetti	Rigetti 与 Moody’s 以及伦敦帝国学院合作，使用量子增强的数据转换和经典特征核方法相结合的机器学习技术，提出了解决经济衰退预测问题的新方法。
QUANTINUUM	Quantinuum 发布了量子自然语言处理工具λambeq 的更新版本 0.3.0，通过与 PennyLane 的集成，增强了功能和用户体验。
IONQ	IonQ 计划优化离子阱技术，增加量子比特数量和密度，并预测将在 2024 年实现量子机器学习的量子优势。

资料来源：光子盒公众号，信通院，国投证券研究中心

量子计算云平台作为一种创新的计算服务平台，推动了量子计算研究和应用的发展。量子计算云平台是依托云计算技术，提供用户接入实体量子计算机硬件或量子计算模拟器的一种服务平台，在平台上用户可以运行算法或进行实验任务。量子云平台为用户带来诸多便利，提供了更广泛的量子计算机接口，对发展量子计算研究有极大地推动作用。云计算是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问，进入可配置的计算资源共享池(资源包括网络、服务器、存储、应用软件、服务)，这些资源能够被快速提供，但只需投入很少的管理工作，或与服务供应商进行很少的交互。

当前各公司量子云平台的逻辑架构基本相同，与云计算分类相似。根据提供服务的类型不同将量子云平台提供的服务细分为量子基础设施即服务 QaaS、量子平台即服务 PaaS 和量子软件即服务 Q-SaaS 三种。部分量子云平台提供的量子计算服务包括其中的两种或三种，如 D-Wave 提供的服务类型包括 Q-IaaS 和 Q-Saas，本源量子和 IBM 包括了上述三种。

图76. 量子计算云平台服务类型



资料来源：光子盒公众号，国投证券研究中心

量子云平台好比连接量子计算机和用户之间的桥梁。用户使用经典计算机访问量子云，然后经由量子云将处理过的指令传输到后端，后端完成量子计算后经由量子云把结果输送给用户。通过量子云平台，即使不能实地使用量子计算机，用户也可以完成所需的量子计算。将量子资源部署在云平台上较一般的本地部署而言在如下方面具有其特殊的优势。

表17：量子云平台的优势及内涵

优势	内涵
较低的购置、运维和研发成本	从购置角度来看，量子计算机的硬件成本高，合适的零部件供应商少，制造难度高，导致配备量子计算机费用高昂。例如，一台超导量子计算机所需的稀释制冷机的价格一般为几百万至一千万人民币之间。全球能提供量子计算机整机的商业化公司极少。此外，量子计算机是国际最前沿的科学仪器，包括其核心硬件可能都在各国禁运或禁售的名单中。因此，量子计算机不仅供应量有限，而且购买难度很大。
	从运维角度来看，量子计算机运行条件苛刻，维护难度大。以技术相对成熟的超导量子计算机为例,计算机的运行除了需要一个接近绝对零度的运行温度外,一个安静稳定的环境和一定的放置空间也是必须的。BM、谷歌等科技公司尚且需要一个庞大的专业技术团队来维护和保证量子计算机的正常运行。而对于普通公司来说，一旦相关设备出现问题将很难解决。
	从研发角度来看，目前量子云平台面向的潜在用户有：量子软件开发者、量子算法研究者、高校教师学生、量子计算爱好者和化学、生物、金融等其他领域的公司。除部分研究机构需要真实量子计算机进行基础量子层面的相关研究外其他潜在用户的需求大多可以通过量子云平台上得到满足。部分量子云平台还可以根据客户的差异性需求提供开发对应软件的服务，这极大的降低了公司的研发成本。
较低的技术要求	当前量子计算软件开发困难。目前同时具备量子计算相关知识与软件开发技术的专业人员极为有限，即使对于未来量子计算有明确需求的化学、生物等行业的公司,从现在起就开始专门培养量子计算机工程师与量子开发人员对于人力资源也会是一种浪费。因而目前更多的选择是应用量子云平台来发展相关算法、软件以回避当前存在的技术人员缺乏问题

资料来源：光子盒公众号，国投证券研究中心

中美两国在量子计算云平台的布局和发展上呈现出各自的特点和优势，共同推动了全球量子计算技术的进步。美国量子云计算布局较早，发展迅速。我国量子计算云平台起步较晚，但发展态势良好，紧跟国际企业发展步伐，整体表现活跃，汇集了多家科技企业、初创企业和研究机构，为国内量子计算发展贡献支撑力量，与国际先进水平相比在量子处理器、量子计算软件方面的差距逐步缩小。

表18：美国量子计算云平台进展

时间	国家	进展
2017 年 3 月	美国	IBM Q Experience 首次发布量子计算 API
2019 年	美国	IBM 已推出 20 位量子比特的量子云服务，提供 QiKit 量子程序开发套件，建立了较为完善的开源社区
2019 年	美国	Google 开发了 Cirq 量子开源架构和 OpenFermion-Cirq 量子计算应用案例，可搭建量子变分算法，模拟分子或者复杂材料的相关特性
2019 年	美国	Regetti 推出量子计算云平台以混合量子+经典的方法开发量子计算运行环境，使用 19 位量子比特超导芯片进行无监督机器学习训练及推理演示，提供支持多种操作系统的 ForestSDK 量子软件开发环境。
2019 年	美国	微软推出量子计算云服务 Azure Quantum，可以与多种类型的硬件配合使用
2020 年 7 月	美国	Honeywell 发布 H0 的 6 量子比特离子阱计算原型机并提供云端访问接入能力，与多种量子软件框架兼容。
2020 年 8 月	美国	Amazon 发布 Braket 作为完全托管的 AWS 服务，可提供开发环境来帮助客户量子计算应用算法，灵活接入多家量子计算公司物理平台后端，也可使用 Amazon EC2 量子计算模拟器运行和验证算法。
2020 年 9 月	美国	D-Wave 发布 5000 量子比特系统 D-Wave Advantage，在 Leap 量子云平台中构建和运行量子混合应用程序，提供量子退火服务。
2021 年	美国	Honeywell 与 CQC 公司宣布合并，未来依托云服务提供更强的软硬件服务。
2021 年	美国	IonQ 与 Google 开源量子计算框架 Cirq 全面整合，提供多种量子软件框架对 IonQ 样机的访问。
2021 年 5 月	美国	Amazon 的 Braket 量子云平台提供完全托管的密度矩阵模拟器，可模拟最高 17 个量子比特的量子噪声路线。
2021 年 6 月	美国	IBM 宣布将其所有量子计算系统整合到了 Strangeworks 第三方量子计算云平台，用户可免费访问全部 28 项量子计算服务，包括 9 台免费量子计算机和 5 个托管模拟器，进一步提供 IBM Q Network 生态系统影响力。

资料来源：信通院，国投证券研究中心

表19：中国量子计算云平台进展

时间	国家	进展
2017 年 10 月	中国	阿里云与中国科学院联合发布量子计算云平台
2017 年 10 月	中国	本源量子上线量子计算云平台，搭建 32 位量子计算模拟机，目前还可提供基于自研超导量子芯片及半导体量子芯片的云平台接入访问。
2018 年	中国	华为宣布了由量子计算模拟器和编程框架组成的云平台
2018 年	中国	阿里与中科大联合发布量子计算云平台并在 2018 年推出量子模拟器“太章”。腾讯在量子 AI、药物研发和科学计算平台等应用领域展开研发。
2018 年	中国	华为发布 HiQ 量子云平台
2018 年 10 月	中国	华为发布了量子计算模拟器 HiQ 云服务平台及量子计算软件解决方案，基于 VQE 算法探索量子化学模拟应用场景
2018 年 2 月	中国	阿里云接入 11 比特超导量子计算服务
2019 年	中国	中科大与阿里云共同推出 11 位超导量子计算云接入服务。华为发布 HiQ 量子计算模拟云服务平台，可模拟泉镇抚的 42 位量子比特，单振幅的 81 为量子比特，并开发兼容 ProjectQ 的量子编程框架。本源量子推出的量子计算云平台可提供 64 位量子比特模拟器和基于半导体及超导的真实量子处理器，提供 Qrunes 编程指令集，Qpanda SDK 开发套件，推出移动端与桌面端应用程序，兼具可怕、教学和编程等功能，为我国量子计算的研究和应用推广提供了有益探索。
2020 年	中国	华为更新 HiQ3.0 量子计算模拟器及开发者工具，增加量子组合优化求解器和张量网络计算加速器。
2020 年	中国	百度发布量易伏量子计算云平台，实现 28 位量子比特的量子随机线路模型，并发布了基于百度开源框架 PaddlePaddle 的机器学习库，支持量子神经网络搭建与训练
2021 年	中国	北京量子信息科学研究院等研究机构爱是提供超导量子计算云平台，为量子算法和量子模拟研究提供实际物理平台后端的测试场景等。
2021 年 10 月	中国	百度发布了云原生量子集成开发环境 YunIDE。

资料来源：信通院，国投证券研究中心

全球量子计算云平台的竞争格局呈现出多元化的特征。近期，国内外众多研究机构和企业发布了不同类型的量子计算云平台，产业在迅速迭代。欧美如 IBM、Google、Microsoft、Amazon、AQT 等公司涵盖了多种量子计算技术路线，包括超导、离子阱、中性原子、光子。中国如华为、本源量子、国盾量子、中电信量子集团等公司也崭露头角，主要采用超导技术路线。

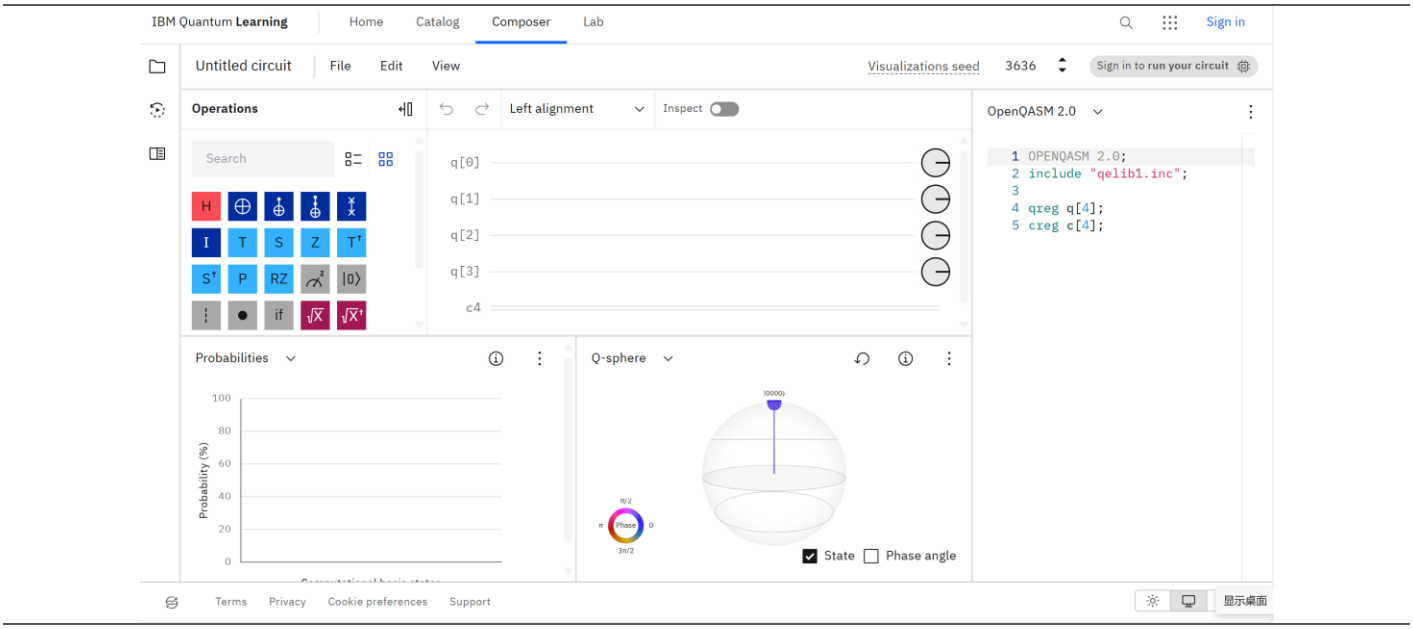
表20：全球量子计算云平台 2023 年进展

时间	机构	2023 年进展情况
2023.03	Microsoft Azure	首次实现量子计算和经典计算云中无缝集成。研究人员现在可以通过它开发将经典代码和量子代码混合在一起的应用程序，这些混合量子应用程序目前可在 Azure Quantum 云平台上 Quantinuum 公司的量子机器中运行。
2023.04	STRANGE WORKS	新的高级计算云平台正式上市，新平台增加了新的经典与量子启发式解决方案，还打转向该平台引入利用了人工智能技术的新工具，并即将推出测试版给用户使用。
2023.05	IBM Quantum	上线了具有 433 量子比特的 Osprey 量子处理器，并于 12 月上线了具有模块化可扩展性能的 133 量子比特 Heron 量子处理器。
2023.05	北京量子信息科学研究院	发布新一代量子计算云平台“QUAFU”，可访问包含 136 个、18 个和 10 个量子比特的超导量子计算芯片。
2023.05	国盾量子	与中科院软件所、中电科十六所、弧光量子等合作，推出量子计算云平台，将“祖冲之号”同款 176 量子比特（66 量子比特，110 耦合比特）量子计算机上云，配备图形及编程两种实验方式，引入多款国产编程语言，面向全球开放。
2023.06	IBM Quantum	IBM 的 127 量子比特 Eagle 处理器上线 Strangework 云平台，并作为现收现付系统的方式来提供。
2023.09	KAIST	开发并测试了一种纠缠见证电路，即使基于云的服务只允许对机器进行有限的控制，它也能证明纠缠。
2023.11	中电信量子集团	发布“天衍”量子计算云平台。该平台融合了“天翼云”超算及 176 量子比特超导量子计算能力，构建混合计算框架体系，支持量子算法与量子模拟计算等系列量子程序应用。
2023.12	IBM Quantum	将 Q-CTRL 的错误抑制技术（Q-CTRL Embedded）集成到 IBM 云量子服务中，用户只需轻轻开关，就能降低错误率。

资料来源：信通院，国投证券研究中心

IBM 在量子计算云平台领域扮演着举足轻重的角色。2016 年 5 月，IBM 推出了量子计算云平台 IBM Quantum Experience，用户可以通过该云平台在 IBM 的量子处理器上运行算法和实验，这是全球范围内量子计算云服务的开端。2021 年 3 月，IBM Quantum Composer 和 IBM Quantum Lab 取代了 IBM Quantum Experience。IBM Quantum Composer 是一个图形化的量子编程工具，允许用户操作来构建量子电路并在真实的量子硬件或模拟器上运行它们。而在 Quantum Lab 中，用户可以在 Jupyter Notebook 环境中编写结合 Qiskit 代码、方程、可视化和叙述文本的脚本，在真正的量子硬件或模拟器上运行代码，从任何地方存储、访问和管理文件。截至目前（2024.4.21），IBM 最受欢迎的软件包 Qiskit 下载量已超 669 万。IBM 全球网络架构比较灵活，主要分布在美洲、欧洲和亚太地区，其中，美国、德国、加拿大和日本已经部署量子计算机服务器，而韩国、西班牙即将部署量子计算机服务器。

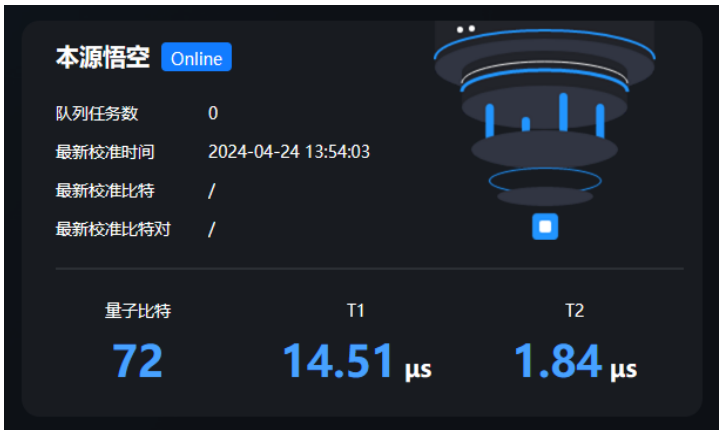
图77. IBM Quantum Composer 操作界面



资料来源：公司官网，国投证券研究中心

本源量子作为国内量子计算云平台的重要参与者，不断推动着相关技术的发展与前进。2017 年 10 月，本源量子联合中科院量子信息重点实验室发布基于半导体量子芯片的量子计算云平台，平台同时采用了超导量子芯片，包含一个最大支持 30 位的量子仿真器，实现国内首个图形化量子编程界面。该平台的一大突破是推出了全球首款半导体量子芯片编程语言“量子音符”，目的在于通过免费的云服务，扩大公众对量子计算的认知，并吸引更多的人使用量子编程语言参与开发应用。**2024 年 1 月 6 日，本源“悟空”正式上线运行。**该量子计算机搭载 72 位自主超导量子芯片“悟空芯”，有 198 个量子比特，其中包含 72 个工作量子比特和 126 个耦合器量子比特。根据官网，截至 3 月 25 日，已经获得了来自全球 115 个国家和地区超 428 万人次的远程访问，累计完成近 16.7 万个全球量子计算任务。

图78. 本源量子云平台提供的量子计算服务算力资源



资料来源：公司官网，国投证券研究中心

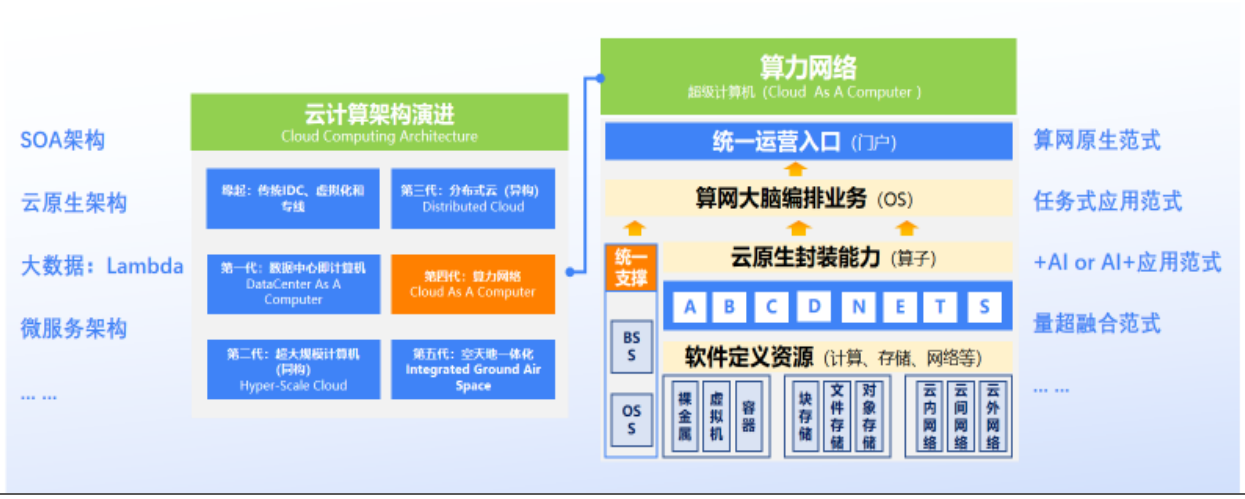
图79. 本源量子悟空超导计算机云平台操作界面 2024.4

资料来源：公司官网，国投证券研究中心

量子云平台技术日益成熟，量超融合算力网络或成为未来新形势。2023 年 8 月，中国计算机学会主办的第二届 CCF 量子计算大会暨量子计算产业峰会在合肥举办。中国科学院院士、中国科学技术大学教授郭光灿在接受采访时表示，量子计算机和超级计算机的“量超融合”可实现量子、经典算力互补，加快量子行业生态建设。

“量超融合”是指将量子计算和经典超级计算机协同工作，实现量子算力和经典算力异构融合。“量超融合”是量子计算-经典计算混合协作的新型计算架构。它将量子计算机的强大并行处理能力和超级计算机的高效数值计算能力结合，使得适合量子计算的任务得到量子加速，而其他任务则由超级计算机处理，从而大幅提升计算效率，也便于推动其在产业应用中不断迭代。根据具体应用算法的特点，量子计算可根本性加速其中的关键步骤，协同经典超级计算显著提高复杂问题求解效率，甚至是解算经典计算无法解算的难题。“量超融合”已成为算力发展的必然趋势。

图80. 云计算架构演进与算力网络



资料来源：本源量子官网，国投证券研究中心

中微达信开发全新融合计算测控单元，量超融合取得显著进展。2023 年 8 月，中微达信与信大协同开发，在国内首次推出适用于经典超级计算机、支持多路量子操控和读出的全新“量超协同”的融合计算测控单元，通过与经典计算单元的深度融合，可极大地降低经典-量子算力之间的协作延迟（降低百倍以上），且可实现分布式的量子测控，从而双向发挥量子计算机和经典超级计算机的各自优势，让量子计算与经典超算实现高效协同来完成异构计算任务。

图81. 中微达信经典+量子融合计算测控组件

资料来源：公司官网，国投证券研究中心

全球发力推动量超融合技术发展，政策和项目陆续出台，其中欧洲多个超算中心已开展了量子-经典计算系统的研发。2022 年 1 月，**法国**政府宣布启动全国量子计算平台，将以 CEA 运行的超大型计算中心（TGCC）为载体，与传统计算机系统和量子计算机交互操作，平台将供国际社会的研究机构、初创企业和行业合作伙伴使用。

西班牙：巴塞罗那超级计算中心（BSC）为研究基于张量网络的大规模量子电路开发了一个高性能计算机群(HPC)模拟器，提出使用机器学习工具对混合量子-经典电路进行算法优化。应用小型量子电路的优化来研究凝聚态系统的物理特性，并计划安装量子硬件以开发真正的混合-量子计算的系统。

德国：尤利希超级计算中心（JSC）和莱布尼茨超算中心（LRZ）均已将量子计算纳入中心业务，2022 年 1 月，尤利希超级计算中心（JSC）购入的 D-Wave 量子退火机已投入使用，为德国（以及欧洲地区）的研究人员们提供基于云端的各种量子系统的访问权限。2021 年 3 月，莱布尼茨超算中心（LRZ）成立了量子集成中心(QIC)，以进一步开展混合量子-经典系统的集成研究，并向法国 Atos 公司订购了量子学习机，同英特尔密切合作，以提高量子系统的扩展性。

美国：2023 年，美国国家超级计算机应用中心与 NVIDIA 合作，开发新的混合量子计算资源。2024 年 2 月，Rigetti 宣布将和英国的量子纠错技术公司 Riverlane 一起参与由美国能源部橡树岭国家实验室(ORNL)领导的一个项目，该项目旨在探索将量子计算机集成到大型超级计算机中心所面临的挑战。

中国：2024 年 3 月，国务院总理李强在《政府工作报告》中提到，“适度超前建设数字基础设施，加快形成全国一体化算力体系，培育算力产业生态”。安徽省在量超融合方面走在前列。2023 年 10 月，安徽合肥开建超量融合计算中心，部署了 2 台超导量子计算机和 1 台离子阱量子计算机。2024 年 4 月，本源量子、国盾量子、国仪量子中标合肥超量融合计算中心招标项目。

2023 年 12 月，安徽省数据资源管理局印发《安徽省数字基础设施建设发展三年行动方案（2023—2025 年）》，此次《行动方案》的发展目标明确指出，布局量子信息基础设施，其中量子通信网的节点数，将从 2022 年的 180 个提升至 2025 年的 350 个。除推动量子通信网络建设及其在多领域的应用外，《行动方案》还将推动量子计算的研究和应用进展，协同攻关解决卡脖子问题，开展超量融合与量子计算云服务等。

本源量子和上海超级计算中心合作，在国内开拓“量超融合”的先例。二者通过合作积极探索量子计算机和经典计算机融合，更好地服务产业发展（上海超级计算中心是是国内首家面向全社会开放的高端计算平台，由“魔方 III”（峰值计算速度 3400TFlops）和“魔盒”（峰值计算速度 100PFLOPS@FP16）两台超级计算机对外提供高性能计算和人工智能计算服务。

图82. 上海计算中心超级计算机“魔盒”和“魔方 III”

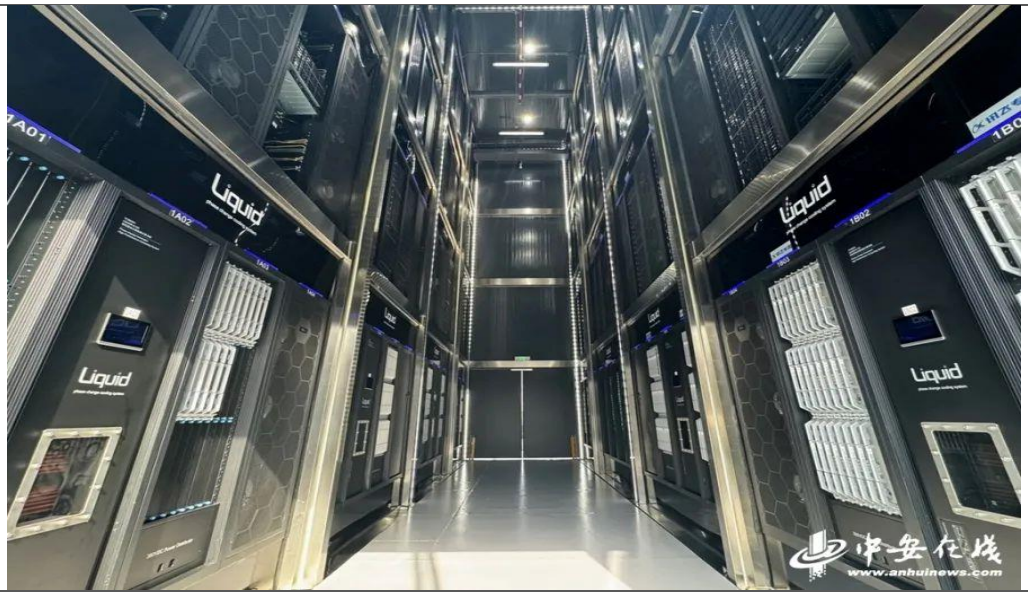
魔盒技术指标	
峰值速度	100PFLOPS@FP16
节点数	40
CPU	Kunpeng920，160块
GPU	Ascend910，320张
系统内存	30720GB
存储系统	3950TB对象存储
网络互联	训练节点间互联带宽800GE
算法框架支持	MindSpore 2.1.0、TensorFlow 1.15.0、PyTorch 1.11.0、自定义镜像

魔方III技术指标	
峰值速度	3400TFlops
计算节点	1120台双路CPU刀片 16台GPU节点（V100）
CPU	Intel Xeon 6142（16 core/2.6GHz）
GPU	Nvidia Tesla V100 GPU卡
系统内存	215TB DDR4内存
存储系统	ParaStor300并行存储系统，裸容量超过8P
网络互联	100Gb Intel Omni-Path 高速计算网络

资料来源：公司官网，国投证券研究中心

巢湖明月超级计算机项目计划与量子计算机深度融合，安徽推动量超融合计算迈出重要步伐。安徽从 2022 年起开始筹划如何让代表下一代先进计算能力的量子计算机，与超级计算机巢湖明月‘合体’，深度融合量子计算与超级计算。量超融合项目将在巢湖明月超级计算机基础上，部署 3 台量子计算机，包括 2 台超导量子计算机，1 台离子阱量子计算机。同时安装配套量子计算机操作系统和量超融合计算云平台，并开发相应的算法软件。本源量子将提供一台“本源悟空”超导量子计算机、一套超量融合系统及相应配套的软硬件设施的建设，国盾量子将提供一台超导量子计算机、超量融合系统及相应配套的软硬件设施，国仪量子将提供一台离子阱量子计算机、超量融合系统及相应配套的软硬件设施的建设。

图83. “巢湖明月”超级计算机

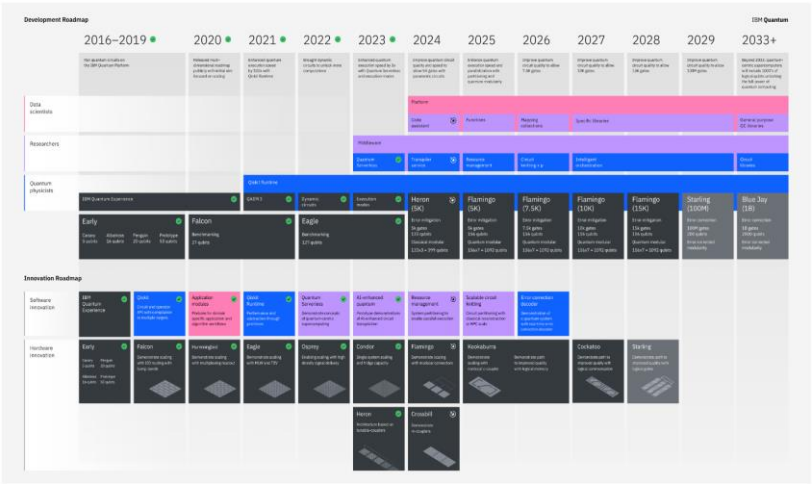


资料来源：公司官网，国投证券研究中心

2.5. 量子计算展望：科技巨头明确发展路线图

在 IBM 2023 Think 大会上，IBM 推出更新后的量子计算路线图。IBM 作为经典计算机产业的核心企业，希望在新一代量子计算产业中继续稳固其地位。IBM 拥有优秀的微纳加工的技术，因此在量子计算系统物理实现的路线上选择了超导量子技术。如今，IBM 的量子计算机 Quantum System One 不仅部署在美国，还部署到了德国和日本。无论是前沿技术研究还是产业化发展，IBM 都是拥有完整量子计算机生态体系的“蓝色巨人”。

图84. IBM Roadmap



资料来源：IBM 官网，国投证券研究中心

表21：IBM 路线图解读

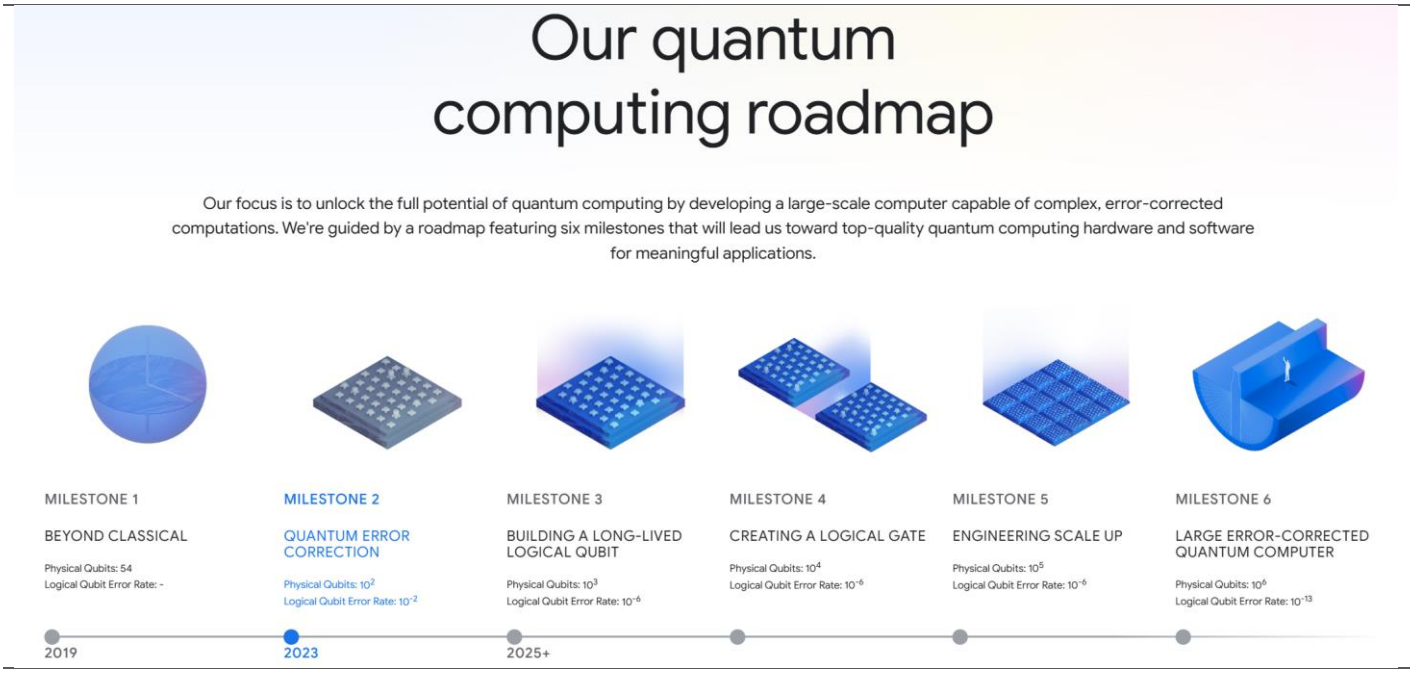
时间节点	阶段特点	相关内容
2023	100+quibts	◘ 推出 Condor 处理器，实现 1121quibts（错误率较高） ◘ 推出 Eagle 处理器，实现 127quibts ◘ 提前推出 Heron 处理器，实现 133quibts （133*3）（Heron 在 2023 年 12 月发布，领先 Development Roadmap 进度）
2024	100+quibts	◘ Heron 处理器将能运行 5,000gates ◘ 推出 Flamingo 处理器，实现 156quibts （将 2022 年 Roadmap 中的 1386+quibts 更改为 156*7quibts） ◘ 推出 Crossbill 处理器，实现 408quibts（将 2022 年 Roadmap 中预计 2025 发布提前至 2024 年发布）
2025 - 2026	1000+quibts	◘ Flamingo 处理器将逐步实现 5000gates、7500gates 运行 ◘ 推出 Kookaburra 处理器，实现 1386quibts（2023 年 Roadmap 明确为 1386*3quibts） ◘ 实现以量子为中心的超级计算机
2027	1000+quibts – 10,000gates	◘ Flamingo 处理器将实现 10,000gates 运行 ◘ 推出 Cockatoo 处理器
2028 - 2029	200quibts – 100milion gates	◘ Flamingo 处理器将实现 15,000gates 运行 ◘ 推出 Starling 处理器，实现 200quibts，运行 100milion gates （将 2022 年 10k-100kquibts 明确为 200quibts）
2030+	2000quibts – 1bilion gates	◘ 推出 Blue Jay 处理器（属于 100,000-quibts system），将实现 2,000quibts 系统，运行 1bilion gates ◘ 预计将于 2033 年实现 100,000 量子中心超级计算机

来源：IBM 官网，国投证券研究中心

谷歌量子计算路线图明确了 6 个重要节点。谷歌在人工智能、机器学习、深度学习领域引领了一个时代，在新的量子时代，谷歌希望延续引领技术革命。谷歌量子计算项目创立于 2006 年，最初专注于软件。2014 年，谷歌与加利福尼亚大学圣塔芭芭拉分校 John Martinis 教授团队合作研究量子计算硬件，该团队于 2019 年成功以名为“悬铃木”的处理器构建的量子计算系统实现了其宣称的“量子霸权”(quantum supremacy)。2021 年 5 月，谷歌建成了新的量子人工智能园区(Quantum AI Campus)，园区包括其第一个量子数据中心、量子硬件研究实验室和量子处理器芯片制造设施。

路线解读来看，谷歌将构建实用化量子计算机的道路划分成了六个步骤：量子计算优越性是第一步；2023 年验证量子纠错码性能随着编码规模增加而增强是第二步；它的终点（第六个步骤）预计是到 2029 年，由一百万个物理量子比特实现可纠错的量子计算。

图85. Google Roadmap

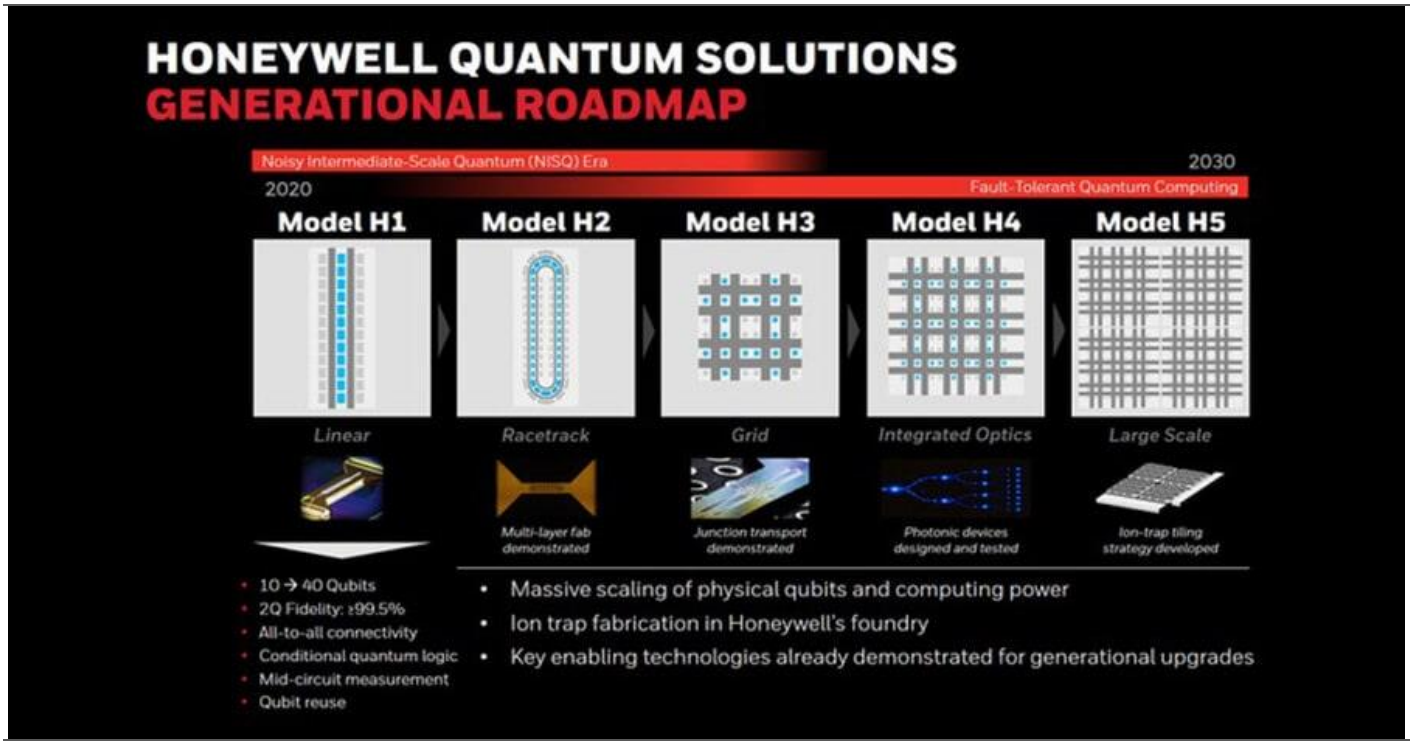


资料来源：公司官网，国投证券研究中心

霍尼韦尔发布 10 年量子计算路线图，向商业化迈进。霍尼韦尔是总部位于美国的财富 100 强科技巨头,业务涉及航空、建筑技术、高性能材料、安全和生产解决方案等领域。霍尼韦尔目前拥有一支由 150 多名科学家、工程师、软件开发人员和功能专业人士组成的跨学科团队，致力于推进量子计算和解决跨行业的实际企业问题。2021 年 6 月，霍尼韦尔和剑桥量子计算(COC)公司宣布组建新的独立量子计算公司，预计于 2021 年第三季度完成合并。霍尼韦尔量子计算系统采用离子阱技术，是离子阱技术路线的佼佼者。2020 年 6 月，霍尼韦尔发布了量子计算系统 Model H0，四个月后发布了 Model H1 保持实验测得的最高量子体积(QV1024)记录。霍尼韦尔建立了很多合作伙伴关系共同推进量子计算产业化应用，包括摩根大通、默克、DHL、宝马、新日铁、三星等。

路线解读来看，在霍尼韦尔的未来十年整体量子路线图中，其计划从 10 个量子比特到 40 个量子比特，并向下一代容错、可大规模部署的设备迈进。霍尼韦尔还表示，量子计算路线图表现了其对于量子业务实现商业规模的信心，霍尼韦尔将会基于云服务模式，为企业客户提供使用霍尼韦尔现有最先进系统。

图86. Honeywell Roadmap

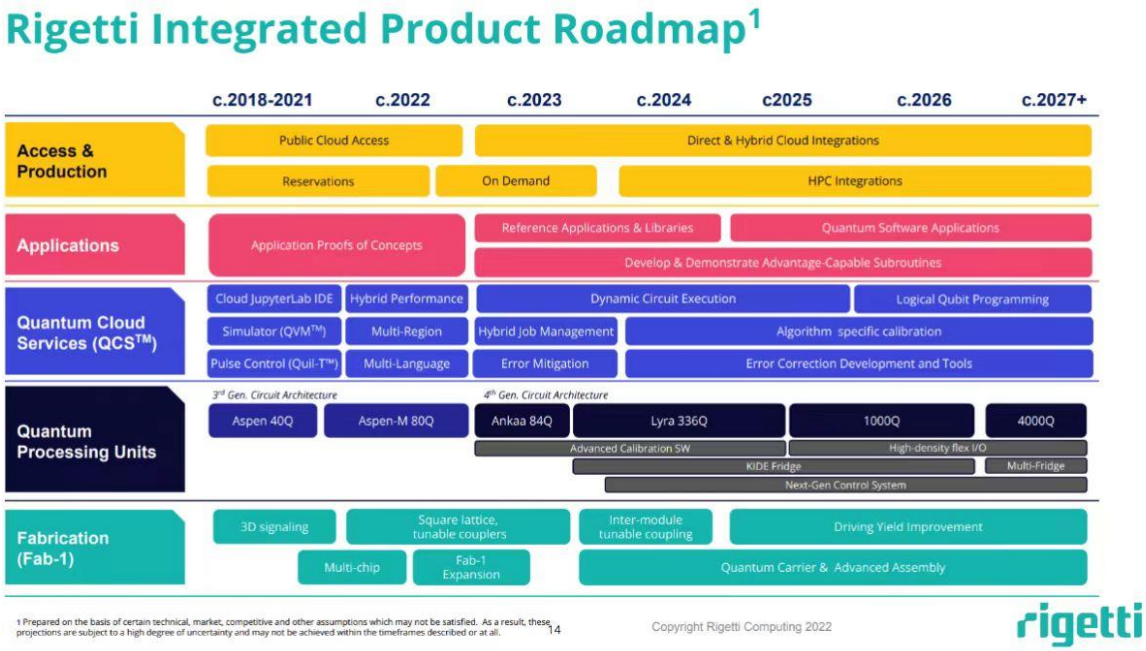


资料来源：公司官网，国投证券研究中心

Rigetti 的量子计算路线图体现其实现“量子优势”这一目标的决心。Rigetti 是一家美国的量子计算初创公司,创立于 2013 年,创始人 ChadRigetti 是一位物理学家，曾在 IBM 从事量子计算机工作。Rigetti 自主开发超导量子处理器(QPU),公司还开发了 Forest 量子编程框架,使程序员能够编写量子算法，并且提供量子云服务(QCS)，其机器可以集成到任何公有云、私有云和混合云中。2017 年，Rigetti 的 Fab-l 工厂投入使用，是世界上第一家商用量子集成电路晶圆厂。

路线解读来看，2025 年推出 1000+量子比特的处理器 QPU， 2027 年推出 4000+量子比特的处理器 QPU。这两个 QPU 由多个 84 量子比特芯片组成，在载体衬底上组装更多的芯片，可能达到几十个。为了实现更高的量子比特数量，4000+QPU 将会利用多个制冷机，这很可能是一种分布式量子计算机。尽管 Rigetti 预计在此期间不会增加 Ankaa 芯片上的量子比特数量，但他们很可能会在随后的修订中继续完善它，以便在门保真度、相干时间和其他参数方面提供持续改进。他们还需要实现更大的稀释制冷机，改进 flex I/O，并为这些更高的容量提供下一代控制系统。

图87. Rigetti Roadmap



资料来源：公司官网，国投证券研究中心

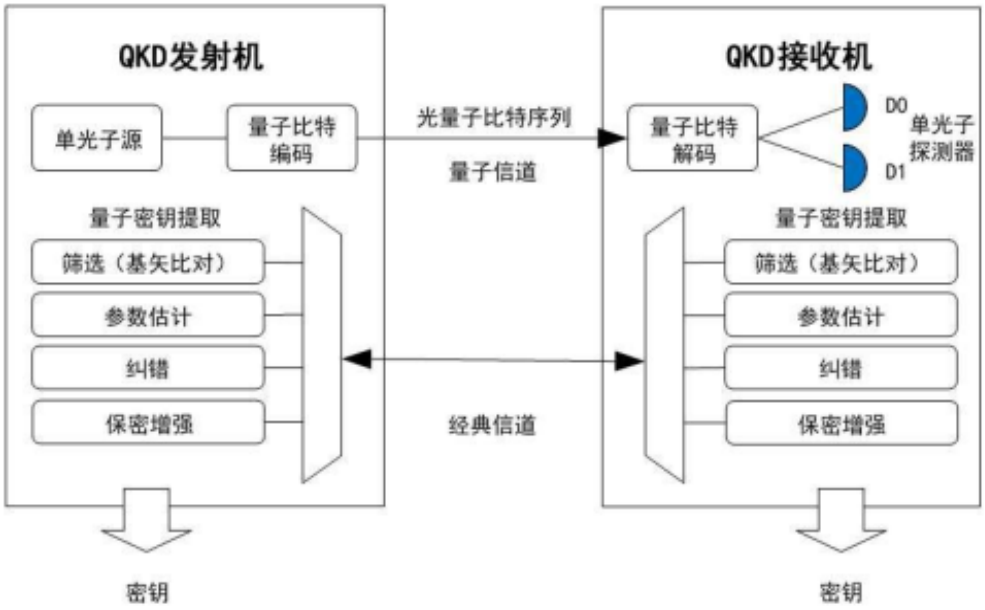
3. 量子通信：量子技术实现密钥分发，信息安全的坚固之盾

3.1.量子通信原理：利用量子技术实现密钥分发

传统基于 RSA 算法的密钥分发过程在量子计算时代存在安全风险。当前在通信加密的过程中，经常采用基于非对称加密的算法如 RSA 实现身份认证和后续的对称加密密钥分发。这一技术构成了当前数字签名的基础。而在量子计算时代，由于 Shor 算法利用量子傅里叶变换和叠加态的原理，可以实现对大数质因数分解的指数级加速，从而在密钥分发环节，基于传统 RSA 算法的密钥分发和数字签名技术，在量子计算时代存在较大的安全风险。

量子保密通信应运而生，实现量子形态的密钥分发。量子密钥分发是一种通过量子力学原理实现加密通信的方法。在量子密钥分发中，发送方利用量子纠缠的特性，向接收方发送一串随机的单光子，接收方通过测量这些光子的状态，可以得到一串随机数，这就是密钥。由于量子纠缠的特性，任何试图窃取信息的第三方都会导致量子态的崩溃，因此这个过程是绝对安全的。接收方利用这个密钥进行加密和解密，从而实现保密通信。目前，量子密钥分发已经被商业化并在实际应用中发挥了作用，例如金融、政府和军事领域。

图88. 量子密钥分发设备示意图



资料来源：国盾量子招股说明书，国投证券研究中心

BB84 协议保障量子密钥分发过程，目前成为业界共识。BB84 协议是一种量子密钥分发协议，由 Charles H. Bennett 和 Gilles Brassard 在 1984 年提出,是目前被广泛应用于量子密码学领域的一种协议。简要来说，**BB84 协议操作过程中同时利用了量子信道和经典信道：**

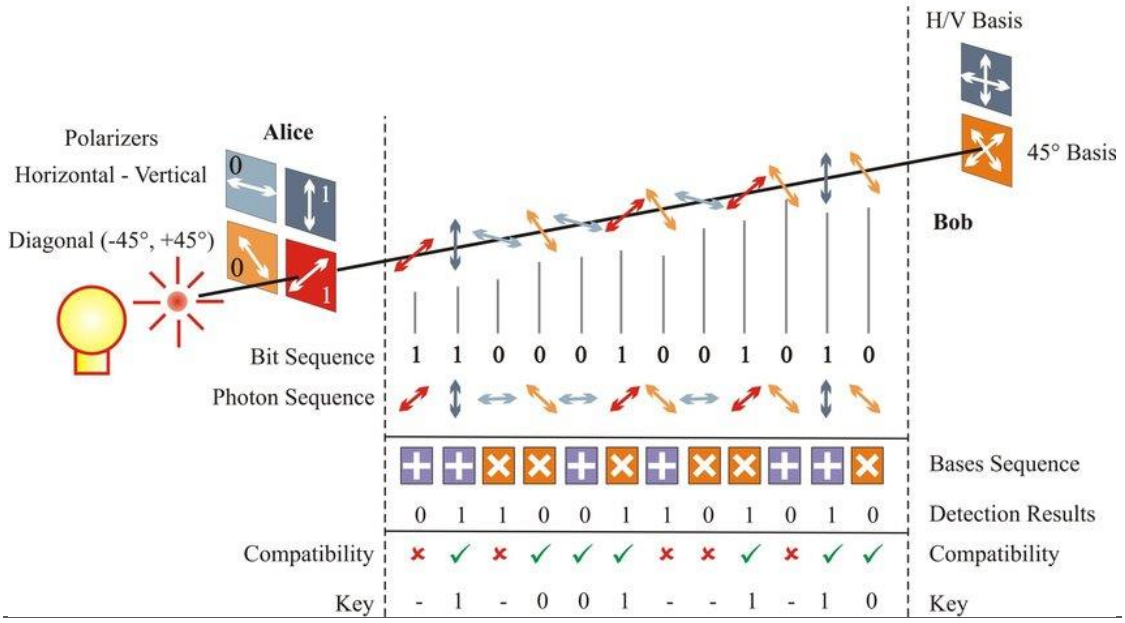
在**量子信道部分**：1）Alice 发送随机的量子比特串给 Bob。Alice 随机选择四种偏振片，制备不同偏振状态的光量子，得到足够多的随机量子比特并将其发送给 Bob；2）Bob 随机选择测量基测量量子比特。由于 Bob 并不知道光量子是由发送端那一种测量基编码的，所以他也只能随机选择测量基来进行测量。当选择正确的测量基时，测量的结果正确。当使用错误的测量结果时，测量结果错误。

在经典信道部分：3）Bob 将使用的测量基发送给 Alice；4）Alice 将接收的测量基与使用的测量基进行比较，并通过信息告诉 Bob 哪些位置的测量基是正确的；5）Bob 根据 Alice 的消息剔除错误的量子比特，并将选择少部分正确的测量结果告诉 Alice；6）Alice 确认 Bob 测量结果的正确性。若错误，则说明存在量子信道可能存在窃听，停止通信或者返回第 1）步（由于实际的量子信道中也存在噪声，因此会根据一个错误率阈值判断是否窃听和停止通信）。若正确，剔除部分的量子比特，剩下的二进制串作为最终的密钥。并发送确认信息给 Bob。7）Bob 收到确认信息。同样剔除部分的量子比特，剩下的二进制串作为最终的密钥。

如果 Eve 在量子信道中旁路窃听，由于量子不可克隆，因此 Eve 无法复制出一份相同的量子比特副本；如果他在量子信道中直接测量光量子，由于 Eve 不知正确的测量基，他也会随机选择，有 50%的概率选择正确，50%的概率选择错误。若选择的测量基错误，测量结果错误，同时光量子的偏振态发生改变。当协议的步骤由 2）执行到 6）时，Alice 将发现到量子信道的窃听，那么她将终止这一过程。

如果在经典信道进行窃听，实际上也是无效的。即使 Eve 知道了测量基信息（步骤 3），然而由于量子不可克隆，无法得到正确的量子比特串副本。由以上分析可知，BB84 协议基于量子不可克隆等原理，实现安全的密钥分配过程。

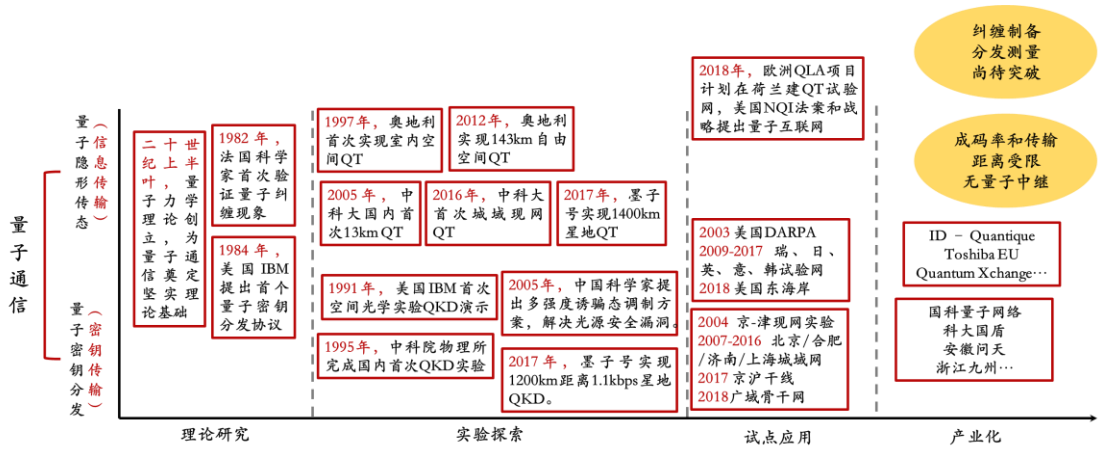
图89. 量子密钥分发 BB84 协议示意图



资料来源：《Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing》，国投证券研究中心

量子保密通信从理论探索转向实际应用，逐渐进入产业化成熟期。自 1984 年 BB84 协议的提出为量子密钥分发奠定了理论基础以来，量子通信领域经历了多个重要的发展节点。从 1989 年首个量子密钥分发实验的成功，到 2016 年中国“墨子号”量子科学实验卫星的发射，再到京沪干线的建成，每一步都标志着量子通信技术的进步和实用化。特别是 2021 年构建的超 4600 公里的量子通信网络，不仅展示了量子通信技术的巨大潜力，也为未来全球广域量子通信网络的形成奠定了基础。这些发展不仅彰显了量子通信技术的科学价值，也突显了中国在这一领域的领先地位。随着技术的不断进步，量子通信有望在全球范围内实现更广泛的应用，为通信安全提供强有力的保障。

图90. 量子通信技术发展历程



资料来源：信通院《量子信息技术发展与应用研究报告 2018》，国投证券研究中心

3.2.量子通信产业链：QKD 是核心设备，关基行业率先落地

量子通信产业上游：芯片+光源+单光子探测器+量子随机数发生器，多种核心器件构筑产业上游。量子通信的核心器件与材料的涵盖囊括了关键的技术组成部分。首要的是先进的量子芯片技术，作为整个产业链的基础，包括数据处理类芯片、电学芯片和光学芯片。光源则成为量子通信不可或缺的关键组件，作为载体，经过对其量子状态的调制操作后，可携带量子信息在不同通信节点间中进行信息传输和共享。在通信接收端，单光子探测器发挥着至关重要的作用，确保对量子信息的精准检测。量子随机数发生器是保障通信不可预测性的关键工具。此外，其他核心器件如 PPLN（周期极化铌酸锂）晶体、PPLN（周期极化铌酸锂）波导、光纤光缆等元件同样在上游产业链中发挥着关键作用。这些核心器件和材料为量子通信与安全产业链的上游提供了创新动力，为实现更安全、更高效的量子通信系统奠定了坚实基础。

表22：量子保密通信上游产业及主要公司

技术	基本情况	部分公司
芯片	数据处理芯片为 FPGA（现场可编程门阵列）芯片通过编程，可以成为实现任意功能的器件。电子学芯片在量子通信中也有所使用，包括模拟信号处理芯片、数模/模数转换芯片（DAC/ADC）、射频芯片、存储芯片等。光学芯片通常指集成了光学功能的芯片，如光波导、光学传感器等。	XILINX LATTICE SEMICONDUCTOR ALTERA 国盾量子 QuantumCTek
光源	光源是产生光子的器件或设备，是实现基于量子物理的安全通信的基本元素。不同技术路线下对光源可能有不同的需求，激光器是一种常见的光源的设备。	QD LASER QUANDELA 国盾量子 QuantumCTek aegiq
单光子探测器	单光子探测器可以检测单个光子的信号强度，并将光信号转换放大为电信号。在量子通信中，主要探测可见光到近红外光波长范围的光信号，探测范围一般在 400 纳米到 1310 纳米之间。半导体探测器和超导探测器是两种常见的单光子探测器类型。	Princeton Lightwave 国盾量子 QuantumCTek PHOTEK QUDOOR 启科量子
量子随机数发生器	量子随机数发生器（QRNG）已成为商业产品，是 QKD 设备中的核心部件。产品成熟度不断提升，从成本角度来看，已可具备了替代经典随机数产品的能力。	IDQ 国盾量子 QuantumCTek QUDOOR 启科量子 quantum motion
其他	晶体：主要用于生成和调制用于传输量子信息的光子。 光纤光缆：光纤光缆是量子通信中所使用的一种传输介质，低损耗光纤可有效提升量子通信的通信距离和通信速率。	iXblue 极量科技 NKT Photonics 亨通光电

资料来源：ICV《2024 量子通信与安全产业发展展望》，国投证券研究中心

量子通信产业中游：核心设备+网络建设集成+保密网络运营，共同构筑产业链中游。核心设备涉及到关键的量子通信设备，如 QKD 设备、组网设备和网络管理软件平台，这些设备确保信息的安全传输。网络建设集成用于构建高效、安全的量子通信网络，例如中国的国家骨干网、省骨干网以及城域网。保密网络运营则包括各运营商参与其中，推动量子通信技术的日常运行与维护。整个中游通过设备、网络建设和运营的协同作用，为量子通信与安全的发展提供支撑，为实现更安全、高效的通信提供了关键保障。

量子通信产业中游：量子通信厂商+运营商+运维商，三大玩家参与市场竞争。中游的参与者有国盾量子、国科量子等量子通信公司，因为目前有能力承担量子通信网络建设的公司数量还较少，有很多公司在成立之时便获得了更多的机会，未来业务可以能会细分或剥离，但也可能成为大型、全面的公司。此外，参与者还有移动、联通和电信三大网络运营商以及神州信息、中国有线和中国卫星通信集团等传统运维商，以及亨通光电和中信国安等建设运维商等。

表23：量子保密通信产业中游及主要公司

技术	基本情况	部分公司
核心设备	主要包括量子密钥分发（QKD）设备、组网设备和网络管理软件平台。QKD 设备的商业化产品当前主要为 DV-QKD（离散变量量子密钥分发）和 CVQKD（连续变量量子密钥分发）两大类。组网设备和网络管理软件平台包括信道交换类、数据处理类及网络管理软件平台。	IDQ、国盾量子、问天量子、TOSHIBA、QUDOOR 启科量子、ThinkQUANTUM
网络建设集成	全球大部分 QKD 网络建设依托现有光纤通信网络，通过选择一些合适的点位，在机房中布设 QKD 发送端和接收端设备。	中电信量子集团、SPEQTRAL、量子网络 QUANTUMNET、QUANTUMXCHANGE
保密网络运营	运营层主要负责管理和协调整个量子网络的运作。这包括监控网络状态、调度量子信号的传输、维护网络安全性和稳定性。在运营层，重要的工作还包括处理密钥管理和分发、优化网络资源分配以及故障检测和响应。	中国电信、中国移动、China Unicom、SK telecom、orange、Telstra

资料来源：ICV《2024 量子通信与安全产业发展展望》，国投证券研究中心

量子通信产业主要产品和设备：量子保密通信产业主要由量子光源、单光子探测器、量子密钥分发设备、量子安全路由器、量子交换机、量子随机数发生器、量子卫星地面站、移动加密产品等收发设备构成。

量子光源：在量子通信中，量子信号起着重要作用，而量子信号的编码、传输和检测等技术都依赖于信号的量子特性，因此，量子通信技术的实现必须获得稳定可靠的量子光源。量子光源主要分为：单光子光源、连续变量光源和纠缠态光源。其中，连续变量光源又分为相干态光源和压缩态光源；纠缠态光源又分为光子对纠缠和多光子纠缠。

图91. 量子光源

资料来源：ICV《2022 全球量子通信产业发展报告》，国投证券研究中心

单光子探测器：单光子探测器是一种超低噪声器件，增强的灵敏度使其能够探测到光的最小能量量子光子。单光子探测器可以对单个光子进行探测和计数，在许多可获得的信号强度仅为几个光子能量级的新兴应用中，单光子探测器发挥重要作用。在生物光子学、医学影像、非破坏性材料检查、国土安全与监视、军事视觉与导航、量子成像以及加密系统等领域有广泛应用。

图92. 单光子探测器

资料来源：ICV《2022 全球量子通信产业发展报告》，国投证券研究中心

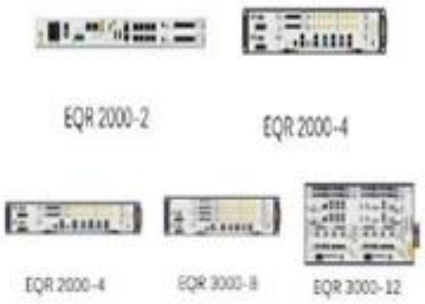
QKD 设备：量子密钥分发（QKD）是量子保密通信的核心产品。负责量子密钥的产生和分发。QKD 设备的研制门槛较高，全球仅少数研发团队能够提供，例如国盾量子、问天量子、启科量子、IDQ 等。

图93. QKD 设备

资料来源：ICV《2022 全球量子通信产业发展报告》，国投证券研究中心

量子安全路由器：量子安全路由器作为量子保密通信解决方案中的核心应用设备，将量子密钥与经典网络设备融合，同时实现了经典通信的加密和路由交换功能，为用户搭建端到端电信级稳定、高速的量子加密应用网络。

图94. 量子安全路由器



资料来源：ICV《2022 全球量子通信产业发展报告》，国投证券研究中心

量子交换机：光量子交换机设备用于实现量子信道时分复用，是量子密钥分发网络组网的重要产品。光量子交换机系列产品包括两种不同类型的光量子交换设备，矩阵型光量子交换机和全通型光量子交换机。矩阵型光量子交换机采用交叉式光纤链路交换，该类型的光量子交换机多用于量子密钥中继内部，实现密钥分发终端的扩容与备份；全通型光量子交换机支持多通道光纤链路连接，每个通道与其他通道间均可实现互连，适用于多用户量子保密通信局域网或城域网络。

图95. 量子交换机

资料来源：ICV《2022 全球量子通信产业发展报告》，国投证券研究中心

量子计算机发生器：随机数是影响通信安全和通信系统可靠性至关重要的因素。随机数是由随机数发生器产生的，随机数发生器可以分为三类：伪随机数发生器、基于经典物理和物理随机数发生器和基于量子物理的量子随机数发生器。与前两类相比，量子随机数具有真正的不可预测性。目前主要量子通信公司几乎都在开发量子随机数发生器。

图96. 量子随机数发生器

资料来源：ICV《2022 全球量子通信产业发展报告》，国投证券研究中心

量子卫星地面站：在星地量子密钥分发中，地面站起到了接收卫星数据的作用。随着技术快速进步，量子卫星地面站已经实现了可移动和小型化。该小型化量子卫星地面站是国盾量子与中国科学技术大学合作研发的具有完全知识产权的卫星 QKD 地面站产品。该系列产品基于卫星平台自由空间量子通信技术，在原墨子号地面站光机系统的经验基础上设计改造，将原有地面站光机系统的大、重、不可移动，需远离城市背景光，转变为现在的口径小、重量轻、体积小，可快速移动部署，适应城市背景光，能够实现精确捕获跟瞄量子卫星，实现量子信号高效耦合。

图97. 量子卫星地面站

资料来源：ICV《2022 全球量子通信产业发展报告》，国投证券研究中心

移动加密应用产品：随着量子技术的不断发展，相关量子通信产品已经逐渐走向普惠消费者，特别是移动加密应用产品，包括量子安全服务移动平台、量子安全 U 盾、量子安全加密卡产品、量子密钥充注机、量子安全手机等。

图98. 移动加密应用产品

资料来源：ICV《2022 全球量子通信产业发展报告》，国投证券研究中心

量子通信产业竞争格局：参与厂商较为多元，共同推进量子产业发展。量子保密通信产业链的主要市场玩家呈现出多元化的竞争格局。随着技术的不断发展和市场的逐步成熟，各方将在技术创新、产品研发、应用推广等方面持续展开竞争和合作，共同推动量子保密通信产业的发展。

核心器件方面，国盾量子、问天量子等国内企业具有较为明显的优势，已成功研发出多种量子保密通信核心器件，并在国内外市场占据一定份额。此外，欧美企业如 ID Quantique、Quantum Xchange 等也在核心器件领域具有较强的竞争力。

系统集成方面，中国电信、中国移动、中国联通等国内大型通信企业，以及华为、中兴等通信设备制造商，在量子保密通信系统集成方面具有较强实力。这些企业具备丰富的网络建设经验和客户资源，有助于推动量子保密通信技术在实际应用中的落地。

网络建设方面，量子保密通信网络建设主要依赖于国家政策支持和资金投入。在中国，量子保密通信城域网、广域网的建设已取得显著成果，如“京沪干线”、“墨子号”量子科学实验卫星等。此外，欧美国家如美国、瑞士、奥地利等也在积极推动量子保密通信网络的建设。

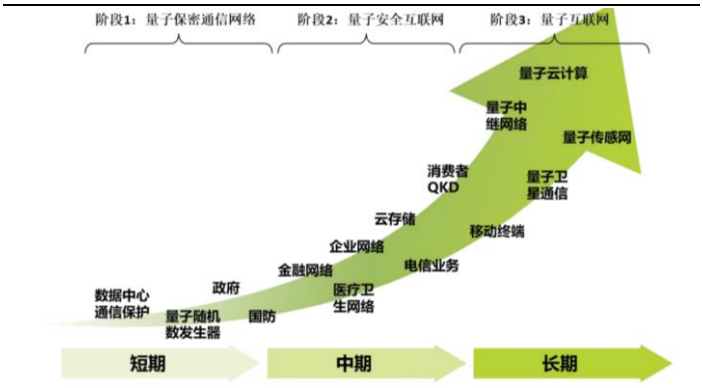
应用服务方面，量子保密通信在金融、军事、政务等领域的应用前景广阔。目前，中国银联、国家电网、军事通信等领域的企事业单位已开始尝试应用量子保密通信技术。同时，欧美国家的一些企业如 BBVA、RWE 等也在探索量子保密通信技术在金融、能源等领域的应用。

图99. 量子保密通信产业链

资料来源：ICV《2022 年全球量子保密通信产业发展报告》，国投证券研究中心

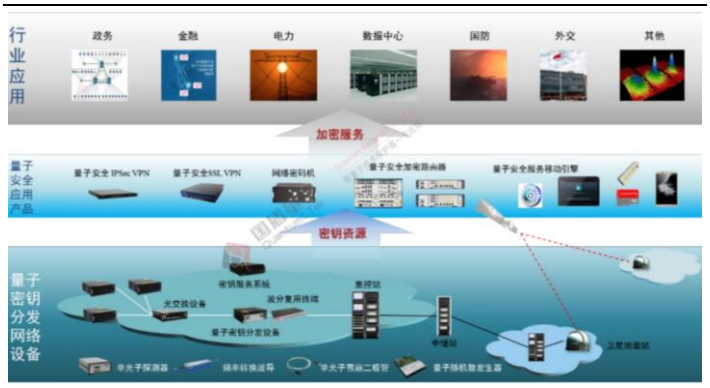
量子通信产业下游应用广泛，多领域均有进展。在国防领域，量子通信技术应用于高度机密的军事通信，确保敏感信息的安全传输，有效防范窃听和网络攻击。在金融领域，金融行业通过量子通信技术实现更安全可靠的数据传输，提高对金融交易和客户信息的保护水平。在电网领域，量子通信可应用于保障电力系统中实时数据的安全传输，预防网络攻击和数据篡改，确保电网运行的稳定性。

图100. 量子保密通信下游应用发展展望



资料来源：国盾量子招股书，国投证券研究中心

图101. 量子保密通信行业应用



资料来源：国盾量子招股书，国投证券研究中心

表24：量子保密通信下游应用进展

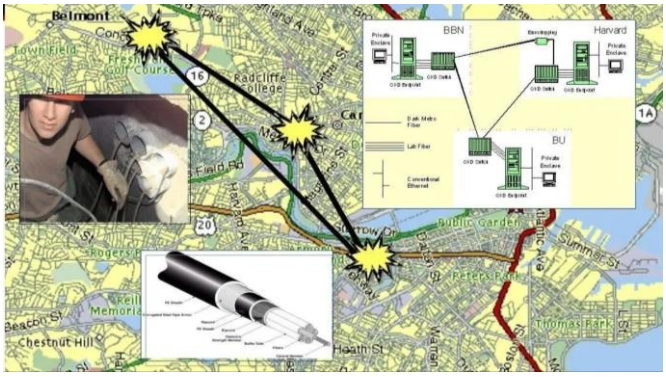
下游行业	进展
国防	美国陆军授予 QuSecure 公司一份小型企业创新研究第二阶段合同，为陆军用户开发基于 PQC 的加密技术和解决方案，并确定如何在战术边缘使用量子技术
	SandboxAQ 企业获得美国国防信息系统局提供的合同，提供端到端的 PQC 管理解决方案。
金融	汇丰银行与 Quantinuum 签署一系列探索性项目，此次合作的目标是利用量子计算的力量来增强加密密钥，同时将其与 PQC 算法相集成。
	汇丰银行使用 QKD 的加密形式保护了其专用平台 HSBC AI Markets 上的一笔交易，将 3000 万欧元兑换成了美元。
电网	中国国网武汉供电公司在武汉经开区供电环网内的配电自动化终端实现了量子加密通信。新安装的量子加密通信线路，配电箱里添置了一个量子加密通信模块，加装在每个配电设备上，通过与电网通信链路连通实现量子加密通信
	浙江省首座量子+变电站 35 千伏稽山变在绍兴老城区投运，该变电站由原 35 千伏城关变经过“无线公网+量子通信”技术改造，将变电站的优先通信变为无线通信，贯通了现有配网量子开关与主网量子+变电站之间的电力信息数据，具备主配网一键联动功能。此次“量子变电站”由国盾量子及参股公司浙江国盾量子电力提供设备及技术支持。
通信	法国 Thales 在其移动安全应用和 5G SIM 卡中采用混合加密技术，引入了 PCQ 算法通信。
	美国 QuSecure 推出具有量子弹性的实时端到端卫星加密通信链路。
	谷歌 Chrome 在其最新版本（版本 116）中推出了一个量子混合密钥协商机制，添加了抗量子攻击的 X25519Kyber768 算法。
	国盾量子推出安全邮件产品——国盾密邮，采用“一次一密”的密钥分发技术，结合高强度国密算法，为用户提供端到端的邮件安全收发服务。
终端	中国电信与华为合作的 Mate60 Pro 手机终端提供量子密话定制功能。
	中国电信与三星推出三星 W24 Flip 两款引入中国电信量子密话功能的手机。
	中国电信发布支持量子密话的天翼铂顿 S9 手机终端，其中天翼铂顿 S9 是搭载天通卫星通话芯片的 5G 卫星双模手机。
	韩国 SKT 与 IDQ、三星电子合作发布 Galaxy Quantum 4 量子通信手机，该手机搭载 QRNG 芯片。

资料来源：ICV《2024 量子通信与安全产业发展展望》，国投证券研究中心

3.3.全球量子通信产业：美国和欧盟积极布局

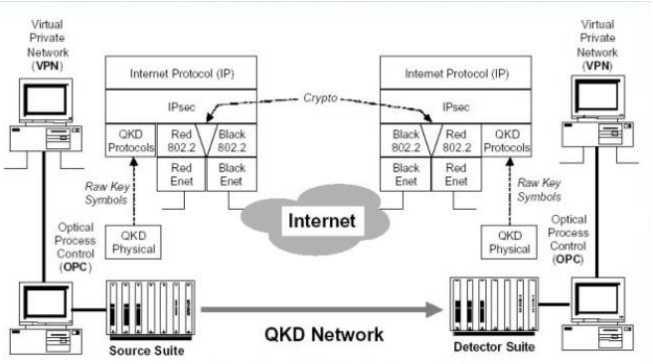
美国：世界首个密钥分发网络，率先布局量子保密通信。美国是最先将量子通信列入国家战略的国家。2003 年，DARPA 建立世界上第一个量子密钥分发保密通信网络。2007 年，美国实现了两个独立原子量子纠缠和远距离量子通信。2016 年，美国航空航天局(NASA)用城市光纤网络实现量子远距传输。美国国防部高级研究计划局(DARPA)量子网络是世界上第一个量子密钥分发(QKD)网络，经营在从波士顿到马萨诸塞州剑桥市的 10 个光节点上，于 2003 年 10 月 23 日在 BBN 技术公司的实验室中全面投入使用，并于 2004 年 6 月通过暗光纤部署在剑桥和波士顿的街道下，并连续运行了 3 年。该项目还创建并部署了世界上第一台超导纳米线单光子探测器。

图102. DARPA 量子通信网络



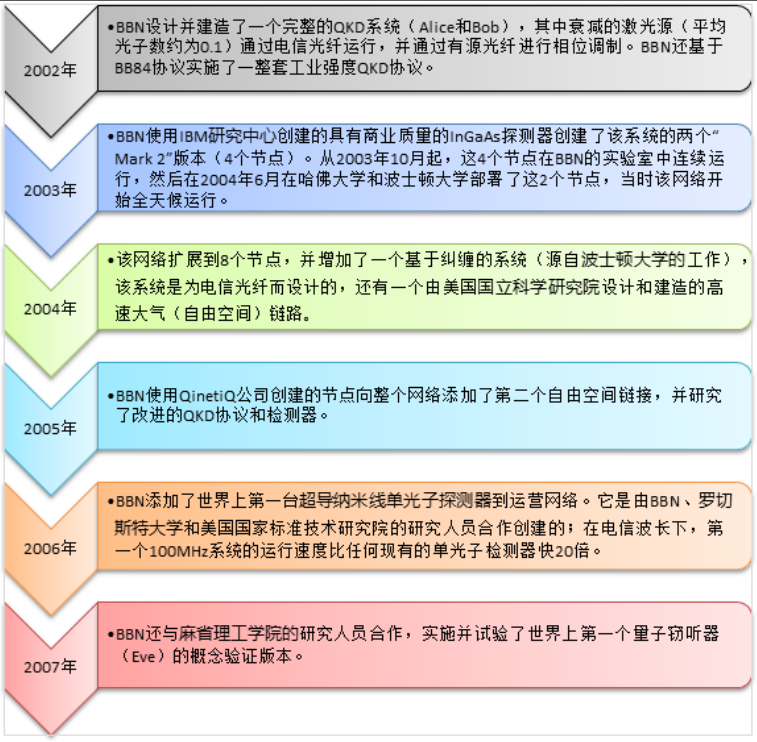
资料来源：高端装备产业中心，国投证券研究中心

图103. DAPRA 量子密钥分发网络结构



资料来源：高端装备产业中心，国投证券研究中心

图104. DAPRA 量子通信网络建成过程



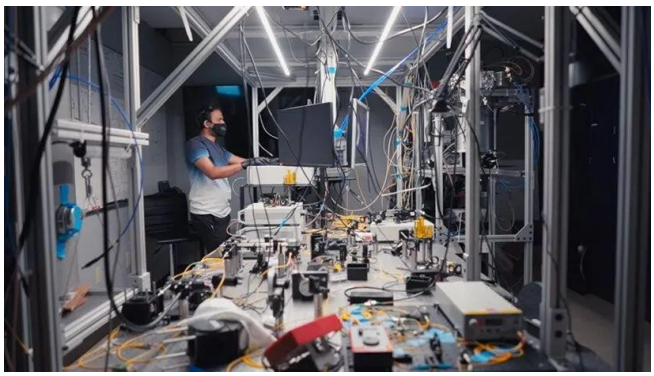
资料来源：高端装备产业中心，国投证券研究中心

美国：通信网络+通信干线齐头并进，为量子网络发展奠定基础。2012 年，NASA 与澳大利亚 Quintessence Labs 公司合作，提出了建设量子保密通信干线的计划，该线路从洛杉矶的喷气推进实验室延伸到 NASA 的艾姆斯研究中心，涵盖了星地量子通信和无人机及飞行器的量子通信链接。另一方面，2018 年，Quantum Xchange 公司宣布建设了全美首个量子互联网——Phio，从华盛顿到波士顿，沿美国东海岸总长 805 公里。2019 年 4 月，Quantum Xchange 与东芝公司合作，将 Phio 网络的容量翻一番，进一步提升了量子密钥分发（QKD）网络的性能和实用性。

美国：开展量子网络链路测试，推动量子通信发展。纽约大学量子信息物理学中心（CQIP）和量子安全网络技术公司 Qunnect 合作，使用 Qunnect 的量子安全网络技术，通过纽约市的标准电信光纤发送量子信息，成功测试了布鲁克林海军造船厂和纽约大学曼哈顿校区之间 10 英里（16 公里）量子网络链路。在 10 英里的光纤中，Qunnect 和 CQIP 实现了以每秒 15000 对的速度传输高度纠缠的量子比特通过光缆，测试过程中链路正常运行时间达到 99%。此次实验打开了纽约都市区的金融服务、关键基础设施和电信公司试点量子网络技术的大门。

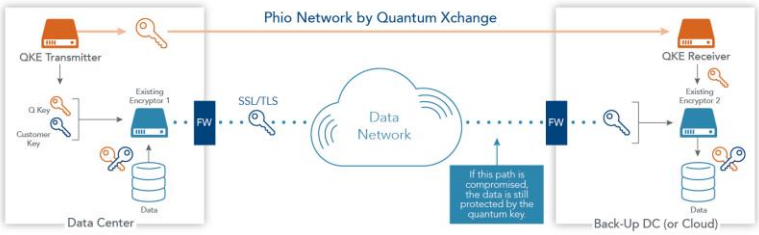
美国：技术研发路线陷争议，未大规模部署，仅开展技术研究。一方面，美国国家安全局 2020 年表示不建议使用 QKD 确保国家安全系统中的数据传输。另一方面，美国能源部、哈德逊研究所认为目前 QKD 仍然是量子通信领域最充分的应用。美国从 2003 年建立第一个 QKD 网络，之后发展进程较为缓慢。2007 年，美国实现了两个独立原子量子纠缠和远距离量子通信。2016 年，美国航空航天局用城市光纤网络实现量子远距传输。2018 年 10 月，美国量子公司 Quantum Xchange 才部署第一个量子密钥分发实用网络，支持纽约到新泽西的量子密钥分发服务。对于美国而言，中国已在 QKD 投入巨额资金，抢占领先地位，要达到中国的规模，必须投入大量的资金。所以发展抗量子密码被美视为比量子密钥分发更具成本效益且易于维护的解决方案。

图105. NASA 使用的量子通信设备



资料来源：高端装备产业中心，国投证券研究中心

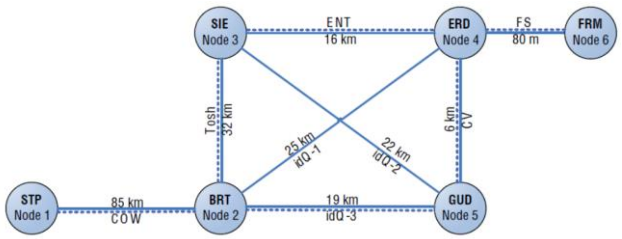
图106. Phio 洲际量子通信网络



资料来源：Quantum XChange 国投证券研究中心

欧盟：集成多种量子密钥手段，构建量子通信网络。欧洲 SECOQC 量子通信网络由英国、法国、德国、意大利等 12 个欧洲国家的 41 个伙伴小组共同设计研发，2004 年开始建设，2008 年在奥地利首都维也纳成功建成。该系统集成了多种量子密钥手段，包含 6 个节点。其组网方式为在每个节点使用多个不同类型量子密钥分发的收发系统并利用可信中继进行联网。SECOQC 量子通信实验网络结构中，6 个网络节点之间通过 8 条点对点量子密钥分发系统相互连接。SECOQC 量子通信实验网络的 8 条链路中，有 7 条是光纤信道，最长为 85km，平均链路长度为 20-30km，可确保在 25km 光纤链路上安全密钥率每秒钟超过 1Kb。

图107. SECOQC 量子通信实验网络结构示意图



资料来源：高端装备产业研究中心，国投证券研究中心

图108. SECOQC 实验网络连接示意图

资料来源：高端装备产业研究中心，国投证券研究中心

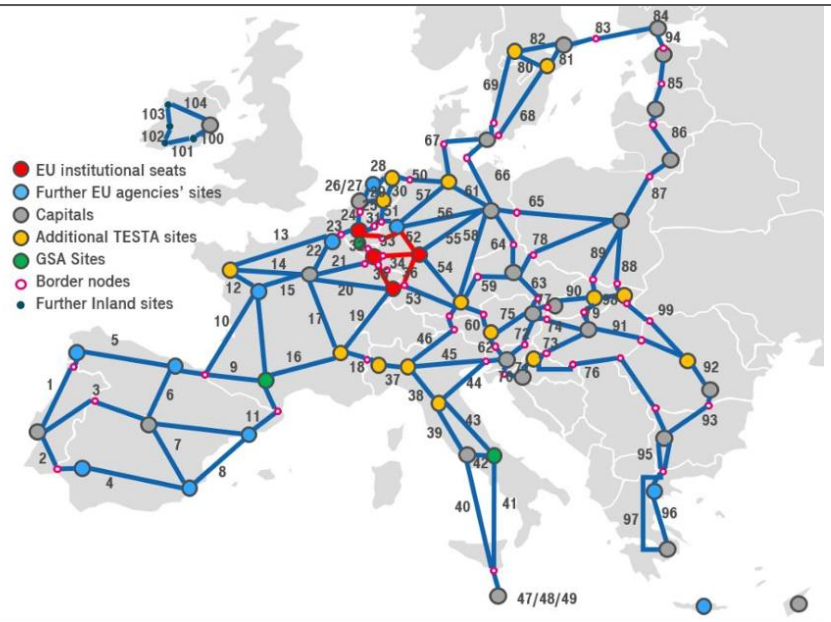
欧盟：光纤融入量子通信网络，世界首创端到端量子安全通信实验。2014 年，英国在 Birmingham、Glasgow、Oxford and York 四所大学设立量子中心用于量子保密通信的研究。同年，英国电信(BT)和东芝两家公司于东芝研究实验室，共同在常规光纤通信网络上整合量子保密技术，首次成功地将量子密码学搭载于 10Gbps 数据传输信号的光纤上传输。2016 年底，他们发现量子密钥分发以及 100Gbps 数据亦可融进同样的光纤。同时，BT 与东芝欧洲研发中心亦在合作打造量子通信网络(英国量子网络)。作为英国投入 2.7 亿英镑的国家量子技术项目的一部分，该计划在剑桥、布里斯托、伦敦和阿达斯特拉尔科技园之间部署量子保密通信。连接 BT 阿达斯特拉尔科技园和剑桥科技园的线路，2017 年上半年完工。此外，3020 年 11 月，英国电信(BT)与剑桥大学附属公司 Nu Quantum、物联网网络安全初创企业 Angoka、量子计算公司 Duality Quantum Photonics 等合作，开始研究在 5G 和联网汽车安全通信开发方面实现飞跃。英国电信指出，此举是一项“世界首创”的端到端量子安全通信试验的一部分，该试验获得了由英国研究与创新(UKRI)资助机构提供的 770 万英镑资助，为期 36 个月。

图109. 东芝欧洲公司展出的量子通信设备

资料来源：高端装备产业研究中心，国投证券研究中心

欧盟：EuroQCI 项目陆续开展，预计 2027 年投入使用。欧洲量子通信基础设施（EuroQCI）是一个覆盖整个欧盟及其海外领土的量子通信安全基础设施。欧盟委员会与所有 27 个欧盟成员国以及欧洲空间局(ESA)合作，设计、开发和部署由地面部分和空间部分组成的 EuroQCI。地面部分依赖于连接国家和跨境战略站点的光纤通信网络，而太空部分基于卫星进行建设。EuroQCI 空间部分主要为欧盟委员会与 ESA 合作，基于已有的第一颗原型卫星 Eagle-1 的基础上制定 EuroQCI 第一代卫星星座的规格，预计该卫星于 2025 年底或 2026 年初发射。

图110. 欧盟 EuroQCI 项目地面部分潜在选址



资料来源：ICV《2024 量子通信与安全产业发展展望》，国投证券研究中心

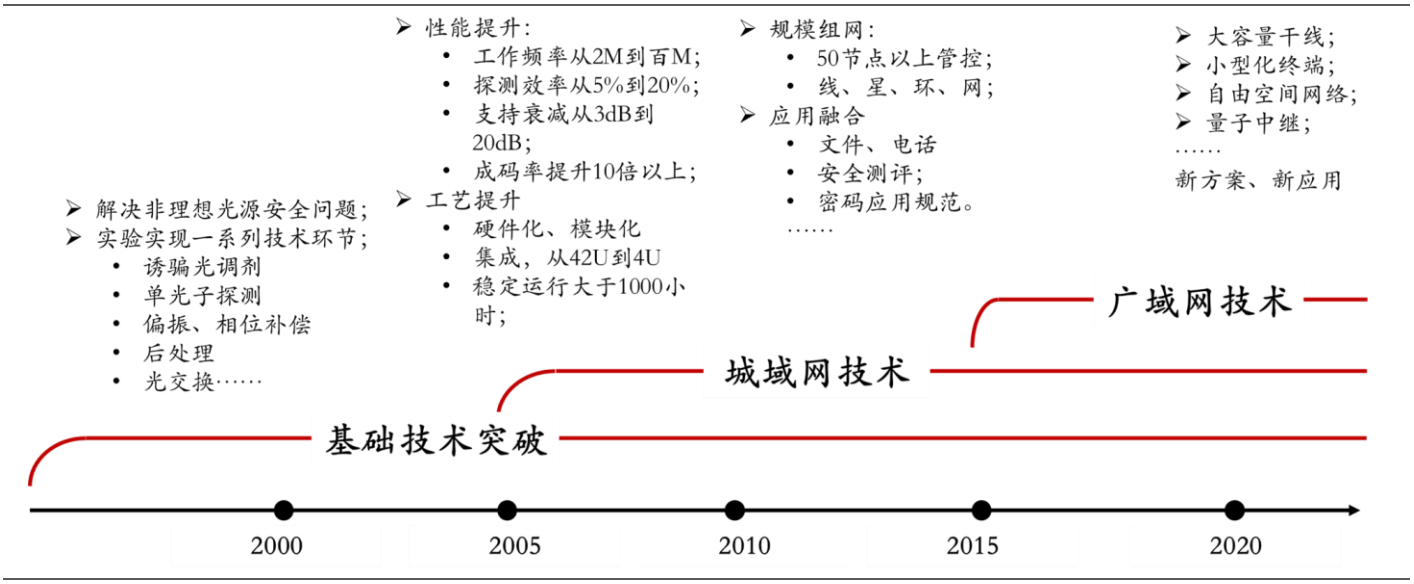
欧盟：紧随中国位居第二，全面建设部署国家级 QKD 网络。政策标准方面，2021 年 7 月，欧盟 27 个成员国联合签署欧盟量子通信基础设施协议，共建欧盟量子安全通信基础设施。2022 年 12 月，欧盟“欧洲量子技术旗舰计划”发布报告，建议全面建设区域、国家 QKD 网络的部署。2023 年 8 月，国际标准化组织推出了首套专门针对 QKD 的安全要求标准。**建设部署方面，**2022 年 9 月，欧空局 Eagle-1（测试远程量子密钥分发 QKD）计划 2024 年发射集成 QKD 模块的卫星，这是第一个用于欧洲网络安全的卫星量子加密系统。2023 年 4 月，欧洲电信标准化协会发布全球首个 QKD 保护轮廓以对制造商提交的 QKD 模块进行安全认证。**对于欧盟而言，**“量子安全”最早是由欧洲电信标准化协会于 2015 年发布的《量子安全密码及其安全性》白皮书中提及并由全球沿用的概念和定义。所以欧盟对于量子密钥分发和抗量子密码两条保证量子安全的路线采取同时推进、全面部署的策略。

3.4.国内量子通信产业：三步走战略实现全覆盖

中国：明确实施三步走战略，助力量子通信产业快速发展。中国量子通信的“三步走”战略主要包括以下几个阶段。1）**第一步：**基于现有光纤的城域网，这一阶段的目标是建立覆盖城市范围的量子通信网络。中国已经建成了一些规模化的城域量子通信网络，例如合肥城域量子通信试验示范网，这是世界上首个规模化量子通信网络。2）**第二步：**基于可信中继的城际网，在这一阶段，中国计划通过量子中继器建立城际网络。量子中继器能够解决光子在长距离传输中的损耗问题，从而实现更远距离的量子通信。3）**第三步：**基于卫星中转的洲际网，最后，中国计划通过卫星中转实现全球范围内的量子通信网络。这包括发射量子科学实验卫星，如“墨子号”，以实现星地之间的量子通信。

这些阶段的成功实施，使得中国在量子通信领域取得了显著的进展，并处于国际领先地位。例如，“墨子号”卫星完成了三大科学实验任务，并建立了人类历史上首次洲际量子保密通信。此外，中国还计划发射更多的量子卫星，以进一步扩展其量子通信网络。

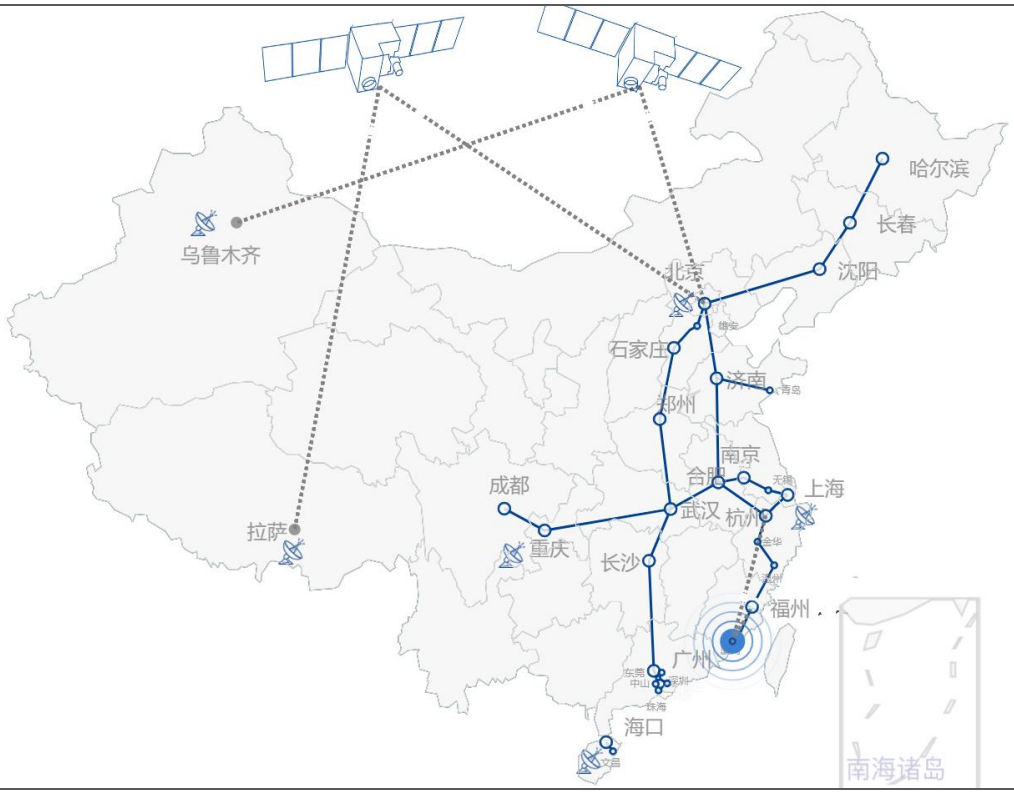
图111. 量子通信发展三步走战略



资料来源：国盾量子招股书，国投证券研究中心

骨干网+城域网建设成果显著，全长超过 1 万公里。2013 年国家发改委批复立项了世界首条量子保密通信干线“京沪干线”，全长 2032 公里，总投资 5.6 亿元，沿线的北京、济南、枣庄、宿州、合肥、上海等地也相继建成了城域网。2018 年国家发改委批复建设“国家广域量子保密通信骨干网络建设一期工程”，建设京汉、汉广、沪合 3 条量子保密通信骨干网络，总里程约 3800 公里。当前，根据国科量子官网介绍，国家广域量子保密通信骨干网络总长超过 1 万公里，覆盖京津冀、长三角、粤港澳大湾区、成渝、东北等区域的 17 个省市约 80 个城市。此外，由国科量子建设和运营的长三角区域量子保密通信骨干网建设成果于 2023 年 6 月在第五届长三角一体化发展高层论坛上正式发布。长三角量子网络线路总里程约 2860 公里，形成了以合肥、上海为核心节点，链接南京、杭州、无锡、金华、芜湖等城市的环网，通过量子业务运营支撑系统及量子卫星调度系统，为星地一体量子保密通信网络提供全方位保障。

图112. 中国量子保密通信网络建设进度



资料来源：国科量子，国投证券研究中心

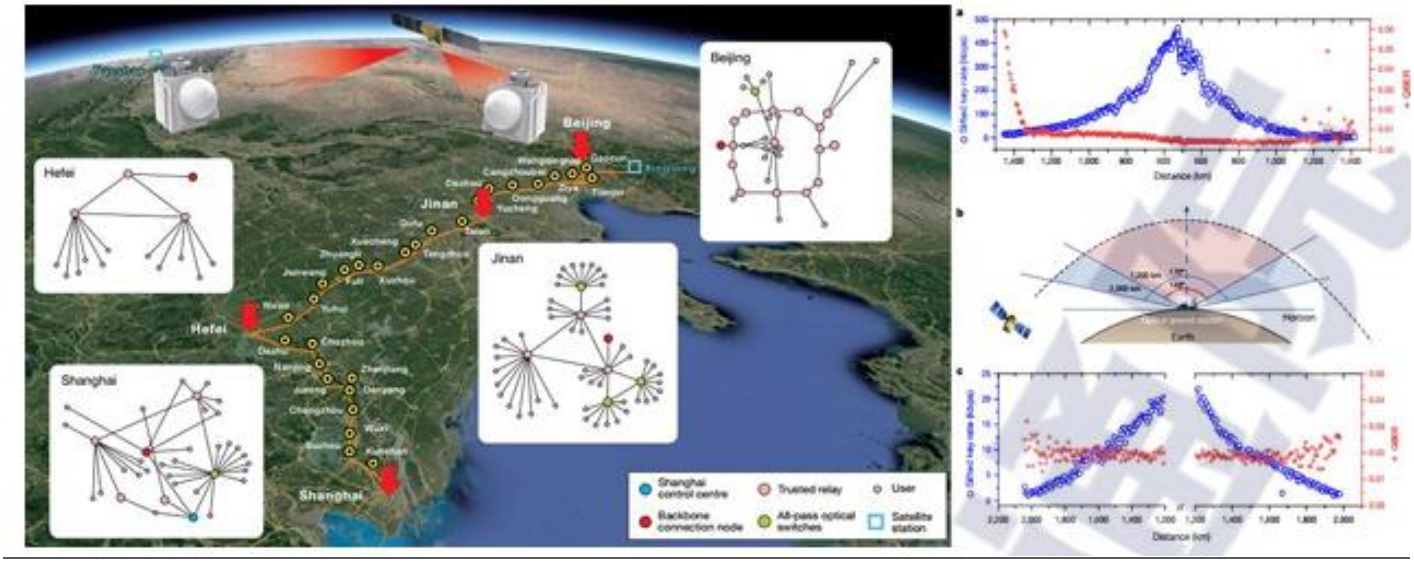
表25：中国量子保密通信网络统计（部分）

时间	地点	名称
2009 年	合肥	5 节点全通型量子通信网络
2009 年	芜湖	7 节点量子政务网
2009 年	北京	建国 60 周年月饼量子保密热线
2012 年	合肥	合肥城域量子通信实验示范网
2012 年	北京	新华社金融信息量子通信试验网
2012 年	北京	十八大量子安全通信保障
2012 年	合肥-芜湖	“合巢芜”城际量子通信网
2013 年	济南	济南量子通信试验网
2014 年	合肥	公安量子通信试点工程
2015 年	北京	抗战胜利 70 周年月饼量子密话及传输系统
2017 年	各地	“墨子号”量子科学实验卫星广成量子密钥应用平台
2017 年	北京-上海	量子保密通信“京沪干线”
2017 年	南京-苏州	江苏省苏宁量子干线
2017 年	合肥	融合量子安全的合肥政务外网
2017 年	济南	济南党政机关量子通信专用
2017 年	北京	十九大量子安全通信保障
2018 年	武汉-合肥	武合量子保密通信干线
2018 年	武汉	武汉量子保密通信城域网
2018 年	北京	北京量子城域网
2018 年	华东	阿里巴巴 OTN 量子安全加密通信系统
2018 年	上海	陆家嘴金融量子保密通信应用示范网
2021 年	宿州	宿州量子保密通信党政军警专用
2019 年	乌鲁木齐	乌鲁木齐量子保密通信城域网
2020 年	海口	海口量子保密通信城域网
建设中	西安	西安量子保密通信城域网
2019 年	贵阳	贵阳市量子保密通信城域网
建设中	中国	国家量子保密通信骨干网（汉广段、沪合段）
2020 年	金华	进化量子保密通信城域网
2020 年	南京	南京江宁区政务网量子通信专网
建设中	成都	成都市电子政务外网（量子保密通信服务试点）
建设中	苏州	苏州市吴江区电子政务外网量子安全通信

资料来源：ICV，国投证券研究中心

天地一体量子保密通信网络蓄势待发，以星地量子通信为契机促进空间量子科学发展。基于卫星平台的星地通信方案，具有信道损耗小、接入灵活性高、覆盖面广和生存性强等优点，成为量子通信科学研究和实验探索的热点方向。2016 年 8 月，中科大联合航天科技集团等多家单位，成功发射了全球首颗量子科学实验卫星“墨子号”，并在之后 4 年取得一系列国际领先科研实验成功。2021 年 1 月，中科大 Nature 发文，对基于“墨子号”量子科学实验卫星和量子保密通信“京沪干线”技术验证及应用示范项目，验证天地一体化量子通信组网可行性科研成果进行回顾综述。通过提升工作频率、地面站望远镜尺寸和耦合效率，使用非平衡选基新协议等改进措施，在理想气象条件下单轨（约 6 分钟）星地 QKD 密钥成码率比早期结果提升 40 倍，可达 47.8bit/s，每周密钥生成量的理想化最大值约 36Mbit。

图113. 基于“墨子号”卫星和“京沪干线”天地一体化组网验证



资料来源：信通院《量子信息技术发展与应用研究报告 2021》，国投证券研究中心

发布世界首颗量子微纳卫星“济南一号”发射，天地一体化广域量子保密通信网络初具雏形。利用“墨子号”积累的成功经验，我国研制并发射了世界首颗量子微纳卫星“济南一号”，为构建低成本、实用化的量子星座奠定基础。同时，地面接收站的重量也已由十几吨降到 100 kg 左右，可初步支持移动量子通信。结合“墨子号”量子卫星与“京沪干线”，我国率先构建了天地一体化广域量子保密通信网络的雏形，成为近年来国际量子信息研究的一大标志性事件。

“济南一号”提升明显，量子通信网络规模化应用成为可能。“济南一号”作为商业卫星，相对于墨子号，有了进一步的发展。“济南一号”量子密钥分发载荷只有 23 公斤，即使算上整星，也只有 98 公斤，仅是“墨子号”的六分之一，尺寸、功耗大大减小，研发成本和发射成本远低于“墨子号”。与“济南一号”配合的地面站，在小型化方面也取得突破性进展，其重量由 12 吨左右降至 100 公斤以下，安装部署时间由数月降低至数小时。“济南一号”将原有的量子通信信道和光通信信道合二为一，可以实时地进行密钥提取和成码，时效性比“墨子号”提升了 2-3 个数量级，增加了“济南一号”实用化前景，同时研发及发射成本也大大降低。随着“济南一号”的研发和顺利升空，构建低成本、实用化的天地一体化量子保密通信网络成为可能。

微纳卫星+小型化地面站，成就星地密钥分发网络开端。对于完整的空地一体广域量子通信网络体系来说，“济南一号”只是其中低轨卫星网络的开始。因为，想要最终实现实用化、全球化的量子通信网络，满足数目日益增长、现实需求不同的客户，必须科学布局中高轨量子卫星、低轨量子通信卫星星座和大规模的地面光纤量子通信网络，根据实际需要，三个体系相互配合。但同时，“济南一号”又是重要的一大步，它**标志着我国将在世界上首次实现基于微纳卫星和小型化地面站之间的实时星地量子密钥分发。**未来，将会迎来更多的低轨量子密钥分发终端，可以为全球大约 100 多个用户提供高频、安全的量子密钥服务。

图114.“低轨微纳卫星+小型化地面站”技术路线

资料来源：物流学报《量子信息科技的发展现状与展望》，墨子沙龙，国投证券研究中心

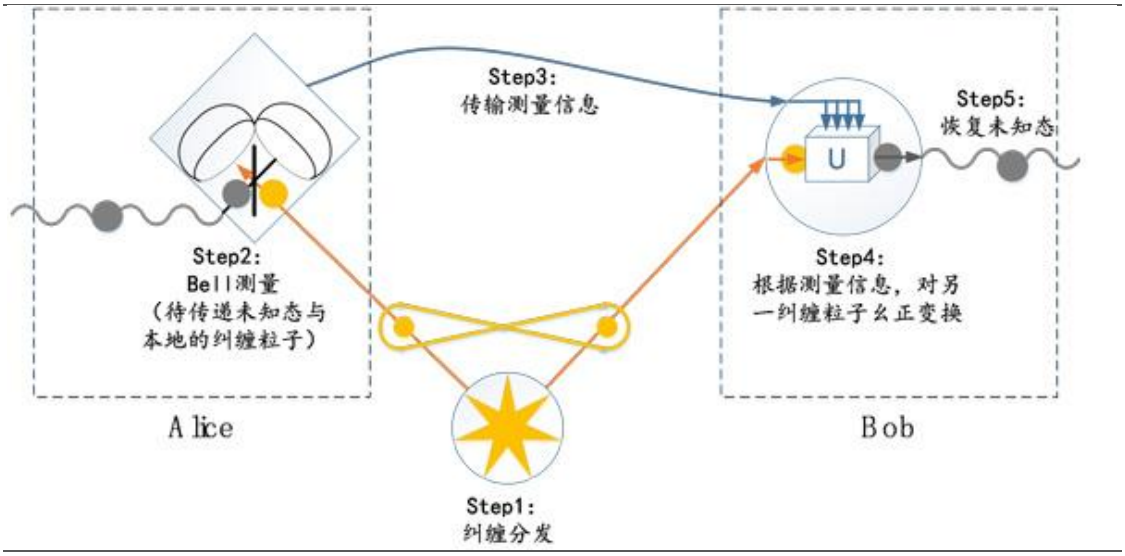
中国在 QKD 领域全球领跑，深耕技术突破与行业应用。当前我国 QKD 相关技术逐渐走入世界前列，并初步形成一条探索型产业链。自由空间传输方面，以“墨子号”为代表的关键工程已实现 1200 千米通信距离的星地量子密钥分发，标志着我国已率先进入 QKD 广域网建设领域，向天地一体量子安全网络逐步演进。中继光纤网络方面，光纤量子保密通信骨干网“京沪干线”、中国合肥量子城域网取得突破，通过联通 8 个核心网站点和 159 个接入网站点向可实用规模的量子保密通信网络演进，且以成功应用于金融、政务、医疗等多个领域，并有望拓展至四县一市，接入国家量子骨干网。就目前发展而言，我国将持续深耕量子通信技术，加强量子网络建设，持续探索量子保密通信行业应用和产业化落地。

3.5.量子隐形传态：未来量子互联网的核心技术

量子隐形传态有望成为未来量子计算机组网核心技术，实现真正的量子互联网。量子隐形传态是以实现量子态的远程传输为目的的一类量子通信协议，将量子纠缠特性作为通信信道使用，从而实现任意未知量子态的传输。在量子隐形传态中，通信前收发双方事先共享一对相互关联的粒子，也称为纠缠粒子。纠缠态本身具有非局域的量子特性，相距很远的纠缠粒子之间形成了特殊的量子信道。发送端将待传输的未知量子态与共享粒子对的本地粒子进行特定的测量后，将测量结果告知接收端。接收端用户根据这个测量结果对其拥有的粒子进行一次本地的操作后，即可获得发送端待传输的量子态。

如图所示，一对纠缠 EPR 光子对被分发给空间上分处两地的 Alice 和 Bob。Alice 另外还持有一个处于任意量子态的光子，现在她需要将该量子态（当然也包括编码在该量子态上的信息）传输给 Bob。那么接下来的工作步骤可以概括为：首先，Alice 让处于未知态的光子与 EPR 对在她那里的一个光子进行以 Bell 态为基矢的投影测量；然后通过经典的方法将测量结果告知 Bob；根据 Alice 发布的经典信息，Bob 随后对他所持有的 EPR 对中另一个光子进行相应的幺正变换，使之变成与 Alice 所要传输的未知态完全相同的态，从而达到量子态转移的效果。

图115. 量子隐形传态示意图



资料来源：中国科学院量子信息与量子科技创新研究院，国投证券研究中心

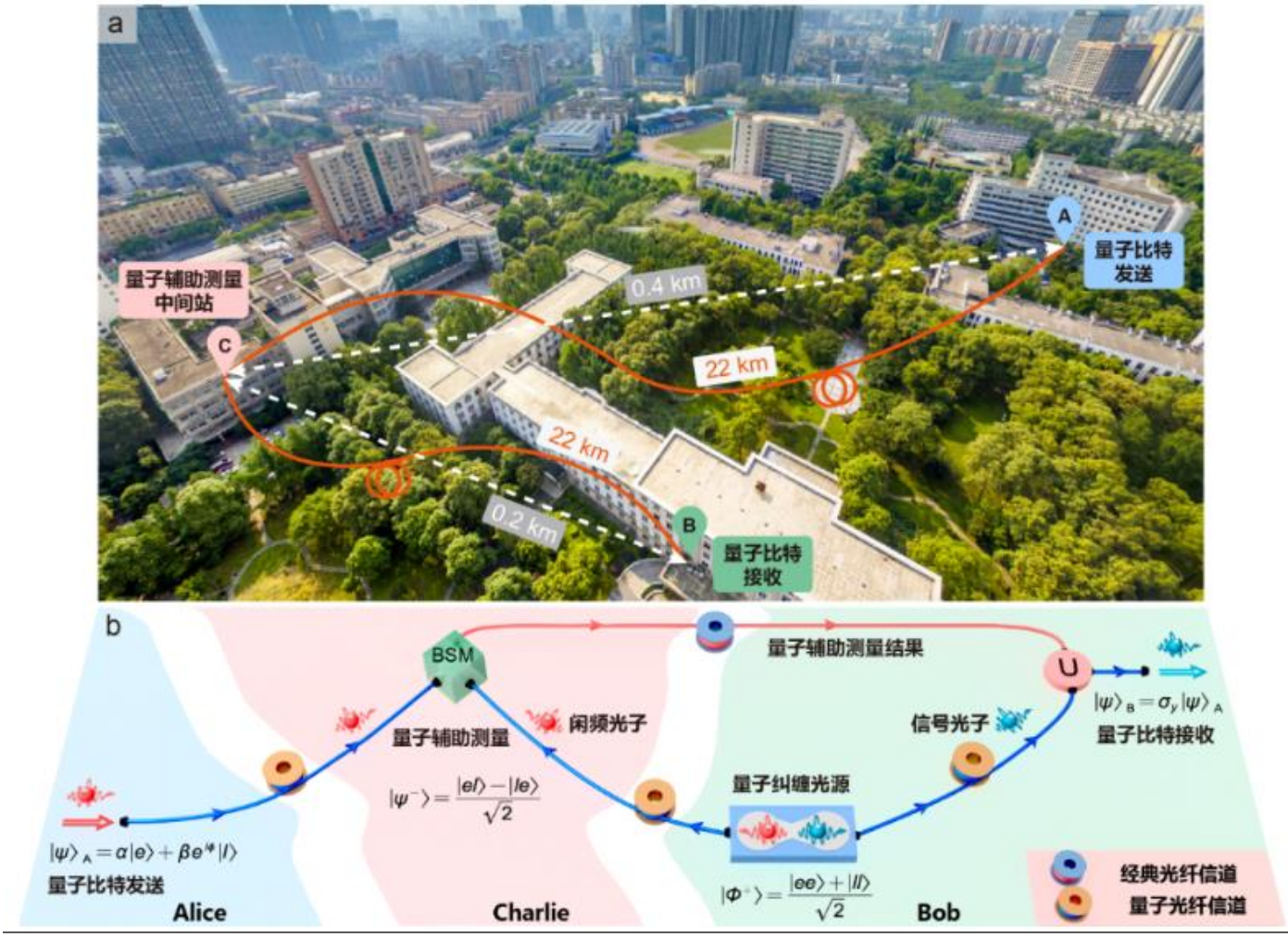
突破多种关键技术，赫兹速率城域量子隐形传态成为可能。2023 年，电子科技大学郭光灿院士团队周强研究组与中科院上海微系统所尤立星团队合作，在电子科技大学“银杏一号”城域量子互联网方面取得了重大进展。研究团队合作研制出高重频量子光源、自动化光子全同测控装置、高性能超导纳米线单光子探测器，突破了量子信息载源、量子信道建立、量子信息检测等技术难题，首次完成“赫兹速率”的城域量子隐形传态。实现量子互联网的关键任务之一便是在不同量子节点间完成量子信息的传递。借助于量子纠缠资源，在量子投影测量和经典通信的辅助下，量子隐形传态可将未知量子信息进行“离物传递”。这次工作建成的“银杏一号”城域量子互联网，使用诱骗态时间片量子比特对待传递的量子信息进行编码，在突破许多关键技术的基础上，首次将城域量子隐形传态的速率提升至赫兹量级。

1）**高重频量子纠缠光源：**研究团队研制出具有自主知识产权的量子纠缠光源，使用单个尾纤耦合周期极化铌酸锂波导模块，实现了 500 MHz 重频触发的高质量量子纠缠光源。

2）**自动化光子全同测控装置：**为了保障量子隐形传态的成功，提高贝尔态投影测量效率，需确保来自 Alice 和 Bob 的光子在长距离光纤传输后保持全同。研究团队自主研发出自动化光子全同测控装置，通过对量子信道中的光子偏振及时延信息进行实时感知，实现了快速响应的光纤信道光子全同稳定测控技术。

3）**高性能超导纳米线单光子探测器：**中科院上海微系统所尤立星团队为实验系统提供了高探测效率、低暗计数、低时间抖动的高性能超导纳米线单光子探测器，用于高效率贝尔态投影测量和光量子态检测过程。此外，研究团队分别使用量子态层析及诱骗态方法获得隐形传态的保真度均大于经典极限（66.7%），并通过三重符合测量得到量子态传递速率为 7.1 Hz，首次实验验证了赫兹速率城域量子隐形传态的可行性。

图116. “银杏一号”城域量子互联网建设场地鸟瞰图和设计示意图



资料来源：ICV，国投证券研究中心

4. 抗量子密码：密码原理的底层创新，应对量子攻击的新型方案

4.1.量子计算对加密构成威胁，抗量子密码应运而生

量子计算对现有密码体系构成威胁。随着量子计算技术不断取得突破，算力大幅提升，特别是以 Shor 算法为代表的量子算法提出，有关运算操作在理论上可以实现将质因数分解算法的计算复杂度从指数级向多项式级转变，这意味着量子计算能够使得公钥密钥的破解实现指数级加速，对现有密码体系构成威胁。

抗量子密码（PQC）应运而生，应对量子计算攻击的新型密码算法。PQC 是能够抵抗量子计算对现有密码算法攻击的新一代密码算法，旨在研究密码算法在量子环境下的安全性，并设计在经典和量子环境下均具有安全性的密码系统。对于对称密码算法，尽管量子计算机可能降低现有算法的安全性，但增加参数的长度对维护安全性是有效的。因此，PQC 研究重点是非对称密码算法。PQC 与 QKD（量子密钥分发）有所差异，QKD 设计利用量子物理特性进行密码的分发，而 PQC 则关注在经典计算机上运行新的密码算法，使得这类算法即使用量子计算机也无法破坏。

表26：量子计算对经典密码体系的影响

密码算法	类型	作用	量子计算的威胁
AES	对称密钥	通信加密	增大密钥长度
SHA-2/SHA-3	哈希密钥	单向散列加密，完整性保证	输出长度增加
RSA	公钥密钥	数字签名 密钥建立	丧失安全性
ECDSA/ECDH	公钥密钥	数字签名 密钥交换	丧失安全性
DSA	公钥密钥	数字签名 密钥交换	丧失安全性

资料来源：光子盒公众号，国投证券研究中心

根据抗量子密码算法所基于的底层困难问题，主流抗量子密码算法大致分为 5 类：（1）基于格(Lattice-based)的抗量子密码算法（2）基于哈希(Hash-based)的抗量子密码算法（3）基于编码(Code-based)的抗量子密码算法（4）基于多变量(Multivariate-based)的抗量子密码算法（5）基于同源(Isogeny-based)的抗量子密码算法。

基于格：格（Lattice）是一种数学结构，定义为一组线性无关的非 0 向量（称作格基）的整系数线性组合。格密码的主要数学基础是格中的两个困难问题：格的最短矢量问题（SVP）和格的最近矢量问题（CVP）。格是一个困难的问题，并且难度还能控制，满足了成为密码学算法核心的必要条件。**PQC 算法中，对格的研究是最活跃、最灵活的。**基于格的算法在安全性、公私钥大小、计算速度上可达到较好的平衡。第一，基于格的算法可以实现加密、数字签名、密钥交换、属性加密、函数加密、全同态加密等各类功能的密码学构造。第二，基于格的算法的安全性依赖于求解格中问题的困难性。这些问题在达到相同的安全强度时，基于格的算法的公私钥大小比上述其他三种方案更小，计算速度更快，且能被用于构造多种密码学原语，更适用于真实世界中的应用。因此，基于格的算法被认为是最有前景的 PQC 算法之一。

基于哈希：基于哈希的签名算法从 Lamport 提出的一次性签名方案演变而来，最早由 Ralph Merkle 提出，并使用哈希树构造。基于哈希的密码算法仅限用于数字签名，至今学术界还没有专家提出基于哈希设计并实现的公钥加密或密钥封装的方案。基于哈希的数字签名方案的安全性依赖于哈希算法的一些安全性质，例如单向性（抗原像攻击）、弱抗碰撞性（抗第二原像攻击）和伪随机性等。如果使用的哈希函数被攻破，完全可以构造新的安全的哈希函数来替代，因此基于哈希的签名是抗量子密码中理论安全性最强的一类。但是主要有以下两点缺点：一是签名体积大；二是对于有状态的基于哈希的签名，其所能支持的签名次数有限，增加签名数量也将降低计算效率，并进一步增加签名的体积。

基于编码：基于编码的算法 1978 年，其理论依据来源于随机线性码的译码是困难问题：经过编码的信息在信道上传输，由于噪声产生错误，在接收端通过译码算法恢复。其核心在于将一定数量的错误码字引入编码中，纠正错误码字或计算校验矩阵的伴随式是困难的。McEliece 提出了首个基于编码的公钥加密方案 McEliece 方案，从而开创了基于编码的密码学这一研究领域。**基于编码的密码算法被认为是抗量子密码中相对具有竞争力的密码算法。**著名的基于编码的加密算法是 McEliece，McEliece 使用随机二进制的不可约 Goppa 码作为私钥，公钥是对私钥进行变换后的一般线性码。基于编码的密码通常具有较小的密文，但其缺点是公钥大、密钥生成慢，在实用化方面有待提升。

基于多变量：基于多变量的算法使用有限域上具有多个变量的二次多项式组构造加密、签名、密钥交换等算法。多变量密码的安全性依赖于求解非线性方程组的困难程度，即多变量二次多项式问题。该问题被证明为非确定性多项式时间困难。目前没有已知的经典和量子算法可以快速求解有限域上的多变量方程组。**基于多变量的算法适用于一些注重算法效率但不关心带宽的应用场景。**多变量密码算法相比于其他抗量子密码算法具有签名验签速度快、消耗资源少的优势，其缺点是公钥尺寸大，因此适用于无需频繁进行公钥传输的应用场景，例如计算和存储能力受限的物联网设备等。

基于同源：同源密码是基于椭圆曲线同源问题的抗量子密码系统，它基于一个新的困难问题，即寻找任意两条椭圆曲线之间的同源。2011 年基于超奇异同源的 SIDH 算法被提出，该算法是一个 Diffie-Hellman 类型的密钥交换算法，2017 年基于 SIDH 算法的高效实现 SIKE 算法被提出，随后一些新的基于同源的密码系统被提出，比如 CSIDH 和 SQIsign 算法等。基于同源的密码继承了椭圆曲线密码的底层运算，公钥和密文尺寸都非常小，可以在通信量受限的环境下运行，但是其运行效率非常低，其密钥生成、加密和解密速度几乎比基于格大两个数量级，这使其不易实现在一些计算性能不足的设备上。在 NIST 将 SIKE 进入第四轮不久，有专家利用 SIKE 的提示信息可以在数小时内恢复私钥信息，即 SIKE 被攻破，不过 CSIDH 和 SQIsign 算法仍未被攻破。

表27：抗量子密码算法比较

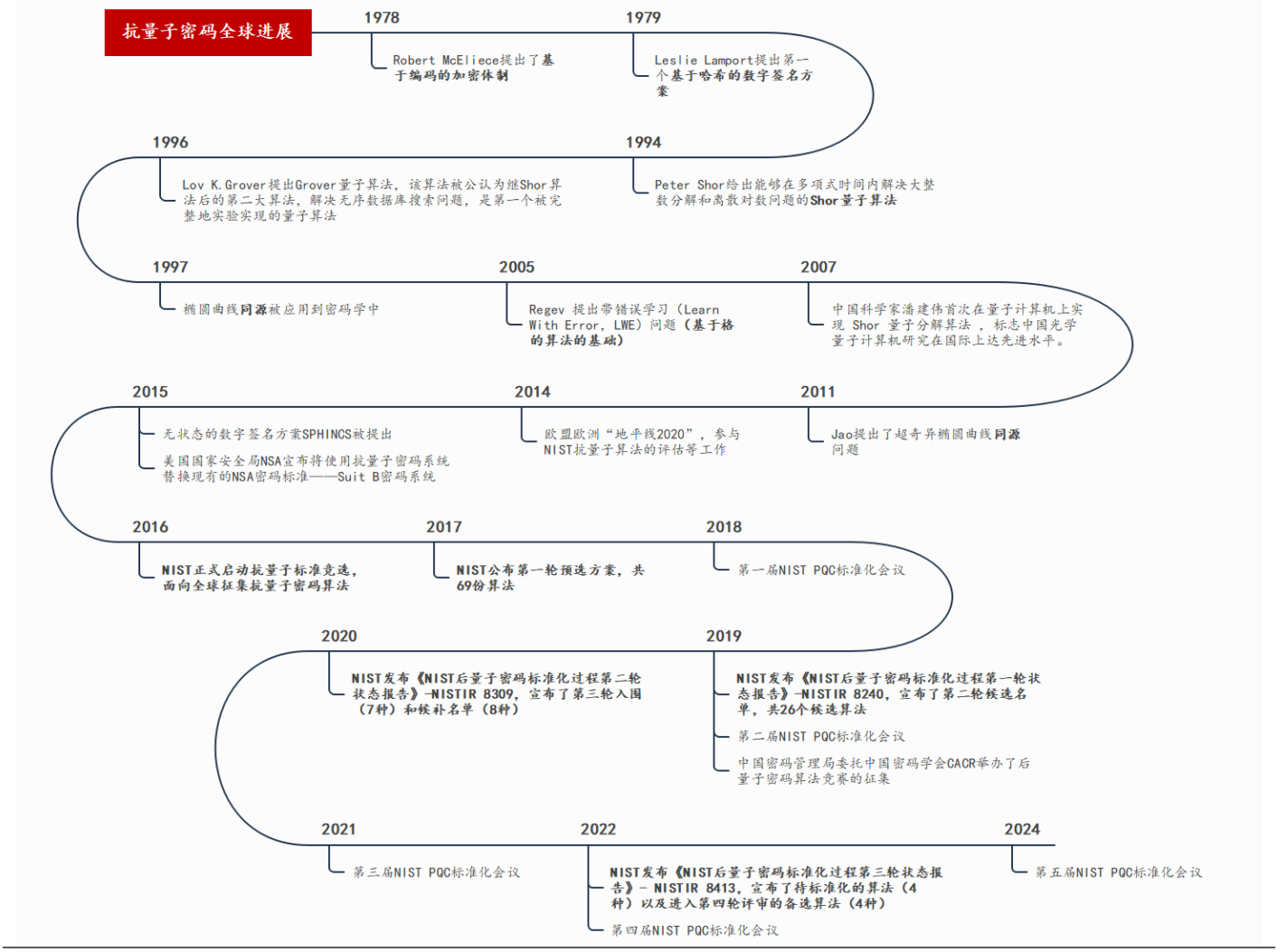
类别	公钥尺寸	计算速度	功能多样性	优点	缺点
基于格	小	快	很好	安全性高，性能优越，功能全	带宽较大
基于哈希	小	较快	有限	公钥很小，安全假设少	性能有待提升，功能上只能构造签名
基于编码	大	快	较好	密文较小	公钥大，密钥生成慢，在实用化方面有待提升
基于多变量	大	较快	较好	签名验签速度快，消耗资源少	公钥大，安全性低
基于同源	极小	慢	较好	带宽很小	计算速度慢，缺乏可证明安全性

来源：“密码+”应用推进计划研究报告，《后量子密码发展综述》，国投证券研究中心

4.2. 全球积极布局抗量子密码，标准即将发布

随着量子计算机的发展，多个国家的密码管理部门对能抵抗量子计算的 PQC 研究越发重视。目前，标准化组织、各国密码或安全管理部门、产业界正推进 PQC 密码的标准化。美国、欧洲、中国等都在积极的投入 PQC 的标准化研究中，影响力最大的是美国 NIST 面向全球的技术方案征集。

图117. 抗量子密码全球进展



资料来源：“密码+”应用推进计划研究报告，中国电信研究院，光子盒公众号，信息安全与通信杂志社，国投证券研究中心

目前，抗量子密码领域中，全球最具实力的市场参与者主要分布在北美和欧洲，例如，美国的公司有 Google、IBM、Microsoft、PQSecure、Cisco、Envieta，加拿大的公司有 ISARA、Quantropi 等，欧洲的公司有 PQShield（英国）、Infineon（德国）、Thales（法国）、CrypotoNext（法国）、Gemalto（荷兰，2019 年被 Thales 收购）等。这些公司是提供芯片设计、数字信息安全和量子安全综合解决方案这三大类服务的科技企业。此外，还有一些顶尖大学和研究院所参与 PQC 研究，例如，慕尼黑工业大学（德国）、佛罗里达大西洋大学（美国）、清华大学（中国）。

美国：针对后量子密码和迁移战略方面，发布和更新了诸多政策。2018 年 9 月，美国国家科学与技术委员会 NSTC 发布《量子信息科学国家战略总览》。2022 年 1 月，美国总统签署第 8 号国家安全备忘录 NSM-8，首次将后量子密码纳入国家安全备忘录。2022 年 5 月，美国签署总统政令，要求确保美国在量子计算领域的领先地位，并推进后量子算法迁移，减少量子计算带来的安全风险。2022 年 9 月，美国 NSA 发布了含后量子密码算法推荐的 CNSA 2.0 套件，给出政府信息系统 6 种场景在 2033 年前完成后量子迁移的时间表。

表28：美国抗量子密码政策

时间	发布单位	政策/内容
2018 年 9 月	美国国家科学与技术委员会 NSTC	发布《量子信息科学国家战略总览》
2018 年 12 月	美国政府	发布《国家量子规划法案》，成立国家量子规划 NQI
2019-2020 年	美国政府	通过《国防授权法案》，国防部开展和支持量子信息科学和技术研发
2021 年 10 月	美国国土安全部(DHS)与 NIST	发布《抗量子密码过渡路线图》
2022 年 1 月	美国总统	签署第 8 号国家安全备忘录 NSM-8，将抗量子密码纳入国家安全备忘录
2022 年 5 月	美国总统	签署总统政令，要求保持量子计算领域领先地位，推进后量子算法迁移
2022 年 7 月	美国国众议院	通过《量子计算网络安全防范法案》，鼓励联邦信息系统向抗量子密码迁移
2022 年 8 月	美国政府	通过《芯片与科学法案》修正 NQI 法案，授权开展量子网络基础设施等研发与标准化
2022 年 9 月	美国国家安全局 NSA	发布 CNSA 2.0 套件，包含抗量子密码算法推荐，提出政府信息系统迁移时间表
2022 年 12 月	美国国家安全局 NSA	发布《2022 年网络安全年度回顾》，强调抗量子密码抵御量子技术威胁
2022 年 12 月 21 日	美国总统拜登	签署《量子计算网络安全防范法案》，成为法律，鼓励采用抗量子加密技术
2023 年 3 月 2 日	美国政府	发布《国家网络安全战略》，提出公共网络和系统过渡到抗量子密码环境
2023 年 8 月	美国 CISA、NSA 与 NIST 联合	发布《量子准备：向抗量子密码迁移》指南
2023 年 9 月	NIST 下属的国家网络安全中心 NCCoE	

来源：“密码+”应用推进计划研究报告，光子盒公众号，国投证券研究中心

美国：NIST 牵头制定抗量子密码算法标准。NIST（美国国家标准与技术研究院）发起的后量子密码标准化项目是当前影响力最大、参与范围最广的标准化项目。其目标是遴选出通用的抗量子算法攻击的公钥加密、签名和密钥封装/建立算法，以替代美国现有的 FIPS 186 和 SP 800-56A/B/C 标准中的 RSA 和椭圆曲线离散对数类公钥密码算法。早在 2012 年，NIST 便开始了对后量子密码的研究，建立相关团队，跟进业界进展，联络工业和国际标准化组织，以筹备该标准化项目。

2016 年，NIST 通过 PQCrypto、亚洲抗量子密码论坛等会议平台进行宣传，以呼吁全球密码学家积极参与；并于 2016 年 12 月发布了正式的算法征集公告 NIST IR 8105。截止到 2017 年 11 月底，共征集到来自全球 25 个国家的 82 个提案，其中 69 个算法满足 NIST 的“完整且合适”接受准则，**进入第一轮评估**。这包含了 3 个来自中国的算法，和 22 个来自欧盟的算法。2019 年初，NIST 发布第一轮评估报告 NIST IR 8240，并宣布有 26 个算法进入**第二轮评估**。2022 年 7 月，NIST 发布第三轮评估报告 NIST IR 8413，**宣布了第一批标准算法。**此外，基于编码的 Classic McEliece、BIKE 和 HQC 以及基于超奇异椭圆曲线同源的 SIKE 进入第四轮评估。NIST 于 2023 年 8 月 24 日发布**第一批抗量子密码算法标准草案**，包括 Crystals-Kyber（FIPS.203）、Crystals-Dilithium（FIPS.204）和 SPHINCS+（FIPS.205），第四种 Falcon 的标准化草案将会在 2024 年发布。

表29：NIST 抗量子密码标准化项目进程

时间	内容
2012 年	NIST 开始对抗量子密码的研究，建立团队，跟进业界进展，联络工业和国际标准化组织
2016 年	NIST 通过 PQCrypto、亚洲抗量子密码论坛等会议平台进行宣传，以呼吁全球密码学家积极参与，并于 12 月发布**算法征集公告 NIST IR 8105**。
2017 年 11 月	共征集到来自全球 25 个国家的 82 个提案，其中 69 个算法满足 NIST 的“完整且合适”接受准则
2019 年初	**NIST 发布第一轮评估报告 NIST IR 8240**
2020 年 7 月	**NIST 发布第二轮评估报告 NIST IR 8309**
2022 年 7 月	**NIST 发布第三轮评估报告 NIST IR 8413**
2022 年 7 月	NIST 宣布将继续征集额外的数字签名算法，尤其欢迎不同于有结构格技术路线的具有“签名短、验证快”优势的通用签名算法提案，这一征集独立于原项目第四轮评估进行
2023 年 7 月	NIST 公布 40 个进入额外数字签名征集的算法
2023 年 8 月	发布第一批抗量子密码算法标准草案

来源：“密码+”应用推进计划研究报告，光子盒公众号，科信量子，国投证券研究中心

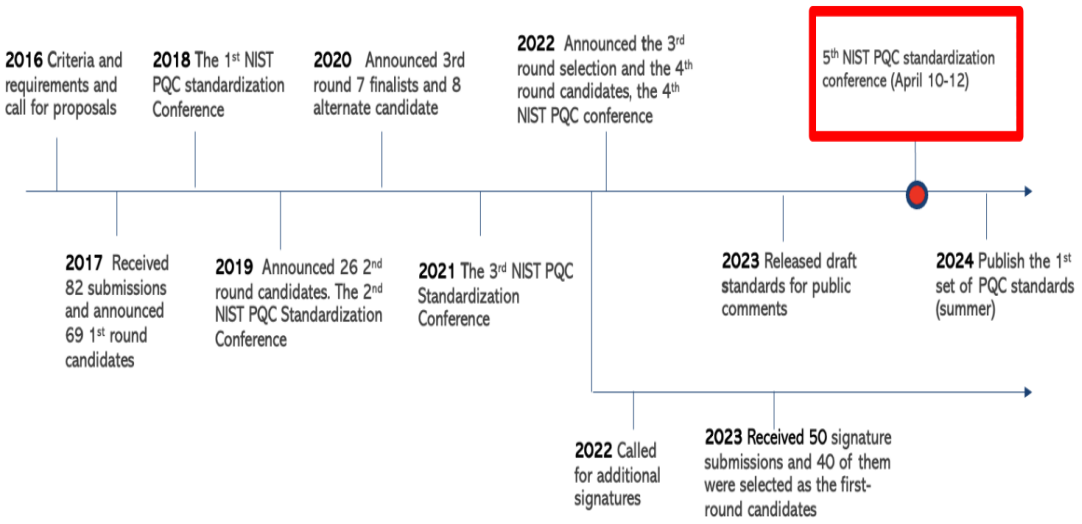
表30：NIST 筛选标准（开发者最低标准建议）

序号	开发者最低标准建议	内涵
1	威胁建模	威胁建模方法创建对系统的抽象、潜在攻击者画像如目标和方法以及创建潜在威胁的分类。应当在开发过程中多次进行威胁建模，尤其是在开发新能力过程中，以便捕捉到新威胁并改进建模。威胁建模可提示哪些输入向量最值得注意，对这些特定输入的变体进行测试应当放到更高的优先级。威胁建模可能会披露某少量代码（通常少于 100 行）具有重大风险。
2	自动化测试	文档建议开展自动化测试，持续运行测试、准确地检查结果并将对人工和专业知识的需求降到最低。自动化测试可集成到现有的工作流中或发布追踪系统。随着测试的自动化，可经常开展测试比如对每个 commit 或在问题过期前进行测试。
3	基于代码的分析或静态分析	NIST 建议使用静态分析工具检查代码中的很多种漏洞，以及检查与组织机构编码标准的合规性。对于多线程或平行处理软件，使用能够检测出竞争条件漏洞的扫描工具。
4	审计硬编码机密	NIST 建议使用启发式工具检查代码中的硬编码密码和私钥。这类工具是可行的，因为将这些作为参数的功能或服务具有特定的接口。动态测试不可能发现这类多余代码。
5	通过编程语言提供的检查和防护措施运行	编译语言和解释性语言提供了很多内置检查和防护措施，在开发过程中和软件交付过程中使用这些能力，也要启用硬件和操作系统安全和漏洞缓解机制。
6	黑盒测试用例	“黑盒“测试并非基于实现或特定代码，而是基于功能标准或要求、负面测试、拒绝服务和过载、输入边界分析和输入结合。在通用安全原则认为安全敏感或关键的地方，测试用例应该更加全面。
7	基于代码的测试用例	假设软件要求处理最多 100 万哥项目,程序员可能决定让软件在统计分配的表格中处理 100 个或更少的项目，但如果出现 100 多个项目则动态分配内存。对于这种实现，可能会有 100 个、99 个或 101 个项目以便测试不同方法下的漏洞。内存对齐可能意味着额外测试。无法仅通过标准来确定这些重要的测试用例。基于代码的测试用例可能也源自覆盖矩阵，多数代码应当在单元测试过程中执行，建议执行测试套件实现最低 80%的语句覆盖率。
8	历史测试用例	某些测试用例的创建就是为了显示漏洞的存在或消失，有时被称作“回归测试“。这些测试在早期是重要的测试来源，在”第一原则“保证方法出现之前应该检测到 bug。更好的方法是使用保证方法如选择语言来完全排除 bug。从生产操作记录的输入可能也是测试用例的良好来源。
9	模糊测试	NIST 建议使用模糊测试工具执行自动化的主动测试，即模糊测试工具在测试过程中创建海量输入。通常很小的输入部分就会触发代码问题。另外，这些工具仅执行一般检查来判断软件正确地处理了测试。一般而言仅会监控宽泛的输出特征和恶意行为如应用崩溃。一般化的优势在于这些工具可通过最少的人工监控来尝试庞大的输入。这些工具可通过通常暴露 bug 的输入（如非常长或空的输入和特殊字符）进行编程。
10	Web 应用扫描	如果软件提供了 web 服务，则使用动态应用安全测试或交互应用安全测试工具。和模糊测试工具一样，Web app 扫描工具监控一般的异常行为。混合工具或 IAST 工具可能也会监控程序执行中的内部错误。当输入引发某些可检测的异常情况，则工具可使用输入变体来检测失败情况。
11	检查所包含的软件组件	使用以上提到的验证技术保证所包含的代码起码和本地开发的代码一样安全。某些保证可能源于自认证或部分自认证信息如核心基础设施倡议 (CII) 最佳实践徽章或可信任的第三方检查。必须持续监控软件组件中的已知漏洞数据库，可能随时会报告现有代码中的新漏洞。

来源：“密码+”应用推进计划研究报告，光子盒公众号，奇安信公众号，NIST 官网，国投证券研究中心

2024 年 4 月 10 日至 12 日，美国国家标准与技术研究院（NIST）在马里兰州罗克维尔举办第五届 NIST PQC 标准化会议，该会议的目的是对 PQC 算法进行全面讨论（包括已选定和正在评估的算法），以获得有价值的反馈。在会议上，Matt Scholl 明确提到：2024 年到 2030 年，必须升级到抗量子算法。2030 年 CRQC 即破解专用量子计算机，可能会出现。Dustin Moody 表示：**2024 年夏季有望提供 PQC 标准化算法出版物，而第四轮筛选将在 2024 年秋季完成。**

图118. NIST 第五节标准化会议公布的时间轴



资料来源：NIST，国投证券研究中心

表31：入选 NIST 标准的四种算法及入围第四轮筛选的四种算法

阶段	算法名称	基于哈希	基于编码	基于多变量	基于格	其他
入选标准化算法	CRYSTALS-Kyber				√	
	CRYSTALS-Dilithium				√	
	Falcon				√	
	SPHINCS+	√				
入围 NIST 第四轮筛选	BIKE		√			
	Classic McEliece		√			
	HQC		√			
	~~SIKE~~ （在 5th Conference 上被否定）					√

来源：“密码+”应用推进计划研究报告，NIST 官网，国投证券研究中心

欧盟：欧盟委员会呼吁其成员国采取统一战略，过渡到抗量子密码学。这一转变对于保护欧盟数字基础设施免受量子计算进步带来的新威胁至关重要。欧盟在抗量子密码上的政策可以从战略层面和经费层面分类。

表32：欧盟抗量子密码政策

视角	时间	内容
战略层面	2020 年	欧盟在其网络安全战略中特别强调量子计算与加密技术的重要性，以强调量子计算与加密技术对于确保关键基础设施安全的重要性。
	2021 年 2 月	欧盟网络安全局 ENISA 发布《抗量子密码学：现状和量子迁移》报告，概述抗量子密码的当前状态和迁移挑战
	2022 年 10 月	ENISA 发布《抗量子密码：集成研究》报告，详细介绍将后量子算法集成到现有 ICT 系统和新安全协议的设计思路
经费层面	2015-2018 年	欧盟地平线抗量子密码方面的 PQCRYPT 项目投入 390 万欧元，支持相关研究和发展
	2018 年	欧盟启动量子旗舰研究规划，支持包括 OpenSuperQ 在内的 20 余个研究项目，旨在构建量子计算机和提升量子技术
	2019 年	欧盟启动 EuroQCI 创新框架项目，目标是在 10 年内研发和部署欧盟境内端到端安全的量子通信关键基础设施，项目包括地面和空间通信方案，且要求达到 EAL4+的高安全级别认证。
	2021-2033 年	EuroHPC JU 将投资 80 亿欧元，用于量子计算和量子模拟的基础设施建设，以及与高性能计算基础设施的集成

来源：“密码+”应用推进计划研究报告，光子盒公众号，国投证券研究中心

德国：近年来，德国政府机构呼吁尽快采用后量子加密技术以抵御潜在的量子威胁。德国联邦信息安全办公室(BSI)等机构陆续出台政策，应对量子时代的到来。

表33：德国抗量子密码政策

视角	时间	内容
战略层面	2015 年	德国联邦教育与科研部 BMBF 发布《2015-2020 年数字世界的自主和安全》政策报告，声明促进长效安全密码及其应用实现的研发
	2020 年 8 月	德国信息安全联邦办公室 BSI 发布关于迁移到抗量子密码的推荐建议
	2021 年	德国联邦内政部 BMI 发布《德国网络安全战略》，指出通过量子技术保障 IT 安全的战略需要，包括在高安系统中进行量子安全密码的迁移
	2022 年 5 月	BSI 发布《量子安全密码—基础，现状和推荐》技术白皮书，推动安全系统的后量子迁移
经费层面	2018 年	BMBF 公布《抗量子密码》研究申请指南，计划在 2019-2022 资助周期内遴选七个研究项目，总研究经费为 2420 万欧元
	2018 年	BMBF 发布《量子技术-从基础研究到市场》的研究规划，目标是在 2018-2022 年提供 6 亿 5 千万欧元经费，用于面向应用和有商业化潜力的量子技术研发

来源：“密码+”应用推进计划研究报告，光子盒公众号，国投证券研究中心

欧洲国家中，英国、法国自 2020 年以来，发布了有关后量子迁移的一些政策。加拿大提出为应对量子计算威胁，新型的抗量子密码(POC)标准正在制定，同时有必要考虑可选的、互补的安全解决方案，例如量子保密通信。

表34： 英国、法国、加拿大抗量子密码政策

国家	时间	内容
英国	2020 年 11 月	国家网络安全中心 NCSC 发布白皮书，提出应对量子计算威胁的安全迁移观点，为技术决策者提供后量子迁移背景信息
法国	2022 年 1 月	信息系统安全局 ANSSI 公布立场文件，为安全产品工业界提供指导，为“Security Visas”安全认证计划规划迁移时间线
加拿大	2023 年 3 月	国防部和武装部队（DND/CAF）发布量子科学和技术战略实施计划《Quantum 2030》，确定国防和安全方面的量子技术任务，提出制定新型抗量子密码（PQC）标准，考虑量子保密通信等互补的安全解决方案

来源：“密码+”应用推进计划研究报告，光子盒公众号，国投证券研究中心

中国在抗量子密码研究项目中给与政策和资金支持，鼓励量子计算和抗量子密码的技术创新和产业发展。2022 年，人民银行《深化金融科技应用、推进金融数字化转型提升工程》相关工作部署中把“探索量子技术金融应用”作为重要的工作任务，加快推进抵抗潜在量子计算攻击的能力研究。2022 年中央经济工作会议首次明确提出加快量子计算等前沿技术的研发和应用推广，但尚未发布后量子密相关政策文件。

表35：中国抗量子密码进展

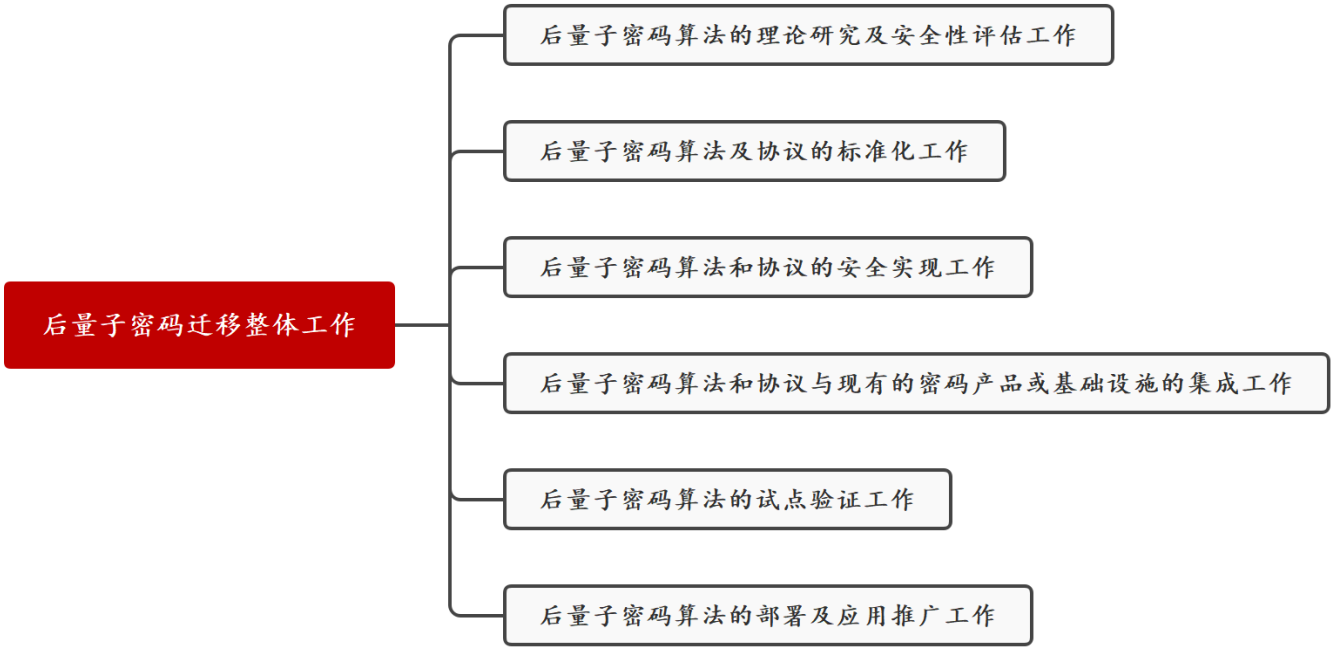
时间	政策进展
2016 年	“十三五”规划中明确设立关于“量子通信与量子计算机”的重大科研项目。
2021 年	“十四五”规划，指出这 5 年是中国量子技术实现“弯道超车”的关键时期，其目标之一就是研制通用量子计算原型机和实用化量子模拟机。
2021 年 10 月	量子密钥分配(QKD，也叫量子密钥分发)首次进入国家密码行业标准，包括《GM/T 0108-2021 诱骗态 BB84 量子密钥分配产品技术规范》《GM/T 0114-2021 诱骗态 BB84 量子密钥分配产品检测规范》两项标准。
2022 年	人民银行《深化金融科技应用、推进金融数字化转型提升工程》相关工作部署中把“探索量子技术金融应用”作为重要工作任务，加快推进抵抗潜在量子计算攻击的能力研究。
2023 年 8 月	工业和信息化部发布的《量子保密通信网络架构》、《量子密钥分发（QKD）网络 网络管理技术要求 第 1 部分：网络管理系统（NMS）功能》《基于 IPSec 协议的量子保密通信应用设备技术规范》三项量子保密通信相关的通信行业标准落地实施。
2023 年 8 月	中国台湾成立量子安全迁移中心。
时间	**产业/进展**
2007 年	中国科学家潘建伟首次在量子计算机上实现 Shor 量子分解算法。
2019 年 5 月	第十届量子密码国际会议（The Tenth International Conference on Post-Quantum Cryptography）在重庆举办。
2020 年 6 月	利用“墨子号”量子科学实验卫星在国际上首次实现千公里级基于纠缠的量子密钥分发。
2021 年 7 月	国盾量子、中国科大、国科量子、济南量子院与上海交大等单位组成的联合团队完成了国际首次量子密钥分发(QKD)和抗量子密码(PQC)融合可用性的现网验证。
2021 年 11 月	南京大学马小松教授、吴培亨院士、祝世宁院士、陆延青教授等联合中山大学蔡鑫伦教授等成功开发了用于 MDI-QKD(测量设备无关的量子密钥分发)的异质集成超导硅光子芯片。
2022 年 4 月	香港科学技术大学物理系曾葆教授团队在预印论文《用于量子纠错的量子变分学习》中提出了 VarQEC（抗噪声的变分量子算法），并可以通过硬件高效的编码电路来搜索量子码。这一成果为理解量子纠错码提供了新的思路，也将有助于通过信道自适应纠错码来提高设备的短期性能。
2022 年 7 月	清华大学无锡应用技术研究院产业化公司无锡沐创集成电路设计有限公司推出抗量子攻击商用密码芯片 PQC 1.0，支持 NIST 公布的抗量子攻击算法 CRYSTALS-KYBER 和 CRYSTALS-Dilithium。

来源：“密码+”应用推进计划研究报告，光子盒公众号，国投证券研究中心

4.3. 抗量子密码迁移进程逐渐开启，产业蓄势待发

抗量子密码迁移是确保现有加密系统在面临量子计算威胁时保持安全的重要举措。抗量子密码迁移不仅仅是替换密码算法，它还包括将密码协议、密码方案、密码组件、密码基础设施等更新为量子安全的密码技术，甚至还包括密码系统的灵活更新机制的能力构建及密码应用信息系统的迭代更新等，是将现有密码安全体系分阶段平稳过渡到抗量子密码安全标准体系所需的一系列过程、程序和技术。考虑到抗量子密码的复杂性以及稳定性，目前多数倾向于采用“两把锁、双保险”的混合模式进行过渡，而不是直接替换的模式。

图119. 抗量子密码迁移整体工作

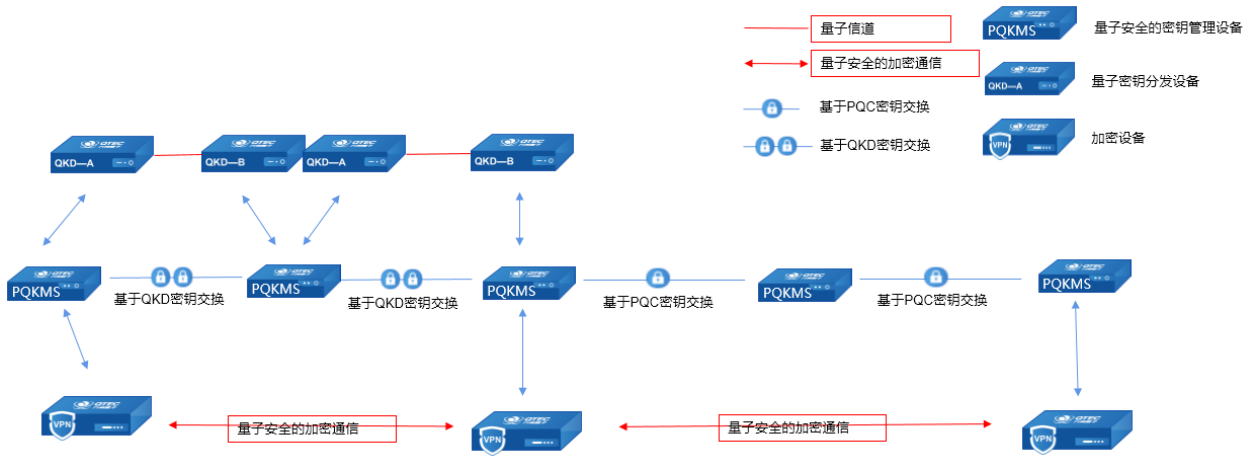


资料来源：“密码+”应用推进计划研究报告，国投证券研究中心

QKD 和 PQC 融合应用有望成为产业趋势。QKD 和 PQC 是目前学术界公认的应对量子计算威胁的两个技术路径和方向。国际较为普遍的观点是 QKD 具有长效安全性，但缺少认证手段、应用成本相对较高；PQC 具有功能和应用体系与传统密码兼容的优势，但缺少安全性证明。将两个抗量子计算威胁的技术融合应用，可能是更为有效的方法。

QKD 大型组网使用需要光纤资源，受地理环境影响较大，应用成本相对较高，采用基于 QKD+PQC 融合组网的方式能有效降低成本。通过量子安全密钥管理设备将加密密钥传输从数据通道分离出来，并进入一个单独的密钥管理子系统，该子系统可以按需配置。一个典型的融合网络配置由一系列的节点组成，其中一些节点与加密数据链路的加密设备通信，一些节点作为可信中继节点。存在成对 QKD 连接的量子安全密钥管理设备通过基于 QKD 完成密钥交换，不存在成对 QKD 连接的节点基于格的 PQC 密钥交换协议完成密钥交换。因此，QKD+PQC 融合组网的方案有望成为未来的产业趋势。

图120. QKD+PQC 融合组网方式



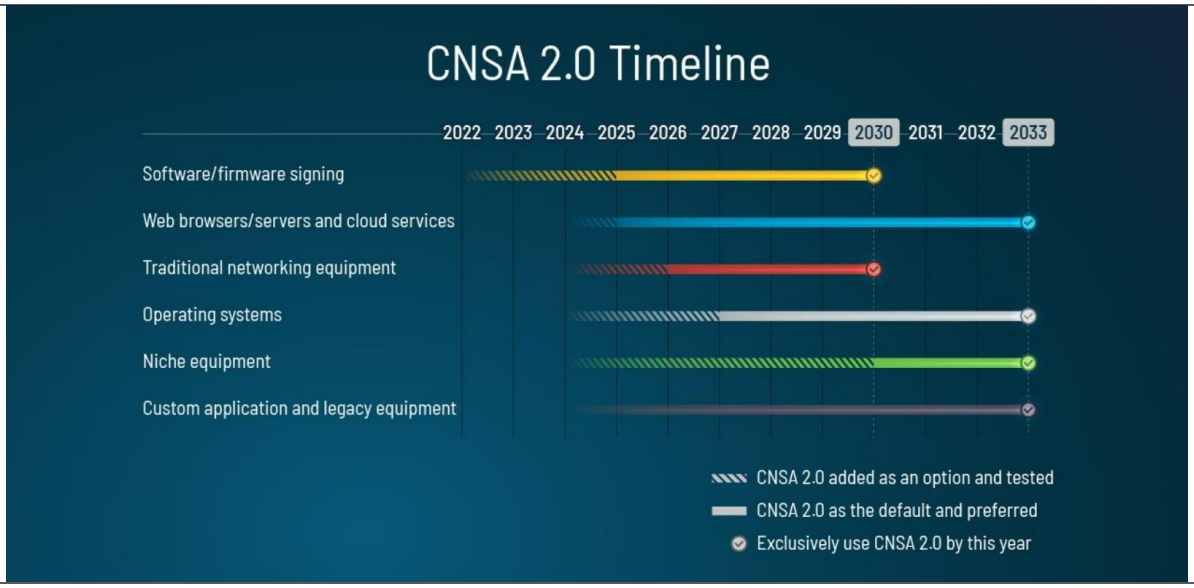
资料来源：“密码+”应用推进计划研究报告，国投证券研究中心

美国国家安全局（NSA）明确迁移路线图，产业蓄势待发。目前，最为明确的康量子密码迁移时间表为美国 NSA 发布的《商业国家安全算法套件 2.0》。（注：CNSA 1.0 是当前标准，而 CNSA 2.0 是未来的标准。NSA 建议现在采用 CNSA 2.0 软件和固件签名算法。）具体而言，对于软件和固件签名的场景，CNSA 2.0 推荐使用 NIST SP 800-208 所给出的基于 hash 的签名算法 LMS 和 XMSS。与基于格的后量子签名标准算法 Dilithium 和 Falcon 相比，这两个基于 hash 的签名算法的特点是私钥有状态，需要小心维护和更新。另外，单个私钥所支持的签名数量有限，而且签名和验签的速度慢。这使得它们可能不如无状态签名通用。关于对称算法，CNSA 2.0 推荐使用 AES 256，SHA384 或 SHA512。对于通用场景下的公钥算法，CNSA 2.0 推荐用 Kyber 和 Dilithium 来代替 RSA、DH、ECDH 和 ECDSA，并且建议使用最高等级的 NIST Level 5 参数。CNSA 2.0 针对的是美国国家安全系统，对于民用系统，特别是中、低安全的民用系统，可以根据安全需求和性能平衡选择更合适的参数。

对于不同场景下的抗量子迁移时间线，CNSA 2.0 给出的要求如下：美国政府将在 2033 年之前完成其信息系统中的抗量子迁移。其中，对于软件/固件签名场景的迁移，需立即启动，在 2030 年前完成；传统网络设备的迁移在 2025 年左右启动，也需在 2030 年前完成。

我们认为，美国 NSA 明确了抗量子密码的迁移路线图，结合 NSIT 即将发布的第一版抗量子密码算法标准，标志着产业即将进入商业化落地的阶段。而抗量子密码的发展在全球范围内已经形成共识，中国也有望积极布局，从而带来对密码产业新的发展和投资机会。

图121. CNSA2.0 迁移路线图



来源：NSA 官网，国投证券研究中心

表36：CNSA2.0 迁移时间线解读

场景	支持和优先使用	完全使用
软件/固件签名	2025 年	2030 年
网络浏览器/服务器和云服务	2025 年	2033 年
传统网络设备(如 VPN、路由器)	2026 年	2030 年
操作系统	2027 年	2033 年
Niche 设备(如资源受限设备、大型 PKI 系统)	2030 年	2033 年
应用程序和遗留设备	2033 年前更新或替换	

来源：NSA 官网，国投证券研究中心

5. 相关标的梳理

5.1. 国盾量子

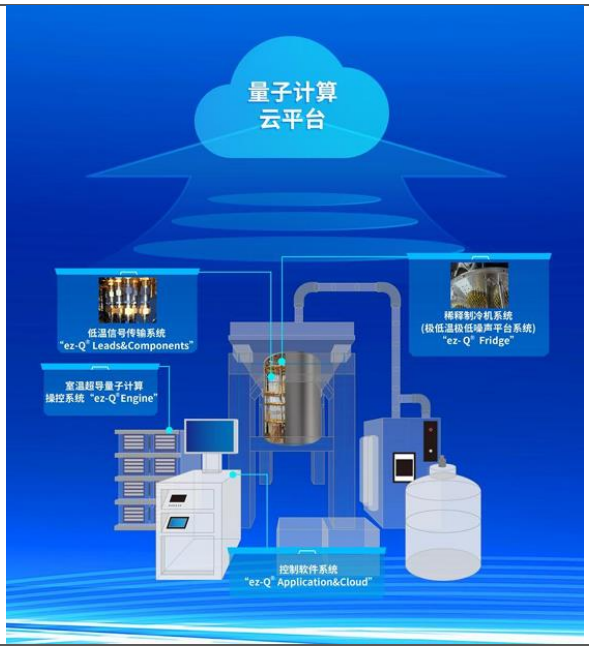
国盾量子围绕量子信息技术的产业化开展业务，主要提供量子通信、量子计算、领子精密测量的产品及解决方案。公司量子通信产品主要包括量子保密通信网络核心设备、量子安全应用产品、核心组件以及量子保密通信网络的管理与控制软件，并提供机遇量子通信的技术开发及验证服务、量子保密通信网络运维服务、面向量子安全应用的相关技术服务等。

图122. 国盾量子：量子保密通信产品及下游应用

资料来源：国盾量子年报，国投证券研究中心

国盾量子的量子计算仪器设备产品主要分为超导量子计算子系统、整机解决方案以及云平台三部分，目前主要包括室温超导量子计算操控系统到控制软件系统、低温信号传输系统等。

图123. 国盾量子：量子计算产品矩阵



资料来源：国盾量子年报，国投证券研究中心

国盾量子在量子精密测量领域产品主要包括冷原子重力仪、飞秒激光频率梳、单光子成像等设备，以及光学传感器、单光子探测器等组件，并提供量子精密测量相关技术服务。

图124. 国盾量子：量子精密测量产品矩阵

资料来源：国盾量子年报，国投证券研究中心

此外，国盾量子近期在量子芯片、标准制定、产品创新等方面均有进展。**量子芯片方面，**国盾量子接收了中国科学院量子信息与量子科技创新研究院交付的 504 比特超导量子计算芯片“骁鸿”，这是国内首款超过 500 比特的超导量子计算芯片，用于验证国盾量子自主研制的千比特测控系统，并计划通过中电信量子集团的“天衍”量子计算云平台向全球开放。**标准制定方面，**国盾量子参与制定了思想量子领域的国家标准，涵盖量子通信和量子测量领域，为量子技术的推广和应用提供重要支撑。**产品创新方面，**国盾量子在量子通信领域推出了“国盾密邮”和“国盾密语耳机”等创新产品，并在电信、电力和办公等领域实现了应用。此外，公司还在量子精密测量方面丰富了产品线，如单光子探测和光学传感组件。

5.2. 国芯科技

国芯科技联合安徽问天量子科技股份有限公司和合肥硅臻芯片技术有限公司，共同建立了量子芯片联合实验室，专注于量子芯片研发和产业化尤其在物联网、云计算、先进存储和智能终端等领域。同时，国芯科技推出多种量子安全产品，如量子安全芯片、量子安全 TF 卡、量子安全 U 盘 key 和量子安全 PCI-E 密码卡，在存储量子会话密钥、提供高安全性鉴权机制等方面发挥重要作用，为信息安全领域带来全新的解决方案。

国芯科技积极开展量子技术合作，实现信创和信息安全芯片的迭代升级。**量子保密通信方面，**根据公司年报，公司作为硅臻芯片的股东，持有其 12.1073%的股权，是管理团队以外的第一大外部股东。硅臻芯片的量子随机数发生器芯片 QRNG-10 通过了国家密码管理局商用密码检测中心的密码检测。硅臻芯片与国芯科技共建了智能终端量子安全芯片联合实验室，双方将开发适于“量产应用”的量子安全智能终端可用芯片及设备，联合推动量子技术的实用化落地。**量子计算方面，**硅臻芯片在光量子芯片方面进展显著，可提供的量子纠缠光源芯片包括硅螺旋波导芯片、片上横向波导模式纠缠光源芯片、基于 SiN 材料的环形微腔量子纠缠光源芯片、两光子高维路径纠缠光源芯片等。

图125. 硅臻量子随机数发生器芯片

资料来源：硅臻量子，国投证券研究中心

5.3. 普源精电

收购耐数电子协同创新，强化量子计算布局。普源精电通过收购耐数电子，与耐数电子技术与创新能力进行协同，共同推进量子计算测控技术的发展。 耐数电子具有数字化的全栈量子测控解决方案，采用高采样率、高模拟带宽、低噪声的射频直出式通道技术，实现对量子比特的数字化测控，极大地提升了量子测控的集成度，以适应日益增长的量子测控规模。模块化的设计也具有极高的配置灵活度，可以满足用户不同规模的测控需求，同时具有量子测控专用的反馈纠错指令集。此外，普源精电的模块化技术能够响应客户在遥感与通信领域、射电天文领域、量子信息领域、工业自动化测量等领域的系统需求。

图126. 耐数电子 NS-Q100 量子测控系统

资料来源：光子盒公众号，国投证券研究中心

5.4. 科华数据

科华数据于 2023 年 4 月于玻色量子达成战略合作，共同推进以光量子计算机为代表的新型算力设备在现有数据中心的应用，构建更加先进、多元化、面向未来的算力基础设施。**量子计算机开发方面，**玻色量子发布了新一代 550 计算量子比特的相干光量子计算机“天工量子大脑 550W”。这个系统基于自研的“空间光路+光纤光路”的异构光路体系架构，采用相干光脉冲相位编码来制备量子比特。该计算机具备高功率态制备、高保真内存、低噪环控、自适应纠错等性能优势，并能在数个毫秒级时间内进行并行搜索，求出优化解，实现了比经典计算在实际应用问题上的数万倍加速。

量子计算与人工智能融合方面，玻色量子强调量子计算与人工智能（AI）的融合，作为实用化量子计算的起点。通过其开发的“开物 SDK”开发套件，玻色量子实现了 QUBO 模型转化、自动调参、真机模拟的自动化，简化了用户的使用流程，无需接入真机即可模拟编程求解。

下游应用方面，玻色量子与深圳华大生命科学研究院达成战略合作，共同探索量子计算在生命科学领域的应用。生命科学数据量大、增长速度快、数据质量低、数据多模态的特点，对算力提出了较高的要求。通过这次合作，玻色量子与华大研究院计划基于量子计算在生命科学中的应用场景，联合打造行业真实场景解决方案，并推动科技成果转化和应用。

图127. 玻色量子天宫量子大脑 550W 的特性

资料来源：玻色量子，国投证券研究中心

5.5. 中国长城

公司与国防科大共建中国长城量子实验室，主要开展基于光量子和拓扑超导量子计算的基础科研，以及量子芯片加工设备等方面的科研工作。根据公司官网介绍，中国长城致力于打造“安全、先进、绿色的自主计算底座”，公司曾研发出我国第一台具有自主知识产权的中文微型电脑、第一块电脑硬盘、第一款终端 ASIC 芯片、第一台显示器、第一台光纤转换器、第一台光笔图形显示终端等。中国长城坚持“芯端一体，双核驱动”的发展战略，致力于构建以“芯-端”为核心的自主计算产品链，全面带动“网-云-数-智”自主计算产业生态发展。

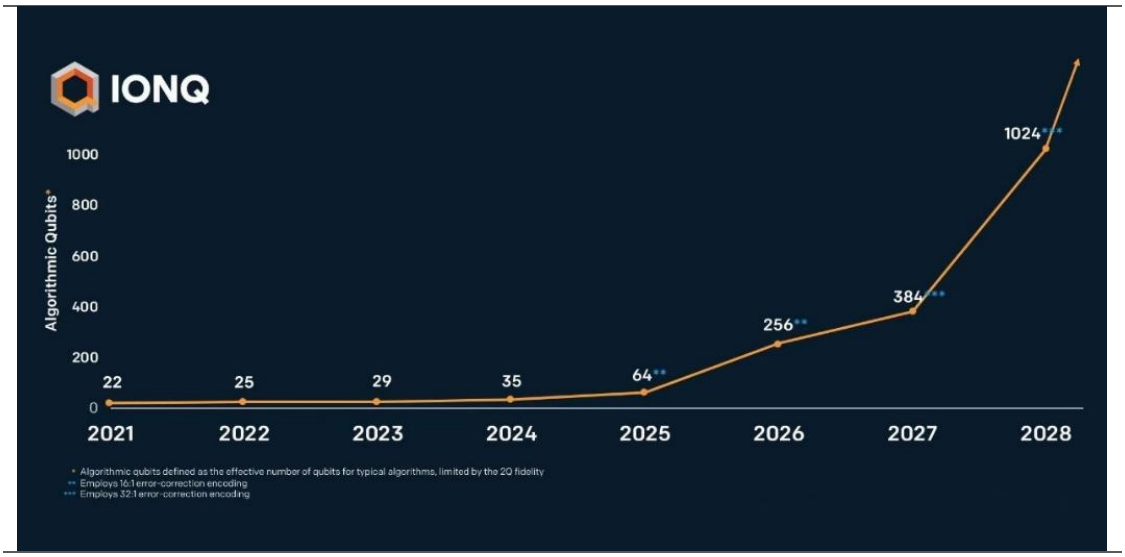
图128. 中国长城智慧计算与存储业务

资料来源：中国长城官网，国投证券研究中心

5.6. IonQ

IonQ 采用离子阱技术方案，出售几种不同量子位容量的量子计算机的访问权限，并正在研究和开发计算能力不断增强的量子计算机技术。IonQ 公布了其离子阱量子计算机的五年发展路线图，计划在 2023 年之前部署机架式模块化量子计算机，并在 2025 年实现“广泛的量子优势”。此外，2024 年 2 月 22 日，IonQ 宣布其研究团队已实现可重复地生成与离子纠缠的光子，从而创建了一种新的量子态，使得未来的量子系统能在彼此之间通信和传输信息。这是光子—离子纠缠在学术环境之外的首次商业演示，标志着 IonQ 在量子网络和光子互连方面迈出的重要一步，有助于在下一代量子系统中提供更高的计算能力。

图129. IonQ：技术路线图

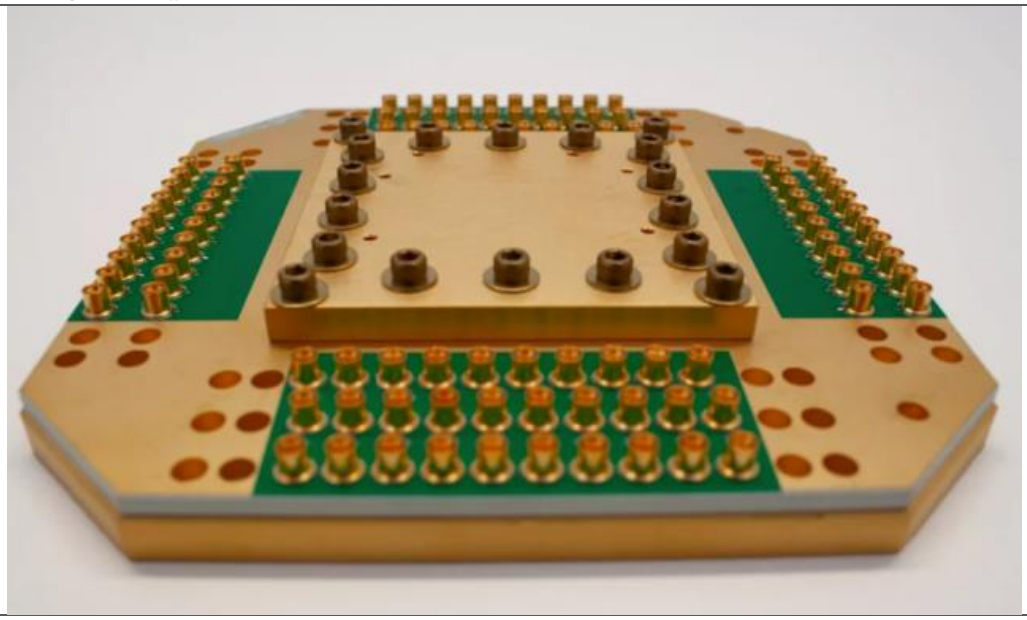


资料来源：IonQ，国投证券研究中心

5.7. Regetti Computing

Rigetti 是一家全栈量子计算公司，构建了超导量子计算系统并通过云提供访问。Rigetti 量子云服务平台为全球企业、政府和研究客户提供服务，Regetti 专有的量子经典基础设施为实用量子计算提供了与公共和私有云的高性能集成。Rigetti 推出的 Aspen-M 是世界上第一个商用多芯片量子处理器，在规模、速度和保真度方面进行了改进，提高了量子程序结果的可靠性。Rigetti 的长期目标是展示实现量子优越性，即利用量子计算机来更好、更快、更便宜地解决目前经典计算机难以解决的现实问题。为此，Rigetti 正在追求量子硬件在规模和性能上的持续、快速改进，并与不同行业和应用领域的合作伙伴合作，从开发最适合一些“狭义”量子优越性的实例的硬件开始，最终将变得更加通用。

图130. Regetti：Aspen-M 商用多芯片量子处理器

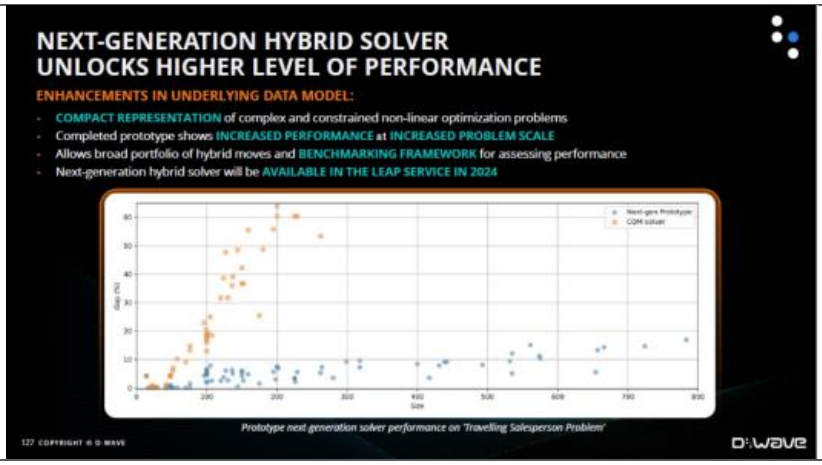


资料来源：Regetti，国投证券研究中心

5.8. D-Wave Quantum

D-Wave 是量子计算系统、软件和服务开发和交付领域的领导者，是世界上第一家量子计算机商业供应商，也是一家同时开发退火量子计算机和门模型量子计算机的公司。D-Wave 多年来开发和增强的重要技术之一是求解器，求解器技术允许将问题转为二次模型并以高水平输入，同时求解器还可以被编译为在量子退火机上运行的硬件配置。同时，D-Wave 还积极改进其 Ocean 软件，为客户提供量子与经典混合环境中的软件开发工具，结合 Leap Quantum 云服务为客户提供量子计算机和混合求解器的实时、安全的云访问。

图131. D-Wave：下一代混合求解器的高水平性能



资料来源：D-Wave，国投证券研究中心

硬件技术方面，D-Wave 持续推进量子退火和基于门的硬件研发工作。D-Wave 一直致力于开发 Advantage 系列产品，并持续构建规模不断增加的量子技术原型机。

图132. D-Wave：Advantage 系列退火机开发进度

资料来源：D-Wave，国投证券研究中心

5.9. 神州信息

神州信息子公司神州数码系统集成服务有限公司参与了国内量子保密通信骨干网的集成建设，是量子保密通信干线的重要服务商之一，承建了京沪、沪合、汉广、武合、粤港澳大湾区干线及多个重点城市的量子城域网建设项目。此外，公司携手国盾量子等成立子公司“神州国信”（根据 2023 年报披露，公司目前持股比例为 69.10%），探索产品研发及行业应用，自主研发了数据加密传输、终端安全接入、安全即时通信、保密视频会议、安全数据加密等典型解决方案。

图133. 神州信息中标量子保密通信骨干网工程

国家广域量子保密通信骨干网络建设工程项目（北京-武汉段及相应 IP 承载网）

系统集成服务采购中标结果公示

（招标编号：0747-2060SCCSHX01 ）

本北京-武汉、武汉-广州、上海-合肥段骨干网络及 IP 承载网系统集成服务采购（招标项目编号：0747-2060SCCSHX01），确定 *(001)国家广域量子保密通信骨干网络建设工程项目（北京-武汉段及相应 IP 承载网）系统集成服务采购* 的中标人如下：

一、中标人信息：

(001)国家广域量子保密通信骨干网络建设工程项目（北京-武汉段及相应 IP 承载网）系统集成服务采购

中标人信息：中标人:神州数码系统集成服务有限公司 中标金额:27949617.14 元;

二、其他公示内容：

项目名称：国家广域量子保密通信骨干网络建设工程项目（北京-武汉段及相应 IP 承载网）系统集成服务采购

项目编号：0747-2060SCCSHX01/标段 1

招标人名称：国科量子通信网络有限公司

资料来源：招标网，国投证券研究中心

5.10. 浙江东方

公司下属控股子公司浙江神州量子通信技术有限公司建设的“沪杭量子商用干线”已融入国家量子通信骨干网。沪杭控制通信商用干线全长 260 公里，依托杭沪、杭甬高速作为路线路径，利用已有光纤资源，铺设量子光纤，为沿线地区的政府部门、金融机构或大中型企业提供基于量子安全的专网通信服务。神州量子通信技术有限公司致力于浙江省和长三角地区量子干线网络的建设运营、量子技术与网络通信和数据安全的应用研发推广，努力为相关机构及企业提供完整的数据传输服务以及基于量子安全的专网通信服务，实现量子通信技术与用户需求的结合。

图134. 浙江神州量子通信展台

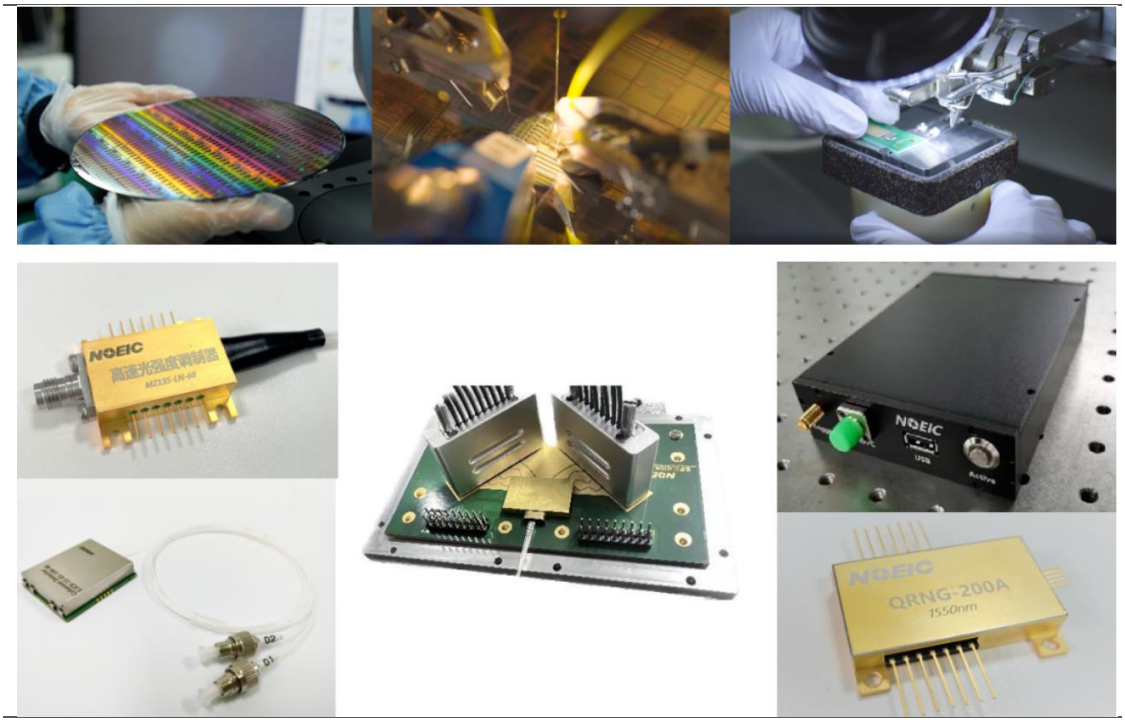
资料来源：神州量子通信微信号，国投证券研究中心

5.11. 光迅科技

光迅科技与科大国盾量子技术股份有限公司成立合资公司**山东国讯量子芯科技有限公司**，公司持有山东国迅量子 45.00%股权，国迅公司的量子芯片主要应用在 QKD 通信与量子测量等领域，产品研发主要瞄准下一代量子信息系统设备所需的集成化、高性能光电子芯片与器件。从产业链来看，光迅科技自 2016 年开始在量子通信领域进行前瞻布局，掌握信号处理芯片和雪崩光电二极管等领域领先的研发和制造实力，并通过收购上下游产业链企业，逐步实现了“芯片研发-器件制造-高端封装”一体化生产和全产业链垂直布局。

2023 年，光迅科技承接的工信部《信息光电子创新中心能力建设项目》通过验收，项目开展了一系列关键光子集成芯片和器件产品的攻关。完成国内首款商用 100Gb/s 硅光芯片及 400Gb/s 的正式投产及规模应用，多款商用芯片取得产业化突破，在光传感、光量子、光测量等领域研制出一批特种光电芯片和器件产品，填补国内空白。在支撑我国通信系统核心器件自主可控方面发挥了重要作用。

图135. 光迅科技光通信产品



资料来源：光迅科技微信号，国投证券研究中心

5.12. 亨通光电

在通信业务方面，亨通光电围绕“技术领先、成本领先、质量领先、服务领先”，打造引领行业发展的全球信息与能源互联解决方案服务商。拥有从新一代绿色光棒-光纤-光缆-光网络-数据中心全价值光通信产业链，及光纤传感、5G 等新一代网络关键技术，形成“产品 + 方案 + 工程”的服务模式，全面布局工业互联网等基于新一代通信技术及“万物互联”的垂直应用场景，跻身全球光纤通信行业前 3 强。**亨通光电围绕“下一代通信技术”，在量子保密通信、硅光技术等领域投入研发**，荣获国际电联 ITU2019 年信息社会世界峰会中国区最高奖。

2020 年，公司承接的“长三角量子通信环网”、“京津冀量子通信环网”的建设，已逐步投入运营。同时公司积极推动量子通信产业化应用，成功交付的苏州量子保密政务网是量子保密通信技术在江苏省政务领域的第一次试点应用。

图136. 亨通光电量子通信解决方案

资料来源：公司官网，国投证券研究中心

图137. 亨通光电量子通信具体产品

资料来源：公司官网，国投证券研究中心

5.13. 迪普科技

迪普科技是全国首条量子通信光纤链路（京沪干线）等国家级重大项目的安全产品提供商，量子通信干线安全产品提供商。“京沪干线”总长 2000 余公里，共设有 32 个量子通信节点。为确保各节点的边界安全，经过全面的测试与评估，**“京沪干线”最终选择迪普科技作为其基础安全设备的供应厂商**。为确保“京沪干线”在运行过程中的稳定可靠，持续为客户提供服务，迪普科技 DPX8000 安全网关采用双机虚拟化部署方式，配合自身的 N+1 电源、冗余主控、不间断重启等高可靠性设计，为“京沪干线”各节点提供稳定可靠的安全防护。

“京沪干线”传输距离长，业务类型复杂，每个站点均涉及到多用户的隔离。DPX8000 安全网关具备 MPLS、VRF、虚拟化等完善的多用户承载与隔离技术，且全面支持 QoS、OSPF、BGP、VXLAN 等网络协议，满足“京沪干线”复杂的组网要求，完整的实现了既定网络设计方案。“京沪干线”将承担起金融数据、政务公文等机要信息的传输任务，构建完善的安全防护体系同样是项目的重中之重。

图138. 迪普科技 DPX8000 系列

资料来源：公司官网，国投证券研究中心

图139. 迪普科技 DPX8000 系列产品性能

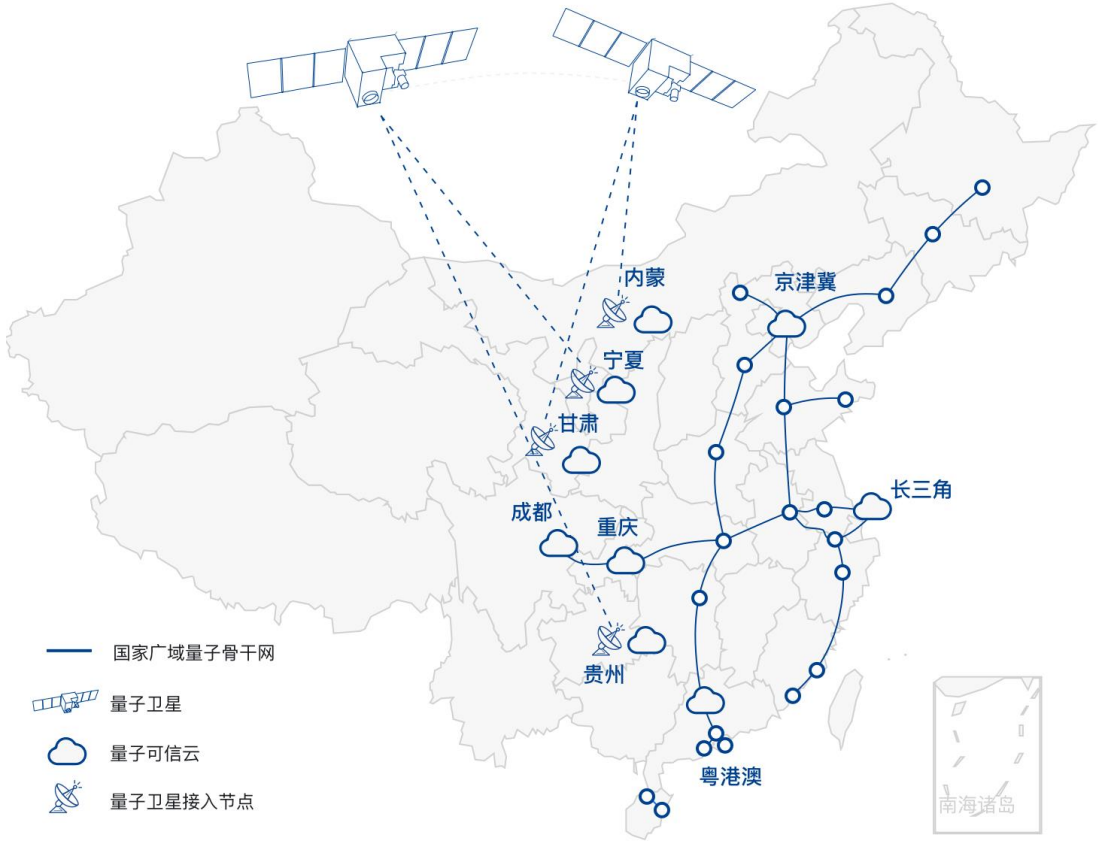
产品型号	DPX8000-A5-E	DPX8000-A3-S	DPX8000-A7-S	DPX8000-A5-X	DPX8000-A12-X
交换容量	27.6Tbps/104.8Tbps	47.7Tbps/168Tbps	86.4Tbps/336Tbps	57.6Tbps/224Tbps	385Tbps/780Tbps
包转发率	30000Mpps	36763Mpps	57600Mpps	38400Mpps	155520Mpps
主控槽位	2				
交换网板数	1—4				
业务槽位数	4	3	6	4	12
电源	N+M冗余电源				
专用软硬件平台**	采用飞腾CPU、盛科交换芯片的专用硬件平台，软件平台拥有麒麟内核使用授权				

资料来源：公司官网，国投证券研究中心

5.14. 金卡智能

金卡智能投资国科量子，并持有账面价值 5000 万元的国科量子股权。国科量子通信网络有限公司（简称“国科量子”或“量子网络”）由中国科学院控股有限公司联合中国科学技术大学等发起成立，是国际电信联盟部门成员、国家高新技术企业。公司致力于研发、建设和运营基于量子通信技术的星地一体、云网融合、应用牵引、自主可控的设施与业务，努力在以量子信息服务数据安全、助力实体经济发展方面发挥先导性、战略性、基础性作用。国科量子是国内量子保密通信骨干网的唯一运营主体，以国家广域量子保密通信骨干网络为基础，在“东数西算”工程的八大枢纽节点建设融合量子通信技术的云平台，为服务数据安全、加强数据治理提供主动管控的技术手段和量子安全增强的数字基础设施底座。

图140. 国科量子云网一体量子设施



资料来源：国科量子官网，国投证券研究中心

5.15. 科大讯飞

科大讯飞于 2021 年推出量子加密智能办公本，除具备讯飞智能办公本在办公、学习、生活场景下手写记录、录音成文、多场景阅读等多项功能外，还支持量子密钥保护功能。科大讯飞股份有限公司成立于 1999 年，是亚太地区知名的智能语音和人工智能上市企业。自成立以来，一直从事智能语音、计算机视觉、自然语言处理、认知智能等人工智能核心技术研究并保持国际前沿水平。作为中国人工智能“国家队”，科大讯飞承建了中国唯一的认知智能全国重点实验室和语音及语言信息处理国家工程研究中心，同时是中国语音产业联盟理事长单位、中科院人工智能产学研创新联盟理事长单位、长三角人工智能产业链联盟理事长单位。

图141. 讯飞量子加密智能办公本

资料来源：公司官网，国投证券研究中心

5.16. 格尔软件

格尔软件于 2023 年投资上海泓格后量子科技，其致力于抗量子密码领域技术研究、标准制定、产品研发，目前已在在政务、金融、军队等领域开展试点、和应用推广工作。公司于 2023 年与复旦大学合作建立实验室，专注于后量子密码研发，抗量子密码是密码技术的未来发展方向。

格尔软件是中国商用密码领域的骨干企业，是国内较早研制和推出公钥密码基础设施（PKI）产品的厂商，是国家科技支撑计划商用密码基础设施项目的牵头单位公司。公司致力提供以身份治理为中心的数字资产安全整体解决方案，拥有大批政务、金融、军工等领域核心客户，面向社会数字化转型的新形势，完成了云计算、大数据环境下大规模复杂场景的安全体系建设，并为工业互联网、物联网、车联网等新型应用保驾护航，全力打造成为国内全栈全域的信息安全服务提供商。

图142. 格尔软件全量子一体化网络安全方案

资料来源：格尔软件微信号，国投证券研究中心

5.17. 信安世纪

信安世纪与银行合作，投入隐私计算、后量子密码技术的研究，推动后量子密码的应用迁移落地。北京信安世纪科技股份有限公司成立于 2001 年 8 月，是科技创新型的信息安全产品和解决方案提供商。公司以密码技术为基础支撑，致力于解决网络环境中的基础性安全问题，在信息技术互联网化、移动化和云化等的发展趋势下，经过二十余年的自主研发和持续创新，信安世纪形成了身份安全、通信安全、数据安全、移动安全、云安全和平台安全六大产品系列。

图143. 信安世纪密码产品概览

资料来源：信安世纪官网，国投证券研究中心

5.18. 吉大正元

吉大正元在抗量子密码算法研究方面取得了一定进展，2022 年，吉大正元率先发布三项抗量子密码领域的最新研究成果：在自研的抗量子签名算法和抗量子密码模块的基础上，自主研发了抗量子 PKI、抗量子电子身份以及抗量子区块链，实现了网络信任体系在抗量子计算能力上的探索，可为构建网络世界中的信任链提供长效安全保障。

图144. 吉大正元抗量子信任体系

资料来源：吉大正元微信号，国投证券研究中心

5.19. 三未信安

三未信安产品主要包括密码芯片、密码板卡、密码整机和密码系统。公司产品全面支持国产 SM1、SM2、SM3、SM4、SM7、SM9、ZUC 等密码算法，为各种信息系统提供数据加解密、数字签名等密码运算，并提供安全、完善的密钥管理机制，可实现各种应用场景的国产密码改造和数据安全保障，为关键信息基础设施和云计算、大数据、区块链、数字货币、物联网、V2X 车联网、人工智能等新兴领域提供数据加密、数字签名、身份认证、密钥管理等服务。

根据公司 2023 年报，作为国内主要的密码基础设施提供商，公司一直保持对密码前沿技术的敏感，将抗量子密码算法与硬件芯片作为重要的研究方向。2023 年，公司在抗量子密码算法的高速硬件实现和产品化方面取得了新的研发成果，**重磅发布了全新产品“抗量子隐私计算一体机”**，填补了公司在抗量子密码算法、隐私计算方向的产品空白。

图145. 三未信安参加抗量子密码技术论坛

资料来源：公司官网，国投证券研究中心

5.20. 电科网安

电科网安持续加大在后量子密码领域的前沿技术研究，覆盖后量子密码理论研究、工程实现及应用技术研究。**量子保密通信方面，**电科网安作为中国移动重要战略合作伙伴以及量子 VoLTE 加密通话业务的研制参与方，公司联手中国移动及其他产业链合作伙伴，对传统 4G VoLTE 加密通话业务进行技术升级，推动量子信息与移动通信网络的融合创新。

图146. 电科网安参与中国移动举办的量子通信年会

资料来源：公司官网，国投证券研究中心

5.21. 浩丰科技

浩丰科技成立于 2005 年 12 月，是国内领先的 IT 系统解决方案提供商，主营业务是向金融（银行、保险）、工商企业（制造、商业流通与服务）、政府及公共事业等行业，酒店及家庭传媒领域，提供基于云计算架构和大数据商业智能的 IT 系统综合解决方案及数字银行解决方案。公司向客户提供卓越的解决方案和贯穿于客户 IT 建设整个生命周期的“一站式”的 IT 服务，业务涵盖软件研发、行业解决方案提供、信息系统集成、建筑智能化和运维服务等领域。浩丰科技在金融、保险、政府、物流、零售、制造、电信、医疗、酒店、能源、教育等领域拥有了大量的成功案例。根据公司公告，浩丰科技致力于量子安全方面的研究，并不断尝试在金融客户中应用量子密码的落地工作。

图147. 浩丰科技产品概览

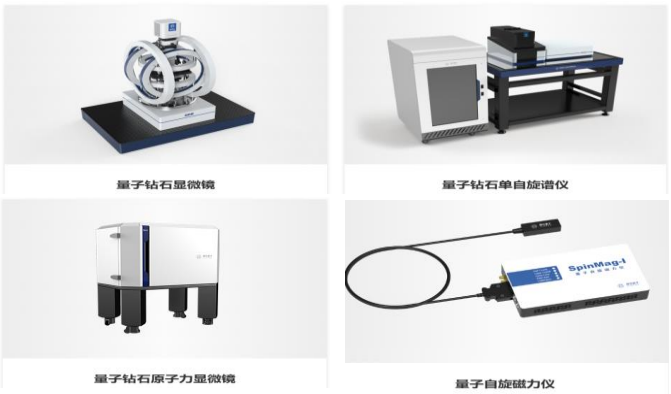
资料来源：公司官网，国投证券研究中心

5.22. 科大国创

科大国创参股的国仪量子是以量子精密测量为核心技术，为全球范围内企业、政府、研究机构提供以增强型量子传感器为代表的核心关键器件、用于分析测试的科学仪器装备、赋能行业应用的核心技术解决方案等产品和服务。

国仪量子源于具有国际知名度的中国科学技术大学，实验室在高端科学仪器、关键核心器件的研制领域深耕十余年，多项技术、研究成果突破国际封锁和禁运，并获得“中国科学十大进展”“ 国家自然科学二等奖”“中国分析测试协会科学技术奖特等奖”等诸多奖项。公司传承实验室的创新基因与探索精神，为全世界的科技工作者提供探知微观世界的一把尺子，获得“2021 年安徽省科学技术奖一等奖”“朱良漪分析仪器创新奖”“安徽省新型研发机构”“安徽省量子精密测量创新中心”“安徽省专精特新冠军企业”等奖项。

图148. 国仪量子量子传感系列产品



资料来源：公司官网，国投证券研究中心

图149. 国仪量子量子计算系列产品

资料来源：公司官网，国投证券研究中心

行业评级体系

收益评级：
领先大市 —— 未来 6 个月的投资收益率领先沪深 300 指数 10%及以上；
同步大市 —— 未来 6 个月的投资收益率与沪深 300 指数的变动幅度相差-10%至 10%；
落后大市 —— 未来 6 个月的投资收益率落后沪深 300 指数 10%及以上；
风险评级：
A —— 正常风险，未来 6 个月的投资收益率的波动小于等于沪深 300 指数波动；
B —— 较高风险，未来 6 个月的投资收益率的波动大于沪深 300 指数波动；

分析师声明

本报告署名分析师声明，本人具有中国证券业协会授予的证券投资咨询执业资格，勤勉尽责、诚实守信。本人对本报告的内容和观点负责，保证信息来源合法合规、研究方法专业审慎、研究观点独立公正、分析结论具有合理依据，特此声明。

本公司具备证券投资咨询业务资格的说明

国投证券股份有限公司（以下简称“本公司”）经中国证券监督管理委员会核准，取得证券投资咨询业务许可。本公司及其投资咨询人员可以为证券投资人或客户提供证券投资分析、预测或者建议等直接或间接的有偿咨询服务。发布证券研究报告，是证券投资咨询业务的一种基本形式，本公司可以对证券及证券相关产品的价值、市场走势或者相关影响因素进行分析，形成证券估值、投资评级等投资分析意见，制作证券研究报告，并向本公司的客户发布。

免责声明

本报告仅供国投证券股份有限公司（以下简称“本公司”）的客户使用。本公司不会因为任何机构或个人接收到本报告而视其为本公司的当然客户。

本报告基于已公开的资料或信息撰写，但本公司不保证该等信息及资料的完整性、准确性。本报告所载的信息、资料、建议及推测仅反映本公司于本报告发布当日的判断，本报告中的证券或投资标的价格、价值及投资带来的收入可能会波动。在不同时期，本公司可能撰写并发布与本报告所载资料、建议及推测不一致的报告。本公司不保证本报告所含信息及资料保持在最新状态，本公司将随时补充、更新和修订有关信息及资料，但不保证及时公开发布。同时，本公司有权对本报告所含信息在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。任何有关本报告的摘要或节选都不代表本报告正式完整的观点，一切须以本公司向客户发布的本报告完整版本为准，如有需要，客户可以向本公司投资顾问进一步咨询。

在法律许可的情况下，本公司及所属关联机构可能会持有报告中提到的公司所发行的证券或期权并进行证券或期权交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或者金融产品等相关服务，提请客户充分注意。客户不应将本报告为作出其投资决策的惟一参考因素，亦不应认为本报告可以取代客户自身的投资判断与决策。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议，无论是否已经明示或暗示，本报告不能作为道义的、责任的和法律的依据或者凭证。在任何情况下，本公司亦不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

本报告的估值结果和分析结论是基于所预定的假设，并采用适当的估值方法和模型得出的，由于假设、估值方法和模型均存在一定的局限性，估值结果和分析结论也存在局限性，请谨慎使用。

国投证券股份有限公司对本声明条款具有惟一修改权和最终解释权。

国投证券研究中心

深圳市
地　址：深圳市福田区福华一路 119 号安信金融大厦 33 层
邮　编：518046

上海市
地　址：上海市虹口区杨树浦路 168 号国投大厦 28 层
邮　编：200082

北京市
地　址：北京市西城区阜成门北大街 2 号楼国投金融大厦 15 层
邮　编：100034