

全球量子科技产业化加速推进中

——量子科技专题报告（一）

行业投资评级：强于大市|维持

孙业亮/刘聪颖

中邮证券研究所 计算机团队

中邮证券

发布时间：2026-02-26

- **全球高度重视量子科技，国际竞争激烈：**量子科技已成为全球主要国家开展科技、经济等领域综合国力竞争，维护国家技术主权与发展主动权的战略重点之一，对国防安全、信息安全等关键领域有深远影响；截至2025年8月，全球30余个国家和地区制定或更新量子信息领域的发展战略规划或法案文件，投资金额已超过350亿美元；“十五五”规划将量子科技列入未来产业布局的首位，政策体系持续完善。
- **量子计算多技术路线竞相发展，亮点成果不断涌现：**近年来，在实验室环境下超导、离子阱、中性原子、光量子等主要技术路线原理样机的量子比特规模和逻辑门保真度等均有明显提升，量子纠错在新型编码方案研究和逻辑量子比特构建等方面取得重要科研成果，量子软件与云平台技术成熟度不断提升，应用场景探索广泛开展，一旦规模、噪声和控制超过某些阈值，性能差距的跃升将转化为巨大经济效益。
- **后量子密码系统迁移势在必行：**量子计算技术的飞速发展，给传统密码学带来前所未有的严峻挑战，PQC作为保障未来信息安全的核心技术，正迎来标准产业化与迁移工程化的战略叠加期。
- **投资建议：**建议关注国盾量子、科大国创、纬德信息、国芯科技、禾信仪器、格尔软件、三未信安等。
- **风险提示：**技术突破不及预期风险；下游应用落地不及预期风险；软件生态系统与供应链不完善风险；政策支持力度减弱风险等。



目录

- 一 | **量子科技已成为大国科技竞争的核心战场**
- 二 | **量子计算正步入首个真正的商业周期**
- 三 | **量子时代即将来临，加速构建后量子安全防线**
- 四 | **相关企业与风险提示**

—

量子科技已成为大国科技竞争的核心战场

量子科技已成为大国科技竞争的核心战场

- **量子时代加速到来：**2025年是量子力学诞生100周年，联合国教科文组织宣布2025年为“国际量子科学与技术年”，从费曼的构想到千比特量子计算机的诞生，量子科技通过“基础理论—技术验证—产业生态”的链式突破，已成为大国科技竞争的核心战场；中国以合肥、北京、上海为枢纽的产业生态，与美欧形成三足鼎立，量子纠错、异构融合与场景落地的突破决定下一阶段各国量子科技竞争力的格局。
- **“十五五”规划核心赛道：**进入“十五五”，量子科技被正式列入未来产业布局的首位，是国家战略重心持续前移的集中体现，政策脉络的演进，正见证着国家对这一前沿领域的重视不断加码。

图表1：顶层设计持续加码量子科技

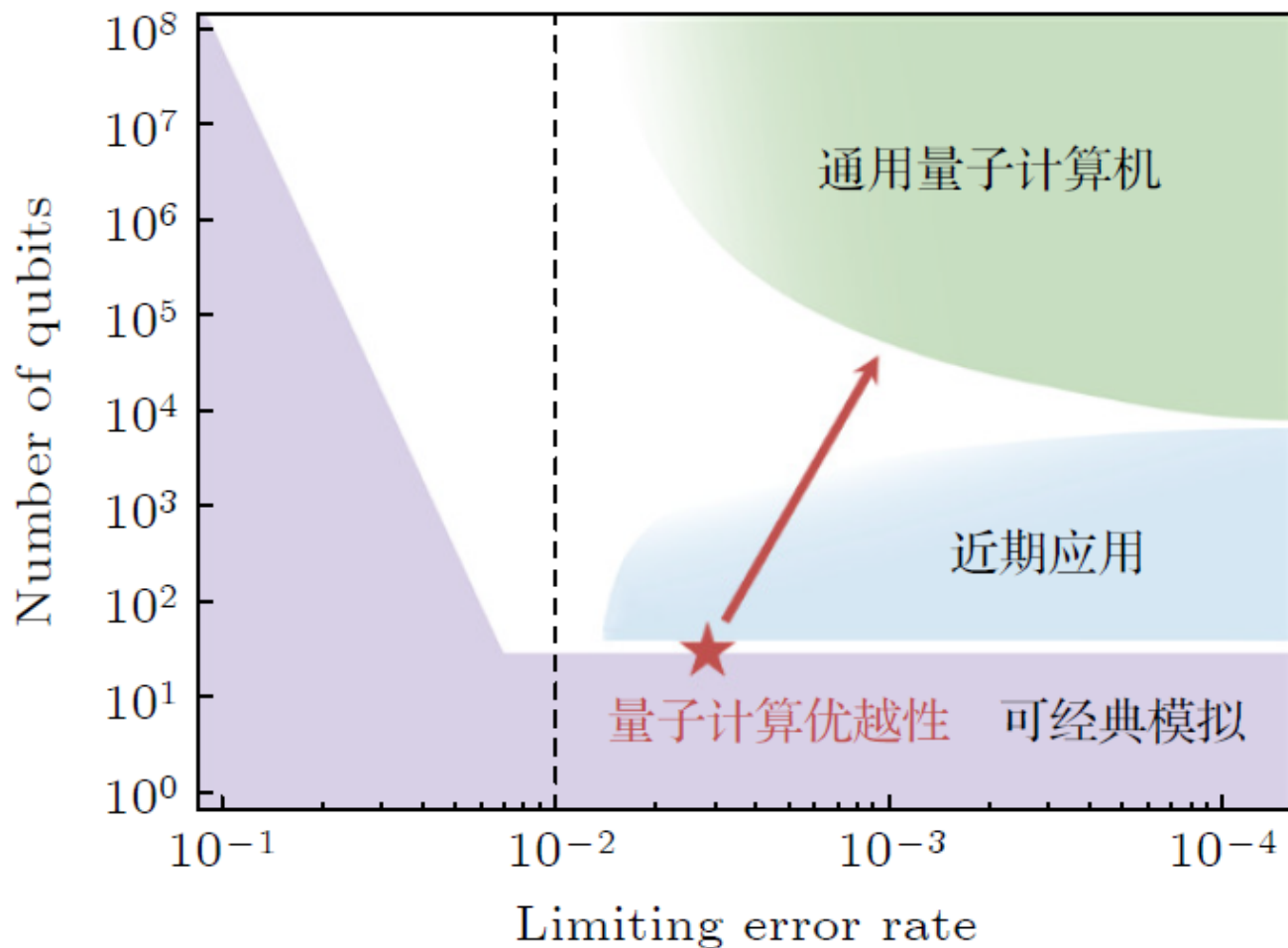
日期	政策名称	主要内容
2016年	《“十三五”国家战略性新兴产业发展规划》	统筹布局量子芯片、量子编程、量子软件以及相关材料和装置制备关键技术研发，推动量子计算机的物理实现和量子仿真的应用
2021年	《第十四个五年规划和2035年远景目标纲要》	瞄准人工智能、量子信息、集成电路、生命健康、脑科学、生物育种、空天科技、深地深海等前沿领域，实施一批具有前瞻性、战略性的国家重大科技项目
2024年	《2024年政府工作报告》	制定未来产业发展规划，开辟量子技术、生命科学等新赛道，创建一批未来产业先导区
2024年	《关于开展2024年度普通高等学校本科专业设置工作的通知》	支持高校面向集成电路、人工智能、量子科技、生命健康、能源、绿色低碳、涉外法治、国际传播、国际组织、金融科技等关键领域布局相关专业
2025年	《关于制定国民经济和社会发展第十五个五年规划的建议》	推动量子科技、生物制造、氢能和核聚变能、脑机接口、具身智能、第六代移动通信等成为新的经济增长点

资料来源：中国政府官网，教育部官网，中邮证券研究所

量子科技已成为大国科技竞争的核心战场

- 目前，量子科技可分为量子计算、量子通信、量子精密测量三大核心领域。
- **量子计算具有强大的并行计算和模拟能力：**一旦成功研制，基于计算复杂度的经典信息安全体系将受到巨大冲击；例如，基于量子计算机的“Shor 算法”能够轻易破解当前在公钥加密和电子商业中被广泛使用的非对称加密算法，而基于量子密钥分发的量子保密通信的安全性与计算复杂度无关，即使是量子计算机也无法破解。
- **量子计算研究的核心任务是实现多量子比特的相干操纵：**实现量子计算主要的物理系统包括光量子、超导量子线路、超冷原子、离子阱、固态自旋、硅基量子点以及拓扑态等，这些系统各自具有优势和缺点，构建量子计算机的技术路线尚未收敛。

图表2：量子计算的三个阶段

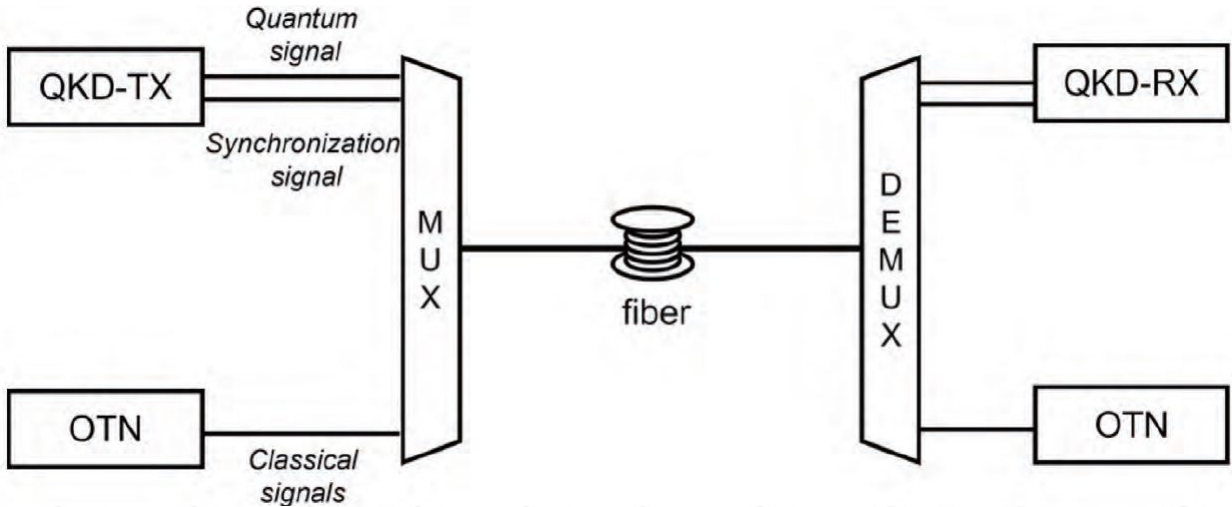


资料来源：潘建伟《量子信息科技的发展现状与展望》，中邮证券研究所

量子科技已成为大国科技竞争的核心战场

- 目前，量子科技可分为量子计算、量子通信、量子精密测量三大核心领域。
- **量子通信包括量子密钥分发和量子隐形传态两种应用方式：**量子密钥分发是指利用量子态来加载信息，通过一定的协议在遥远地点的通信双方共享密钥，基于量子密钥分发的量子保密通信是迄今唯一原理上无条件安全的通信方式，也是最先走向实用化和产业化的量子信息技术；量子隐形传态利用量子纠缠来直接传输微观粒子的量子状态(即量子信息)，而不用传输这个微观粒子本身，量子隐形传态技术可以链接量子信息处理单元来构建量子网络，同时也是构建远距离量子密钥分发所需的量子中继的关键环节。
- **量子通信的发展目标是构建全球范围的广域量子通信网络体系：**利用光纤构建城域量子通信网络，通过中继器链接邻近两个城市的城域量子通信网络，通过卫星平台的中转链接遥远区域之间的量子通信网络。

图表3：“经典-量子共纤传输”拓扑图



量子科技已成为大国科技竞争的核心战场

- 目前，量子科技可分为量子计算、量子通信、量子精密测量三大核心领域。
- **精密测量进入量子时代：**量子精密测量利用量子效应、量子相干、量子纠缠或量子隧穿等量子系统的特有性质实现高精确、高灵敏探测和测量，可以用于测量磁场、电场、重力、时间和频率、温度/ 压力、加速度、角动量等多种物理量，实现远超经典传感器的测量精度，可以达到甚至超过海森堡精度极限。

图表4：量子精密测量主要技术路线和物理量

物理量	量子精密测量系统与装置		物理量	量子精密测量系统与装置			
时间频率	量子时钟	微波钟	重力	量子重力仪/量子重力梯度仪 冷			
		光钟		量子陀螺仪	核磁共振陀螺仪		
		核钟			SERF陀螺仪		
		芯片级原子钟			原子干涉陀螺仪		
磁场	量子磁力计	光泵磁力计	角速度	原	冷	固	NV色心陀螺仪
		SERF磁力计					量子增强雷达
		CPT磁力计					量子干涉雷达
		NV色心磁力计					量子照明雷达
		SQUID磁力计					
电场	量子场强计	里德堡原子场强计	位移/相位	量子雷达	纠	单	
		NV色心场强计					
温度	量子温度计	固	原	原子蒸气	固	固态自旋（系综/单自旋）	量子精密测量主要技术路线/方案
			冷	冷原子	超	超导	
应力应变	量子压力计	固	离	离子阱	纠	纠缠光子	
			里	里德堡原子	单	单光子探测	

资料来源：中国信通院《量子信息技术发展与应用研究报告（2025年）》，中邮证券研究所

请参阅附注免责声明

量子科技已成为大国科技竞争的核心战场

- 量子信息产品可被划分为量子计算产品、量子通信产品、量子精密测量产品以及支撑开展量子产品加工/ 测试/ 试验的设备等4个子体系。

图表5：量子信息产品体系结构



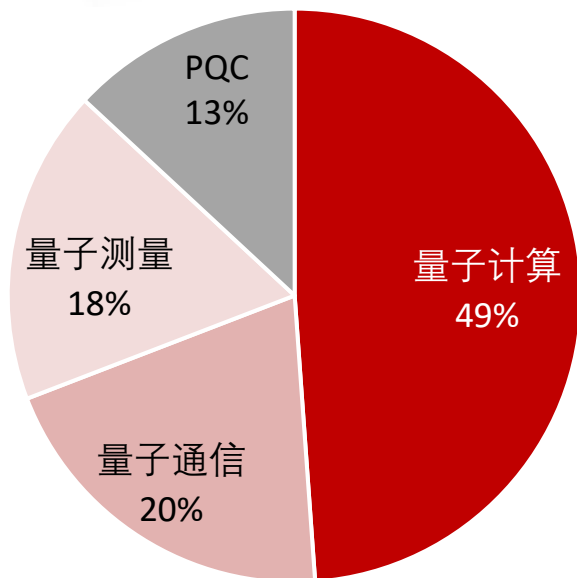
资料来源：张学骞等《量子信息产品标准化路线图研究》，中邮证券研究所

请参阅附注免责声明

量子科技已成为大国科技竞争的核心战场

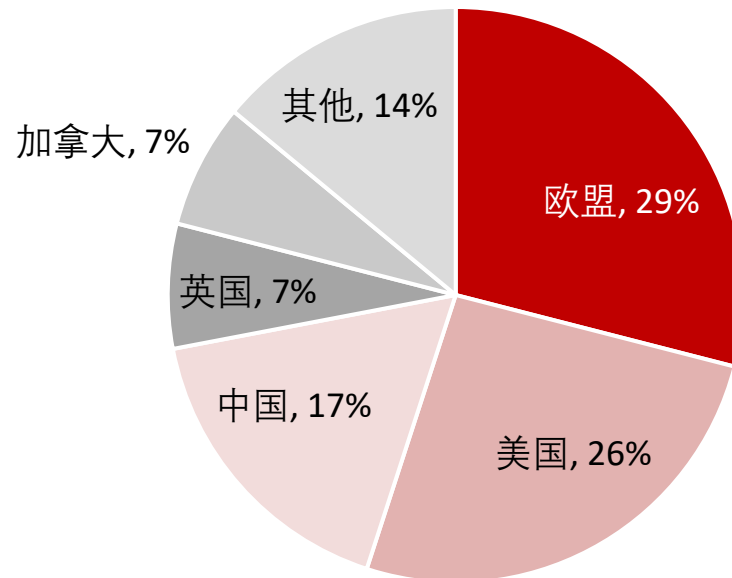
- **企业已成为量子信息技术与产业发展的重要力量：**全球量子信息相关企业数量突破800家，其中量子计算领域占比约49%，PQC领域发展迅速，相关企业已突破百家。从企业国家分布看，欧盟有量子企业238家，占比29%，其中德国量子企业数量超过70家；美国有量子企业数量215家，占比26%；我国有量子企业145家，占比17%。
- **我国企业数量相较欧美仍有一定差距：**欧美量子计算产业生态聚集度高，相关企业数量是我国的近6倍，量子通信领域我国企业数量领先，量子测量领域则是美国领先，PQC多为初创企业和信息安全领域企业新增布局。

图表6：全球量子信息企业技术领域分布



资料来源：中国信通院《量子信息技术发展与应用研究报告（2025年）》，中邮证券研究所
请参阅附注免责声明

图表7：全球量子信息企业国家分布



资料来源：中国信通院《量子信息技术发展与应用研究报告（2025年）》，中邮证券研究所

量子科技已成为大国科技竞争的核心战场

- **市场投融资热情高涨，量子计算明星企业是资本市场追逐热点：**近十年来全球量子信息领域产业投融资事件达1400余笔，融资金额超145亿美元；其中，风险投资占比约67%，金额近百亿美元，占据主导地位，说明产业化仍处于早期起步阶段，政府和军方的赠予类投资近年增长迅速；从地区分布看，美国企业和市场投融资活跃度高，全球占比约50%，欧盟量子企业融资超20亿美元，我国约为14亿美元；从技术领域看，量子计算企业融资近百亿，占比约80%，是市场关注焦点，PQC企业近年来开始逐步成为投融资热点。

图表8：量子信息领域企业投融资事件数量与金额



资料来源：中国信通院《量子信息技术发展与应用研究报告（2025年）》，中邮证券研究所（截至2025年8月）

二

量子计算正步入首个真正的商业周期

量子计算正步入首个真正的商业周期

- **为什么量子计算现在如此重要？** 一旦硬件突破关键阈值，传统超级计算机需要数个世纪才能解决的问题，在几分钟内即可解决，从而为从制药到金融等各个行业释放巨大价值；到目前为止，尽管量子计算利用叠加态、纠缠等现象有望实现远超最先进经典计算机的计算能力，但尚未解决任何一件经典计算机无法处理的实际问题；**目前量子计算虽然优势有限，但在某些领域具有工业应用价值；**
- **D-Wave (2025 Science) 在工业相关任务中首次清晰地展示了量子霸权：**量子退火器可以解答一些经典计算无法解决的、具有实际意义的问题，在几分钟内完成了可编程材料模拟，而Frontier超级计算机需要近一百万年的时间和全世界一年的电力消耗才能完成；
- **D-Wave (2023 Nature) 证明了5000量子比特可编程自旋玻璃中的量子临界动力学：**利用超导量子退火器在数千个量子比特上实现了量子临界自旋玻璃动力学，为大规模量子模拟提供了理论和实验支持，并在能量优化方面具有拓展优势；
- **IBM (2023 Nature) 证明了量子计算在容错技术出现之前的实用性：**利用误差缓解技术，在噪声较大的127量子比特处理器上实现了在超越传统经典计算的规模下，对电路体积进行精确期望值的测量，描绘出一幅噪声量子计算机实用性越来越光明的图景；
- **Google (2023 Nature) 通过缩放表面码逻辑量子比特来抑制量子误差：**巧妙地利用更多物理量子比特，实现前所未有的误差控制，该量子纠错方案的量子纠错性能随着量子比特数量的增加开始提升，为达到计算所需的逻辑错误率指明了方向；
- **Quantinuum是全球最大的综合量子计算公司：**推出业内首台囚禁离子56量子比特量子计算机，实现了比现有行业基准高出100倍的性能提升；与微软合作，发布了2030年实现通用、完全容错量子计算的路线图，显著加快了商用量子计算系统的研发进程；
- **量子技术已经开始发挥作用：**这些结果具有领域特异性，不具有普遍性，但它们证明了一旦规模、噪声和控制超过某些阈值，性能差距就会从渐进式增长跃升至天文数字，而这种差距是可以转化成为经济效益的。

量子计算正步入首个真正的商业周期

- **量子计算目前处在NISQ时代：**当今设备中的“嘈杂”量子比特极易出错，目前尚无通用且简单的纠错方法，现在的量子计算机还无法执行在传统高性能计算机上无法完成的、具有实际应用价值的计算任务，当前的现状通常被称为“嘈杂中等规模量子”（NISQ）时代；
- **量子设备采用的量子比特物理系统差异极大：**与经典计算机一样，量子计算机也有一个核心处理器和一套控制堆栈，其核心取决于所使用的量子比特类型，每一种都基于不同的物理机制来创建和操控量子比特，尚无明确迹象表明是否会有哪一种最终成为主流。

图表9：当前的量子计算并不存在单一的平台

模态	工作原理	关键优势	关键限制	代表性公司
超导量子比特	由超导材料制成的电路，在毫开尔文温度下运行，电流无电阻流动，量子比特由约瑟夫森结构成	门操作速度快、纳米加工技术成熟、生态系统完整	相干时间短、低温布线复杂	IBM、Google、Rigetti、IQM
离子阱	将单个带电原子困在电磁阱中，通过激光操控	极高的保真、长相干时间、全连接	操作速度慢、光学系统复杂	IonQ、Quantinuum、Alpine
中性原子	中性原子被困在光镊中，并激发到里德伯态以产生相互作用	天然一致的量子比特、可扩展阵列、支持并行门操作	需要高精度激光控制、电子学扩展存在挑战	QuEra、Pasqal、Infleqtion
光子量子比特	单个光子在光路或光纤中传播，并在偏振、时间或路径上编码	可在室温运行、易于网络化	光子损耗、纠缠具有概率性	PsiQuantum、Xanadu、ORCA
硅自旋量子比特	半导体量子点中的电子或核自旋，通过电控或磁控实现操作	与CMOS工艺兼容、面积小	需要极低温，相干性存在挑战	Diraq、Quantum Motion
量子退火	超导磁通量子比特被排列用于寻找优化问题的低能量解	唯一目前已有商业化收入的量子计算机模式（用于优化）	非通用量子计算	D-Wave

资料来源：韩明等《量子计算：处在商业应用的临界点》，中邮证券研究所

量子计算正步入首个真正的商业周期

- **量子计算正处于理论研究向应用落地探索转化的关键阶段：**早期突破将集中在量子力学具有结构优势的四个领域，**1) 模拟**，用于加速药物发现、新型催化剂和先进制造的分子和材料建模；**2) 优化**，通过复杂的物流、财务和产业规划，实现小的收益，从而获得巨大的经济回报；**3) 机器学习**，更快地训练和推理复杂模型，使人工智能能力超越当前极限；**4) 密码学与安全**，破解现有加密技术并创建抗量子攻击的标准，这对国家安全具有重要意义。

图表10：一旦获得量子优势，各领域的预计市场价值

行业	应用场景	市场潜力（低端，亿美元）	市场潜力（高端，亿美元）
汽车	自动驾驶AI算法	10	100
金融	反洗钱与反欺诈	200	300
	投资组合优化	200	500
	市场模拟	200	350
科技	搜索/广告优化	500	1000
物流	网络优化	500	1000
保险	风险管理	100	200
航空航天	路线优化	200	500
	计算流体力学（CFD）	100	200
制药	药物研发	400	800
化工	催化剂设计	200	500
能源	太阳能转换	100	300
政府	加密、解密（网络安全）	200	400
企业	加密（网络安全）	200	400
通信	安全、网络与服务	240	360

资料来源：PatentVest，中邮证券研究所

量子计算正步入首个真正的商业周期

- **在商业上可行的量子系统部署后，各领域领先应用案例预计每年创造的经济价值超万亿美元：** 业界持续挖掘与量子计算技术匹配的垂直应用场景，寻找面向金融、化工、生物、交通等不同行业领域的解决方案，跨行业、多场景的应用探索已成为推动应用落地突破的核心驱动力；据PatentVest数据，在商业上可行的量子系统部署后，金融、科技、物流、制药、航空航天、化工行业的市场潜力分别达到1750、1500、1500、1200、1000、700亿美元/年，政府、企业、通信行业市场潜力均约为600亿美元/年。

图表10：一旦获得量子优势，各领域的预计市场价值

行业	应用场景	市场潜力（低端，亿美元）	市场潜力（高端，亿美元）
汽车	自动驾驶AI算法	10	100
金融	反洗钱与反欺诈	200	300
	投资组合优化	200	500
	市场模拟	200	350
科技	搜索/广告优化	500	1000
物流	网络优化	500	1000
保险	风险管理	100	200
航空航天	路线优化	200	500
	计算流体力学（CFD）	100	200
制药	药物研发	400	800
化工	催化剂设计	200	500
能源	太阳能转换	100	300
政府	加密、解密（网络安全）	200	400
企业	加密（网络安全）	200	400
通信	安全、网络与服务	240	360

资料来源：PatentVest，中邮证券研究所

量子计算正步入首个真正的商业周期

- **量子计算云平台正逐渐发展为量子计算领域的核心基础设施：**为降低量子计算机的使用门槛，推动技术成果的开放共享，云计算算力资源共享模式被引入量子计算领域，即量子计算云平台；量子计算云平台通过整合量子计算硬件资源、经典计算控制系统以及量子软件工具链，为用户提供按需、远程的量子计算服务，已逐渐成为**量子计算应用探索与产业化落地的重要实现途径。**
- **国际巨头主导全球市场，国内平台同步发力：**国际方面，IBM、谷歌、微软、亚马逊等科技巨头凭借其云服务优势，持续扩大全球版图，其中IBM Quantum已在北美、欧洲、亚太地区布局多个区域量子计算中心，其服务覆盖全球百余家企业及机构用户；国内方面，我国量子云平台建设同步加速，已涌现出如中国移动“五岳纪元”、本源量子“本源量子云”、北京量子院“夸父”、中国电信“天衍”等一批具备自主技术特色的代表性平台；相较国际巨头，**国内量子云平台在接入真机性能、用户规模及生态活跃度等方面仍存在差距。**

图表11：国内外量子计算云平台现状特征对比

对比维度	国际平台	国内平台
发展阶段	商业化扩张时期	商业化早期
量子云平台数量	保持接近水平	
平台接入真机情况	真机接入数量多，且真机比特数高（百比特量级居多）	部分平台真机接入数量少，真机比特数比国际平台偏少（数十比特量级居多）
社区活跃度	用户数量多且稳定，用户活跃度高	用户数不稳定，用户活跃度低
商业模式	具备成熟订购机制，面向全球高预算客户提供高价值分层订购	尚未建立成熟完善的商业模式，以“普惠基础服务 + 政策联动收费”为主
主要应用	覆盖金融、生物医药、材料科学、能源、汽车等；支持量子—经典混合算法在真实业务场景中验证	集中在金融、新材料、生物医药等局部场景，应用案例较少，多处于概念验证阶段

资料来源：姚飞等《量子计算云平台产业发展态势及标准化研究》，中邮证券研究所

量子计算正步入首个真正的商业周期

- **量子计算与超级计算协同成为量子-经典融合计算重要发展方向：**在NISQ时代，量子处理器虽然在比特数上不断增长，但其固有的噪声、退相干和有限的连通性等物理限制，使得执行复杂、长深度的纯量子算法尚不可行，因此量子-经典混合计算作为一种务实的解决方案应运而生，它通过将计算任务在量子处理器（QPU）与经典处理器（CPU/GPU）之间进行合理分配，以最大化发挥当前硬件的潜力。
- **量子-经典融合计算可能成为实用化落地突破口：**全球主要国家和地区通过战略引导等推进布局，美国发布《国家量子倡议重新授权法案》、《量子技术政策指南》推动量子-经典融合计算应用发展，新加坡推出“混合量子-经典融合计算计划（HQCC 1.0）”并投资2450万美元用于计划实施；英伟达、IBM、亚马逊等国际科技巨头亦加紧相关布局，纷纷开展量子计算与高性能计算融合的探索实践。

图表12：量子-经典异构算力混合示意图

	SISD	SIMD	MIMD	通用量子计算机	专用量子计算机
SISD					
SIMD					
MIMD					
通用量子计算机					
专用量子计算机					

经典异构

量子-经典融合计算

量子异构

资料来源：张萌等《量子-经典融合计算发展现状与趋势研究》，中邮证券研究所

量子计算正步入首个真正的商业周期

- **量子计算与AI的协同发展未来前景广阔：**随着深度学习、模式识别等技术的持续演进，人工智能有望加速量子芯片设计、量子态测控等环节的研发过程，拓展量子计算在更多行业场景中的应用，进一步促进量子计算技术的发展；量子计算凭借其数据并行处理能力，在计算海量数据、加速机器学习算法训练、优化AI模型等方面表现出巨大潜力，从而使AI系统实现更高效、更精准的学习与推理。
- **量子AI平台的研发及应用逐渐成为热点方向：**量子AI平台通过提供量子机器学习算子库、混合编程框架以及参数优化工具，实现量子算法与经典深度学习框架的协同，核心是量子力学赋能机器学习，强化传统学习模型的计算效率与高维问题处理能力，突破经典AI在复杂优化、大数据训练中的算力瓶颈；全球主要云服务商和量子技术企业正通过构建软硬协同的算法环境，推进量子计算AI平台的行业适配。

图表13：全球主要机构量子AI平台进展动态

时间	主体	事件/进展	量子AI平台基本情况
2025年10月	Quantum Elements	推出用于量子软硬件开发的人工智能原生平台	该平台依托代理 AI、自然语言提示及专有模拟后端，助力用户快速开发多行业量子解决方案
2025年8月	D-Wave	推出开源工具包以推进量子人工智能探索和创新	该开源工具包允许开发人员使用量子计算机来帮助训练人工智能模型，专注于图像生成和模式识别等机器学习任务
2025年8月	NVIDIA	发布CUDA-QX 0.4版本	CUDA-QX 0.4 增加了新的量子纠错和求解器功能，包括生成式AI 驱动算法、GPU 加速张量网络解码器和自动检测器错误模型生成
2025年7月	中国移动	发布五岳量智量子人工智能训推平台	该平台内核实现了基于Python 的量子神经网络计算框架，基于PyTorch、Numpy 支持量子神经网络架构的定义和参数调优训练
2025年2月	Quantinuum	推出生成式量子AI框架Gen QAI	该框架利用独特的量子生成数据，能够在新药开发、金融市场精准预测建模以及全球物流和供应链实时优化等多个领域实现商业应用

资料来源：姚飞等《量子计算云平台产业发展态势及标准化研究》，中邮证券研究所

三

量子时代即将来临，加速构建后量子安全防线

量子时代即将来临，加速构建后量子安全防线

- **量子计算技术的快速发展对现有密码体系造成威胁：**传统密码技术作为信息安全的基础，涵盖了对称密码算法、非对称密码算法和哈希算法等多种技术手段，传统公钥密码系统基于数学难题(如大整数分解、离散对数) 实现加密、签名和密钥交换，主要包括RSA、ECC、DSA、Diffie-Hellman 等， 这些系统广泛应用于网络安全；量子计算机利用Shor算法和Grover算法，能够在多项式时间内破解传统公钥密码系统，这对现有的网络安全基础设施构成了严重威胁。

图表14：现有密码体系与典型通信应用

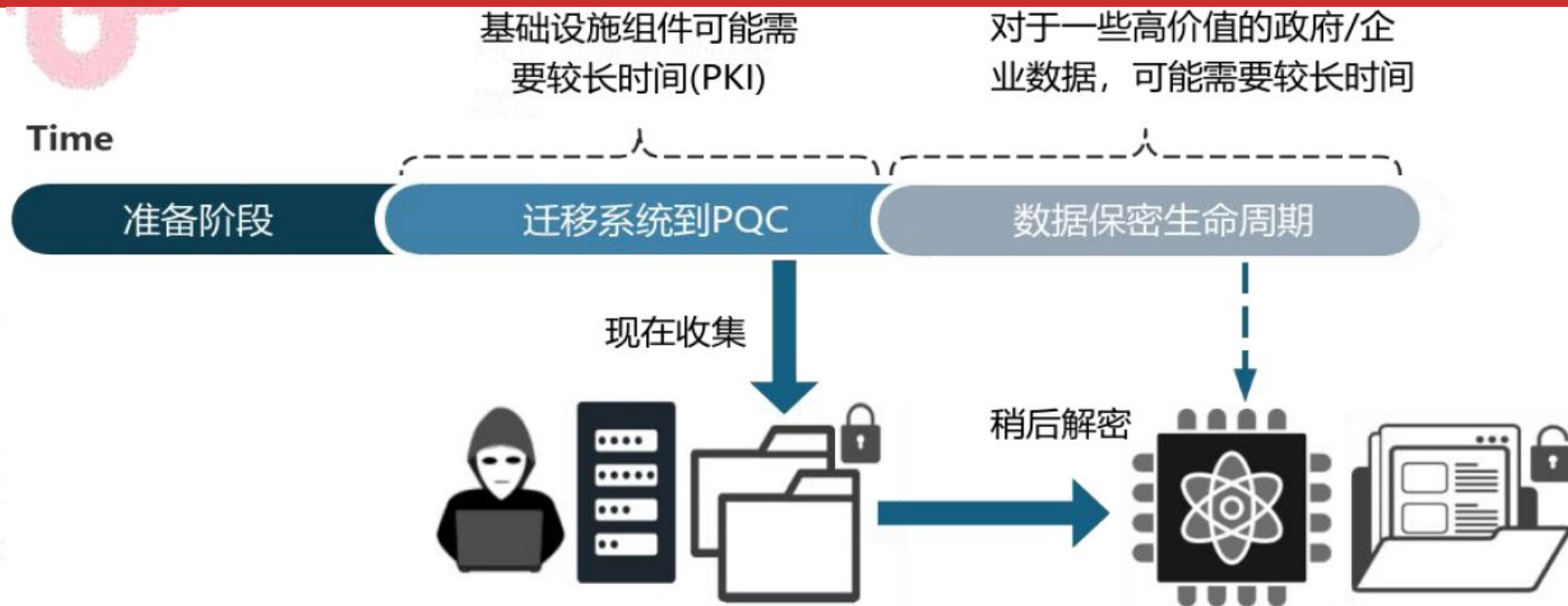


资料来源：中国联通研究院《2025中国联通后量子密码白皮书》，中邮证券研究所

量子时代即将来临，加速构建后量子安全防线

- **“先获取，后破解”的策略对需要长期保密的敏感信息构成了严重威胁：** 尽管当前的量子计算能力仍不足以破解大规模密钥，但随着量子技术的快速发展，预计2035年左右，百万级量子比特的计算机可能问世，届时现有的公钥密码系统将面临巨大挑战，攻击者可存储当前无法破解的密文，待量子计算能力足够强大后再行破解，因此，对未来保密期超过的敏感信息，使用现有公钥密码已不再安全，必须尽早转向后量子密码方案。

图表15：后量子密码迁移具有紧迫性



资料来源：中国联通研究院《2025中国联通后量子密码白皮书》，中邮证券研究所

量子时代即将来临，加速构建后量子安全防线

- **量子密钥分发和后量子密码在应对量子计算威胁的密码学领域中各有优势和特点：**为了应对量子计算机威胁，全球密码学界提出了两种主要应对策略：基于量子物理原理的量子密钥分发（QKD）和基于数学难题的抗量子密码算法（PQC）；**QKD的核心原理是量子不可克隆定理和海森堡测不准原理**，前者确保任何未知量子态无法被完美复制，后者则保证任何测量量子系统的行为都会扰动系统状态，这意味着一旦有窃听者试图拦截量子信道，通信双方就能够通过误差率分析检测到窃听行为；**PQC是基于那些被认为在经典计算机和量子计算机上都难以解决的数学难题构造的**，主要包括格子密码、编码密码、多变量密码和哈希密码等几种类型，不需要专门的量子设备，可以在现有数字基础设施上运行。
- **量子密钥分发与后量子密码可以互补和融合，构建一套综合性密码基础设施：**QKD难以直接应用于复杂的多节点网络，PQC无法提供QKD级别的物理层安全保障，单一使用QKD或PQC均无法全面满足电信运营商在复杂网络环境中的多样化需求，而QKD和PQC的结合能够形成一种多层次的安全保障机制，QKD负责提供底层密钥分发的绝对安全性，PQC则在更高层次上为加密和认证提供抗量子攻击的能力；使用**QKD生成密钥**，结合**PQC算法加密数据**，确保即使某一层被攻破，整体系统仍然安全。

图表13：QKD与PQC技术对比

	安全基础	安全性性质	保护范围	部署需求	部署成本	传输距离	标准化进度	适用场景
量子密钥分发（QKD）	物理定律	量子物理特性安全	密钥分发	专用设备与链路	较高	受限（需中继）	国内CCSA、国际ITU-T	高安全专线/专网
抗量子密码（PQC）	数学难题	计算安全	端到端安全	软件/固件更新	较低	无限制	以NIST为主导	通用互联网应用

资料来源：黄建康等《后量子时代数据加密安全方案研究》，中邮证券研究所

量子时代即将来临，加速构建后量子安全防线

- **后量子密码技术基于全新的数学难题和计算假设：**设计抗量子计算攻击的公钥密码算法，关键在于寻找具备抗量子攻击能力的数学困难问题，目前主流的抗量子密码算法按照所基于的技术路线分为格、编码、多变量、哈希、同源等，这些技术各有优劣，共同为应对量子计算带来的安全威胁提供了多样化的解决方案；后量子密码在安全性与实用性的平衡中持续突破，基于格的密码技术凭借通用性强、性能均衡等优势成为主流方向，而其他技术路径也在特定场景中展现独特价值；在应用层面，已在网络通信、金融交易、军事指挥等关键领域形成示范，为各行业量子安全升级提供了可行方案。

图表14：不同路线的抗量子密码算法比较

技术路线	原理	优势	缺点
格	以格上最短向量问题、最近向量问题等为安全基础，可实现加密、签名等多种功能，加密解密依赖格向量运算	安全性强，理论基础扎实；性能均衡，通用性高，适配多种场景，升级成本低	算法实现复杂，高维计算对资源要求高，内存占用较大，受限设备应用有难度
编码	利用纠错码构造，公钥为随机线性码，私钥为纠错生成矩阵，安全性依赖译码困难性，加密加随机错误，解密靠私钥纠错	抗量子攻击能力较强，部分场景加密速度快	密钥尺寸过大，存储传输成本高；编码解码运算复杂，计算效率低
多变量	依托多变量二次方程组求解难题，通过多项式系统实现加密签名，验证和解密依赖方程组运算	加解密及签名验签速度快，参数可调，适配部分资源受限场景	密钥存储需求大，管理复杂；安全性依赖系统设计，易受代数攻击
哈希	借助哈希函数单向性、抗碰撞性实现签名和密钥交换，签名验证通过比对哈希值完成	实现简单，部署容易；运算速度快，通用性好，兼容现有系统	签名值较长，增加传输存储开销；安全性依赖哈希函数，需持续更新维护
同源	以超奇异椭圆曲线间同源映射困难性为基础，用于密钥交换等，通过同源操作生成共享密钥	安全性有保障，量子环境下难破解；特定场景计算效率较高	理论复杂，实现难度大；与传统系统兼容性差，改造成本高，长期安全性待验证

资料来源：刘毅等《量子计算机下的密码技术研究综述》，中邮证券研究所

量子时代即将来临，加速构建后量子安全防线

- **欧美国家在迁移方案准备与后量子密码领域均走在前列：**国内外研究机构和学者们正在推进密码算法和安全协议的标准化进程，以应对量子计算带来的威胁；随着PQC标准初具雏形，各国先后提出后量子迁移规划及指南，同时在PQC产业化方面也加快推进，抢占先机。

图表15：各国PQC迁移进展

国家	纳入考虑的PQC算法	已发布的指导文件	简略时间表
澳大利亚	NIST	CTPCO (2023)	开始规划; 2025-2026 年早期实施
加拿大	NIST	Cyber Centre (2021)	开始规划; 2025 年开始实施
中国	中国特定	CACR (2020)	开始规划
欧盟委员会	NIST	ENISA (2022)	开始规划和放缓
法国	NIST (但不限于)	ANSSI (2022, 2023)	开始规划; 2024 年开始迁移
德国	NIST (但不限于)	BSI (2022)	开始规划
日本	参考NIST	CRYPTREC	开始规划; 初步时间表
荷兰	AES,参考NIST、SPHINCS-256、XMSS	NCSC (2023)	带有时间表的行动计划草案
新西兰	NIST	NZISM (2022)	开始规划
新加坡	参考NIST	MCI (2022)	无时间节点
韩国	KpqC	MSIT (2022)	2022-2023第一轮算法筛选
英国	NIST	NCSC (2023)	开始规划; 2024年开始实施
美国	NIST	CISA (2021, 2022, 2023) 、 NIST (2023) NSA (2022, 2023) 、 White House (2022)	2023-2033实施
捷克	NIST算法 (但不限于)	NÚKIB-2023	2027 年前完成迁移 (密钥协商、加密) ; 尽快实施 固件/软件签名
以色列	未明确	IL-2022, IL-2025	开始规划, 建立密码资产清单; 合同中纳入PQC 要求; 金融机构需管理量子风险并制定计划
意大利	NIST算法	IT-2024	未明确
西班牙	NIST 算法及FrodoKEM	CCN.ES-2022	四阶段推进, 当前至2030年后
印度	NIST	IT-2024	无时间节点
瑞士	NIST+QKD融合架构	瑞士量子中心《混合密钥分发协议》 (2024)	金融交易试点中 (2024 年启动)
巴西	NIST算法为主	国家电信局《5G 量子安全要求》 (2025) 、《数字盾牌计划》	5G 网络部署ML-KEM-768 (2026)
俄罗斯	GOST标准+抗量子扩展	量子安全国标草案 (GOST R 2025)	能源/军工系统优先迁移 (2027)

资料来源：中国联通研究院《2025中国联通后量子密码白皮书》，中邮证券研究所

四

相关企业与风险提示

- **IBM - 量子计算行业的领导者**：以自研硬件为核心，通过风投绑定初创企业与学术机构，最终形成“硬件-软件-应用”的闭环，构建**全栈量子生态系统**；**硬件方面实现了从量子比特数量竞争到系统性能突破的重大转变**，Nighthawk架构推动计算效率跃升，Heron处理器实现了双量子比特门错误率的历史性突破，300mm晶圆先进制造工艺可以将量子芯片研发速度提升一倍，其量子芯片发展遵循一条清晰的路线图，从2023年的433比特到2025年的1121比特，再到2027年的4096，最终在2029年实现10万逻辑比特的容错量子计算机；**软件方面Qiskit成为“量子界的Python”**，Qiskit SDK最新版本转译速度较竞争对手快83倍，动态电路技术允许在量子程序运行中插入经典计算逻辑，Qiskit C++接口打破量子计算与经典超算的壁垒，可直接用C++等语言调用量子算力；**量子纠错的双重突破打造“容错护盾”**，Loon处理器以更少物理量子比特编码更多逻辑量子比特，实时解码器将纠错时间压缩至480纳秒内，速度领先行业一个量级。
- **Google – 率先展示“量子优越性”**：2014年开启量子计算的发展之路，2019年用Sycamore处理器演示了超越经典的计算，该量子系统用200秒完成了一个需要花费经典计算机一万年的时间才能完成的目标计算，2023年实现了逻辑量子比特原型的首次演示，2024年发布量子芯片Willow，2025年在《Nature》发表量子算法突破性进展，**在Willow芯片上实现了首次可验证的量子优势算法“量子回声”**，其运行速度比世界上最好的超级计算机快1.3万倍，算法结果可重复验证，解决了之前量子计算结果难确认的问题。
- **IonQ – 首家上市的纯量子计算公司**：采用**离子阱技术路线**，正在通过一系列战略性收购和投资，构建一个涵盖硬件、软件、网络和传感的全面量子生态系统，其第五代量子计算机IonQ Tempo系统已成功实现了算法量子比特(#AQ) 64的破纪录性能，比原定路线图提前了整整三个月，其计算空间比IBM当前公开的量子系统大36万亿倍，是**唯一一家达到#AQ 64标准的公司**，有力地证明了离子阱技术在高保真度、高复杂度和规模化实用计算方面的固有优势。

- **Quantinuum – 全球最大的集成量子计算公司：**是一家综合性量子技术公司，2024年展示了创纪录的50个纠缠逻辑量子比特的GHZ态，相较微软和Atom Computing报告的结果，数量又翻了一倍多，保真度超过98%，是**英伟达首家投资的量子计算公司**；于2025年11月推出最新一代离子阱量子处理器**Helios**，该处理器基于量子电荷耦合器件（QCCD）架构，采用98个钡离子作为物理量子比特，实现了99.9975%单比特门保真度，99.921%的全连接双比特门保真度以及99.952%的量子态探测与制备保真度，**在商用级量子计算机中达到了最高的综合精度。**
- **Rigetti – 业界首个多芯片量子处理器：**是一家专注于超导量子处理器开发的上市公司，提供从芯片设计到制造、软件及云服务的垂直整合量子计算全栈解决方案；2025年8月其36量子比特多芯片量子计算机Cepheus-1-36Q全面上市，是业界最大的多芯片量子计算机，可实现高达99.5%的中位双量子比特门保真度，由四个包含9个量子比特的独立小芯片拼接而成，这种**多芯片架构**是Rigetti的专利技术；其核心价值在于它成功验证了多芯片架构在扩展超导量子计算机方面的可行性，并通过这种新方法实现了关键性能指标的显著提升。
- **D-wave – 量子计算商业化的先行者：**战略上将总部迁至佛罗里达博卡拉顿，并与佛罗里达大西洋大学（FAU）深度合作，建立研发中心，同时FAU签署了一项价值2000万美元的协议，购买并安装一台Advantage2物理系统；**技术上推进“退火+门模型”双路线**，其Advantage2系统已在物流调度、金融组合优化和材料模拟等领域展现出超越传统算法的实战能力，但要实现通用的量子算法，必须依靠门模型技术，D-Wave通过收购Quantum Circuits Inc.拥有了全球最顶尖的超导门模型技术团队，目标是在2026年底推出首个商用级门模型系统；**商业上已经开始通过其实际运行的量子系统产生千万美金级的现金流**，联手Anduril和Davidson进军防空拦截领域，与一家财富100强公司签订了价值1000万美元、为期两年的企业级量子计算即服务（QCaaS）协议，与意大利政府及Q-Alliance签署了一项价值1000万欧元的协议，为其在伦巴第大区建设最先进的量子研究设施提供Advantage2系统50%的算力容量。

- **国盾量子 (688027.SH)**：技术起源于中国科学技术大学，主要从事量子通信、量子计算、量子精密测量产品的研发、生产和销售，并提供相关的技术服务；在量子计算领域，深度参与“祖冲之”系列量子计算前沿研究，参与合肥超量融合计算中心项目，为合肥先进计算中心“巢湖明月”提供200 比特超导量子计算机、超量融合系统及配套软硬件设施等，为中电信量子集团“天衍”量子计算云平台提供了一体化整机搭建服务，同时量子计算业务国际推广实现突破，将向海外交付一台25比特超导量子计算机整机；
- **本源量子 (2025年9月完成IPO辅导备案)**：2月24日，我国首款自主研发量子计算机操作系统“本源司南”正式开放线上下载，这是全球首个开放下载的量子计算机操作系统，“本源司南”由本源量子自主研发，2021年首次发布，历经多轮迭代升级，已成为兼容超导、离子阱、中性原子等多种主流技术路线的“量超智”融合先进计算操作系统，目前已部署在“本源悟空”系列量子计算机上并对外开放。
- **国仪量子 (2025年12月科创板IPO申请获上交所受理)**：已构建起以量子信息技术与自旋共振系列、电子显微镜系列为核心的五大产品线，在自旋共振领域，国仪量子是国内唯一具有电子顺磁共振波谱仪自主研发与生产能力的企业，打破了国外巨头的长期垄断，其产品在全球市场份额已达25%，位居全球第二，仅次于布鲁克；在量子传感领域，公司是国内唯一实现全系列基于NV色心技术路径的量子传感产品研发的企业，其量子钻石单自旋谱仪是“国际首台”，扫描NV探针显微镜是“我国首个产业落地产品”；此外，公司在电子显微镜领域也占据国内品牌市场份额第一的位置。
- **玻色量子 (完成数亿A++轮融资)**：在相干光源、低损耗光路、高速测控等关键技术上持续攻坚，构建起完全自主的光量子计算整机工程体系，2025年8月其自建的“专用光量子计算机制造工厂”正式落地深圳南山区，同时在南山智城注册成立分别负责相干光量子计算机整机及核心部件的规模化生产任务和相干光量子计算机销售与技术服务的两家子公司；2025年11月，中国首个规模化专用光量子计算机制造工厂启幕仪式在深圳南山智城举行，预计工厂年产光量子计算机可达数十台/套，可形成专用光量子计算机的批量生产产能。

- **整机或产品：**国盾量子（量子通信绝对龙头，业务覆盖量子通信/量子计算/量子精密测量三大领域）、科大国创（参股国仪量子与九章量子）、纬德信息（参股玻色量子，量子应用）、神州信息（量子通信在金融等领域应用落地）等；
- **零部件与基础设施：**国芯科技（量子安全芯片）、禾信仪器（量子测量，拟收购上海量羲控制权）、华工科技（量子点激光器）、光迅科技（量子通信光器件）、亨通光电（量子光缆）等；
- **后量子安全：**格尔软件（抗量子密码产品与服务）、三未信安（抗量子密码产品）、信安世纪（后量子密码迁移）等。

- **技术突破不及预期风险：**尽管量子计算的前景令人振奋，但要从今天的几十、几百个噪声量子比特发展到未来拥有数百万个容错逻辑量子比特的通用量子计算机，仍需跨越一系列巨大的科学和工程障碍；若相关技术突破不及预期，会导致行业整体商业化进度滞后；
- **下游应用落地不及预期风险：**量子比特所独有的叠加与纠缠特性，赋予了量子计算机在原理上超越经典计算机的强大并行计算能力，为解决人类在基础科学、新药研发、材料设计等领域面临的若干“不可解”难题带来了希望的曙光，若下游场景验证与适配进展不顺利，则会大幅拉长企业投入回收周期；
- **软件生态系统与供应链不完善风险：**一个开放、活跃、繁荣的软件生态系统，才是将硬件算力转化为实际应用价值，若我国在量子软件生态方面的差距未得到及时补足，或影响行业整体发展，同时量子计算相关的核心材料与器件对提升物理量子比特的质量非常关键，若核心材料与器件依赖进口，则可能面临供给受限，拖慢产业化进程；
- **政策支持力度减弱风险等：**量子计算处在从实验室走向产业化的关键跃迁阶段，目前各主流路线各有优劣，技术还远未收敛，可能还需要较长一段时间的发展，需要在政策、资金以及人才等方面给予持久性的支持。

感谢您的信任与支持!

THANK YOU

孙业亮（首席分析师）

SAC编号: S1340522110002

邮箱: sunyeliang@cnpsec.com

刘聪颖（分析师）

SAC编号: S1340525100001

邮箱: liucongying@cnpsec.com

分析师声明

撰写此报告的分析师（一人或多人）承诺本机构、本人以及财产利害关系人与所评价或推荐的证券无利害关系。

本报告所采用的数据均来自我们认为可靠的目前已公开的信息，并通过独立判断并得出结论，力求独立、客观、公平，报告结论不受本公司其他部门和人员以及证券发行人、上市公司、基金公司、证券资产管理公司、特定客户等利益相关方的干涉和影响，特此声明。

免责声明

中邮证券有限责任公司（以下简称“中邮证券”）具备经中国证监会批准的开展证券投资咨询业务的资格。

本报告信息均来源于公开资料或者我们认为可靠的资料，我们力求但不保证这些信息的准确性和完整性。报告内容仅供参考，报告中的信息或所表达观点不构成所涉证券买卖的出价或询价，中邮证券不对因使用本报告的内容而导致的损失承担任何责任。客户不应以本报告取代其独立判断或仅根据本报告做出决策。

本报告所载的意见、评估及预测仅为本报告出具日的观点和判断。该等意见、评估及预测无需通知即可随时更改。过往的表现亦不应作为日后表现的预示和担保。在不同时期，中邮证券可能会发出与本报告所载意见、评估及预测不一致的研究报告。

中邮证券及其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头寸并进行交易，也可能为这些公司提供或者计划提供投资银行、财务顾问或者其他金融产品等相关服务。

《证券期货投资者适当性管理办法》于2017年7月1日起正式实施，本报告仅供中邮证券签约客户使用，若非中邮证券签约客户，为控制投资风险，请取消接收、订阅或使用本报告中的任何信息。本公司不会因接收人收到、阅读或关注本报告中的内容而视其为签约客户。

本报告版权归中邮证券所有，未经书面许可，任何机构或个人不得存在对本报告以任何形式进行翻版、修改、节选、复制、发布，或对本报告进行改编、汇编等侵犯知识产权的行为，亦不得存在其他有损中邮证券商业性权益的任何情形。如经中邮证券授权后引用发布，需注明出处为中邮证券研究所，且不得对本报告进行有悖原意的引用、删节或修改。

中邮证券对于本申明具有最终解释权。

公司简介

中邮证券有限责任公司，2002年9月经中国证券监督管理委员会批准设立，是中国邮政集团有限公司绝对控股的证券类金融子公司。

公司经营范围包括:证券经纪，证券自营，证券投资咨询，证券资产管理，融资融券，证券投资基金销售，证券承销与保荐，代理销售金融产品，与证券交易、证券投资活动有关的财务顾问等。

公司目前已经在北京、陕西、深圳、山东、江苏、四川、湖北、湖南、福建、辽宁、吉林、黑龙江、广东、浙江、贵州、新疆、河南、山西、上海、云南、内蒙古、重庆、天津、河北等地设有分支机构，全国多家分支机构正在建设中。

中邮证券紧紧依托中国邮政集团有限公司雄厚的实力，坚持诚信经营，践行普惠服务，为社会大众提供全方位专业化的证券投、融资服务，帮助客户实现价值增长，努力成为客户认同、社会尊重、股东满意、员工自豪的优秀企业。

投资评级说明

投资评级标准	类型	评级	说明
报告中投资建议的评级标准： 报告发布日后的 6 个月内的相对市场表现，即报告发布日后的 6 个月内的公司股价（或行业指数、可转债价格）的涨跌幅相对同期相关证券市场基准指数的涨跌幅。 市场基准指数的选取：A 股市场以沪深 300 指数为基准；新三板市场以三板成指为基准；可转债市场以中信标普可转债指数为基准；香港市场以恒生指数为基准；美国市场以标普 500 或纳斯达克综合指数为基准。	股票评级	买入	预期个股相对同期基准指数涨幅在 20%以上
		增持	预期个股相对同期基准指数涨幅在 10%与 20%之间
		中性	预期个股相对同期基准指数涨幅在-10%与 10%之间
		回避	预期个股相对同期基准指数涨幅在-10%以下
	行业评级	强于大市	预期行业相对同期基准指数涨幅在 10%以上
		中性	预期行业相对同期基准指数涨幅在-10%与 10%之间
		弱于大市	预期行业相对同期基准指数涨幅在-10%以下
	可转债评级	推荐	预期可转债相对同期基准指数涨幅在 10%以上
		谨慎推荐	预期可转债相对同期基准指数涨幅在 5%与 10%之间
		中性	预期可转债相对同期基准指数涨幅在-5%与 5%之间
		回避	预期可转债相对同期基准指数涨幅在-5%以下

中邮证券研究所

北京

邮箱: yanjiusuo@cnpsec.com

地址: 北京市东城区前门街道珠市口东大街17号

邮编: 100050

上海

邮箱: yanjiusuo@cnpsec.com

地址: 上海市虹口区东大名路1080号大厦3楼

邮编: 200000

深圳

邮箱: yanjiusuo@cnpsec.com

地址: 深圳市福田区滨河大道9023号国通大厦二楼

邮编: 518048



中邮证券

CHINA POST SECURITIES