

后量子密码技术：应对量子计算威胁的关键防线

2025 年 09 月 16 日

► **量子计算有望成为解决 AI 算力瓶颈的颠覆性力量。**与传统计算相比，量子计算能够带来更强的并行计算能力，同时具备更低的能耗，在 AI 领域具有较大潜力。在全球科技巨头的争相布局下，量子计算软硬件体系已经初具雏形，根据 ICV 数据，2023 年市场规模已达到 47 亿美元，预计 2035 年有望超过 8000 亿美元。硬件层面，超导量子计算进展斐然，国内量子计算产业与海外科技巨头差距不断缩小。应用层面，量子计算与各领域加速融合。

► **应对量子计算挑战，后量子密码技术加速演进。**随着量子计算技术在硬件、算法等层面不断取得突破性进展，其强大的计算能力正给传统密码体系带来前所未有的威胁，现有基于大整数分解的大量加密系统都可能面临被破解的风险。后量子密码技术旨在构建能够抵御量子计算机攻击的新型密码体系，成为保障未来信息安全的重要手段。目前，美国在后量子密码领域的发展处于全球领先地位，国内则处于标准完善与产业试点阶段。

► **聚焦未来技术变革，国内龙头企业加速布局。**随着后量子密码技术的迅猛发展，国内网络安全与量子计算领域的龙头企业纷纷加速布局，从算法研发、硬件创新到行业场景落地等多个维度发力，积极推动后量子密码技术的迭代与应用拓展，力求在这一前沿领域占据先发优势，为我国构建未来自主可控的信息安全屏障提供坚实支撑。

- **国盾量子：**完整产业链支撑后量子密码技术商业化落地；
- **三未信安：**自主研发的量子计算时代的密码产品，涵盖从密码芯片到密码板卡、密码整机、密码系统的全系列抗量子密码产品体系；
- **吉大正元：**积极推进抗量子密码迁移研究，实现从算法到应用的全栈创新；
- **天融信：**战略投资入局量子计算，芯片级后量子密码卡引领安全产品升级；
- **电科网安：**发布“量铠”抗量子密码系列产品，构建全链条安全生态；
- **格尔软件：**精研前沿技术，抗量子迁移解决方案聚焦金融行业落地试点；
- **国芯科技：**推动量子技术+信创芯片结合，“算法-芯片-产品”全链条布局。

► **投资建议：**量子计算凭借指数级并行处理能力、全域协同特性与超低能耗优势，正从根本上颠覆传统计算架构，不仅成为破解 AI 算力瓶颈的颠覆性力量，也对传统密码体系的安全性构成严峻挑战。后量子密码技术旨在构建能够抵御量子计算机攻击的新型密码体系，成为保障未来信息安全的重要手段。当前，该技术的标准化进程加速推进，应用探索不断深入，国内外龙头企业亦纷纷加大布局力度，竞争态势日益凸显。建议关注国盾量子、三未信安、吉大正元、天融信、电科网安、格尔软件、国芯科技等后量子密码技术标的，以及启明星辰、科大讯飞、禾信仪器、神州信息、科华数据、中国长城、光迅科技、紫光国微、亨通光电等量子计算相关标的。

► **风险提示：**量子计算技术发展不及预期，行业竞争加剧。

推荐

维持评级



分析师 吕伟

执业证书：S0100521110003

邮箱：lwwei_yj@glms.com.cn

相关研究

- 1.计算机周报 20250914：再次强调国产 AI i nfra 机遇-2025/09/14
- 2.计算机周报 20250907：空天计算为什么会成为“东数西算”破局关键？-2025/09/07
- 3.计算机行业 2025 年中报总结：收入加速复苏，盈利质量稳中有升-2025/09/03
- 4.计算机周报 20250831：国产 AI Infra 崛起：从算力到云与数据库-2025/08/31
- 5.计算机周报 20250824：国产 AI 算力与信创有望共迎拐点-2025/08/24

并购家 免费行业报告网

IPOIPO.CN 每日更新 不用注册会员 无广告 永久免费

目录

1 应对量子计算挑战，后量子密码技术加速演进	3
1.1 量子力学颠覆经典计算体系，运算能力空前增强	3
1.2 巨头争先入场，量子计算边界持续拓展	5
1.3 量子计算威胁加密系统，后量子密码构筑全新防线	8
1.4 后量子密码发展现状：美国全球领先，中国持续追赶	9
2 聚焦未来技术变革，国内龙头企业加速布局	13
2.1 三未信安	13
2.2 天融信	14
2.3 电科网安	15
2.4 吉大正元	16
2.5 国盾量子	17
2.6 格尔软件	17
2.7 国芯科技	18
3 投资建议	20
4 风险提示	21
插图目录	22
表格目录	22

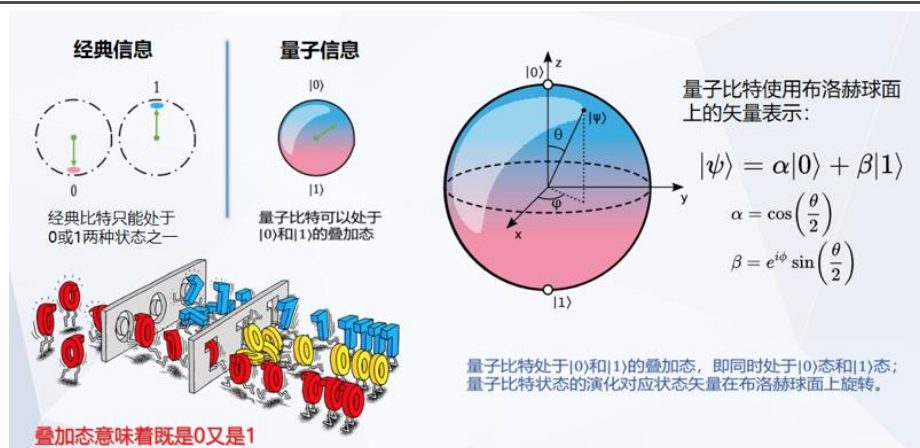
1 应对量子计算挑战，后量子密码技术加速演进

1.1 量子力学颠覆经典计算体系，运算能力空前增强

量子计算是基于量子力学的独特行为（如叠加、纠缠和量子干扰）的计算模式，基本信息单位为量子比特。据微软，在物理学中量子是所有物理特性的最小离散单元，通常指原子或亚原子粒子（如电子、中微子和光子）的属性。量子比特是量子计算中的基本信息单位，在量子计算中发挥的作用与比特在传统计算中发挥的作用相似，但经典比特是二进制、只能存放 0 或 1 位，而量子比特可以存放所有可能状态的叠加。量子计算所运用的物理特性主要包括：

- 1) **量子叠加**：处于叠加态时，量子粒子是有可能状态的组合，它们会不断波动，直到被观察和测量；以抛硬币为例，经典比特可以通过正面和反面来度量，而量子比特能够代表硬币的正反面以及正反交替时的每个状态；
- 2) **量子纠缠**：纠缠是量子粒子将其测量结果相互关联的能力，当量子比特相互纠缠时，它们构成一个系统并相互影响，人们可以使用一个量子比特的度量来作出关于其他量子比特的结论，通过在系统中添加和纠缠更多的量子比特，量子计算机可计算指数级的更多信息并解决更复杂的问题；
- 3) **量子干扰**：量子干扰是量子比特固有的行为，由于叠加而影响其坍缩方式的可能性，量子计算机旨在尽可能减少干扰，确保提供最准确的结果。

图1：经典比特与量子比特对比

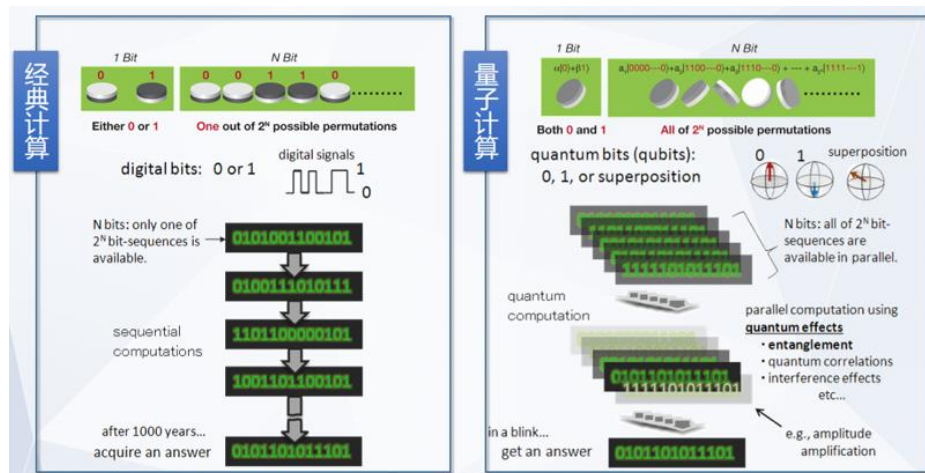


资料来源：爱集微，本源量子，民生证券研究院

与传统计算相比，量子计算能够带来更强的并行计算能力、协同处理能力和更低的能耗。据赛迪智库、东进技术，量子计算通过量子态的受控演化实现数据的存储计算，可以分为数据输入、初态制备、量子逻辑门操作、量子测算和数据输出等步骤，其中量子逻辑门操作是一个幺正变换，这是一个可以人为控制的量子物理演

化过程；经典计算机的运算模式为逐步计算，一次运算只能处理一次计算任务，而量子计算为并行计算，可以同时处理 2^n 个数进行数学运算，相当于经典计算重复实施 2^n 次操作。同时，量子计算机中多个处于纠缠态的量子比特之间存在瞬时关联，即便相隔甚远，对一个量子比特的操作也会立即影响其他纠缠量子比特，这种特性使得量子计算机在处理多体系统、复杂网络等问题时，能够快速捕捉到系统各部分之间的关联和相互作用，完成传统计算机难以胜任的复杂计算任务。能耗方面，传统芯片的特征尺寸很小（数纳米）时，量子隧穿效应开始显著，电子受到的束缚减小，使得芯片功能降低、能耗提高，传统摩尔定律失效。相较之下，量子计算中的幺正变换属于可逆操作，有利于提升芯片的集成度，进而降低信息处理过程中的能耗。

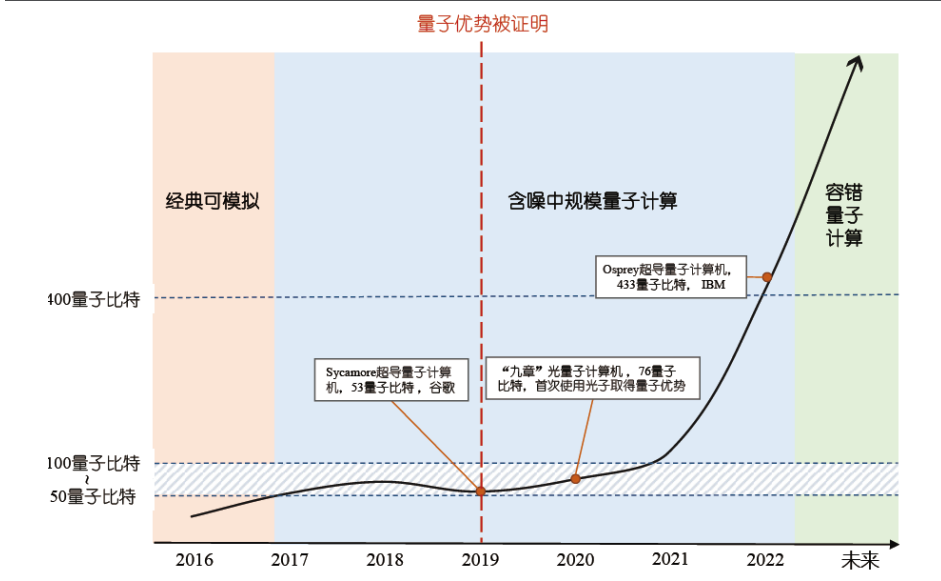
图2：量子计算与经典计算体系对比



资料来源：爱集微，本源量子，民生证券研究院

量子计算的运算能力根据量子比特数量指数级增长，在 AI 领域具有较大潜力。在经典计算中，计算能力与晶体管数量成正比例线性关系，而量子计算机中算力将以量子比特的指数级规模增长，据中国计算机学会微信公众号，2012 年“量子优势”（同样的计算任务，量子计算速度高于传统计算）的概念被提出，并在 2019 年由谷歌团队实现了实验验证，2020 年，潘建伟院士团队基于高斯玻色采样模型成功构建了 76 个光子的量子计算原型机“九章”进一步验证了量子优势。量子计算机所能拥有的量子比特数由最初的 2 量子比特增长到了数百量子比特，并正以可观的速度继续增长，这为实现更可靠、更大规模的量子计算，以及挖掘基于量子计算的人工智能应用带来更多可能性。

图3：经典计算机与量子计算机运算能力对比



资料来源：中国计算机学会微信公众号，民生证券研究院

1.2 巨头争先入场，量子计算边界持续拓展

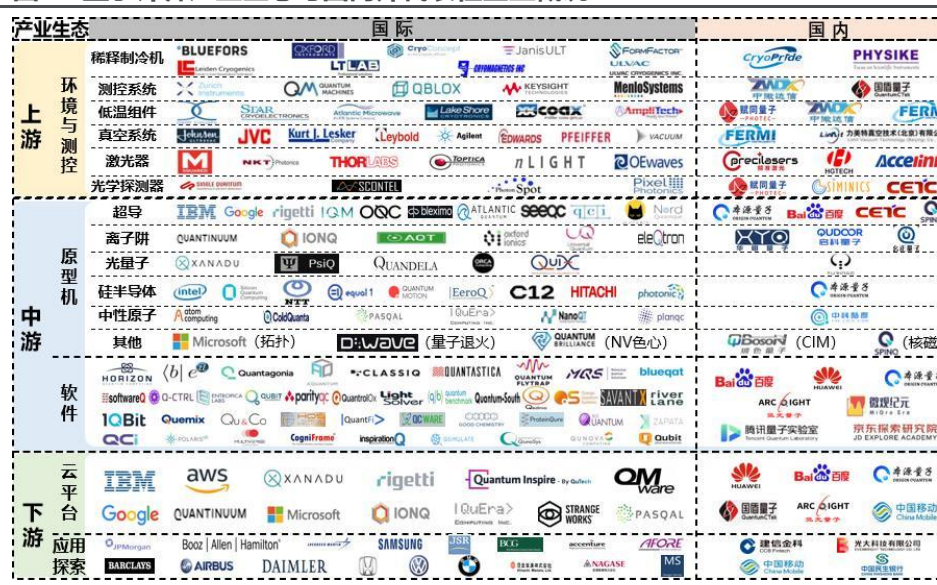
量子计算软硬件体系已经初具雏形。据信通院：

量子计算产业上游主要包含环境支撑系统、测控系统、各类关键设备组件以及元器件等，是研制量子计算原型机的必要保障，目前由于技术路线未收敛、硬件研制个性化需求多等原因，上游供应链存在碎片化问题，逐一突破攻关存在难度，一定程度上限制了上游企业的发展。

量子计算产业生态中游主要涉及量子计算原型机和软件，其中原型机是产业生态的核心部分，目前超导、离子阱、光量子、硅半导体和中性原子等技术路线发展较快，其中超导路线备受青睐，离子阱、光量子 and 中性原子路线获得较多初创企业关注。美国原型机研制与软件研发占据一定优势，我国量子计算硬件企业数量有限且技术路线布局较为单一，集中在超导和离子阱路线，量子计算软件企业存在数量规模较少、创新成果有限、应用探索推动力弱等问题。

量子计算产业下游主要涵盖量子计算云平台以及行业应用，处在早期发展阶段。近年来全球已有数十家公司和研究机构推出了不同类型的量子计算云平台，积极争夺产业生态地位，目前量子计算领域应用探索已在金融、化工、人工智能、医药、汽车、能源等领域广泛开展。国外量子计算云平台的优势体现在后端硬件性能、软硬件协同程度、商业服务模式等方面，大量欧美行业龙头企业成立量子计算研究团队，与量子企业联合开展应用研究；我国下游行业用户对量子计算重视程度有限，开展应用探索动力仍需提升。

图4：量子计算产业生态与国内外代表性企业概况



资料来源：信通院，民生证券研究院

硬件层面：超导量子计算进展斐然，国内量子计算产业与海外科技巨头差距不断缩小。据光子盒研究院，从技术路线上看，近年超导量子计算的进展最为亮眼，主要原因包括：1) 超导量子计算路线本身具备保真度高、运算速度快、扩展性好、可控性强等优势，从而受到更多科研人员与投资机构的关注；2) 超导量子计算机与成熟的电子学、半导体工艺密切相关，而离子阱、中性原子等技术路线所用设备多为成熟度相对较低的光子学设备。

图5：中国第三代自主超导量子计算机“本源悟空”

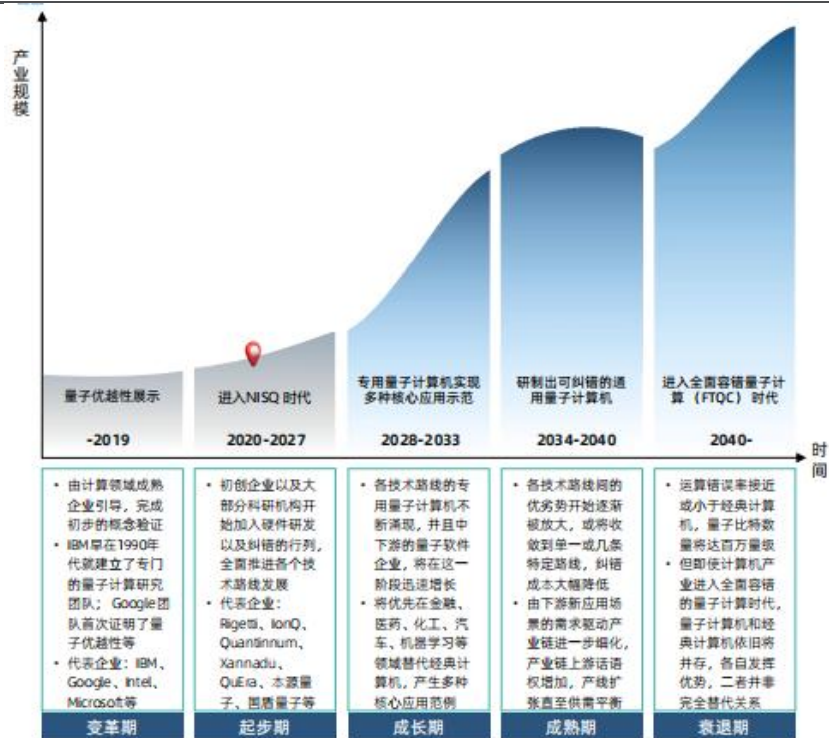


资料来源：本源量子官网，民生证券研究院

应用层面：量子计算与各领域加速融合。据光子盒研究院，量子计算的行业应用合作广泛涉及教育科研、生物医药、化工材料、国防政务、能源电力、金融服务、

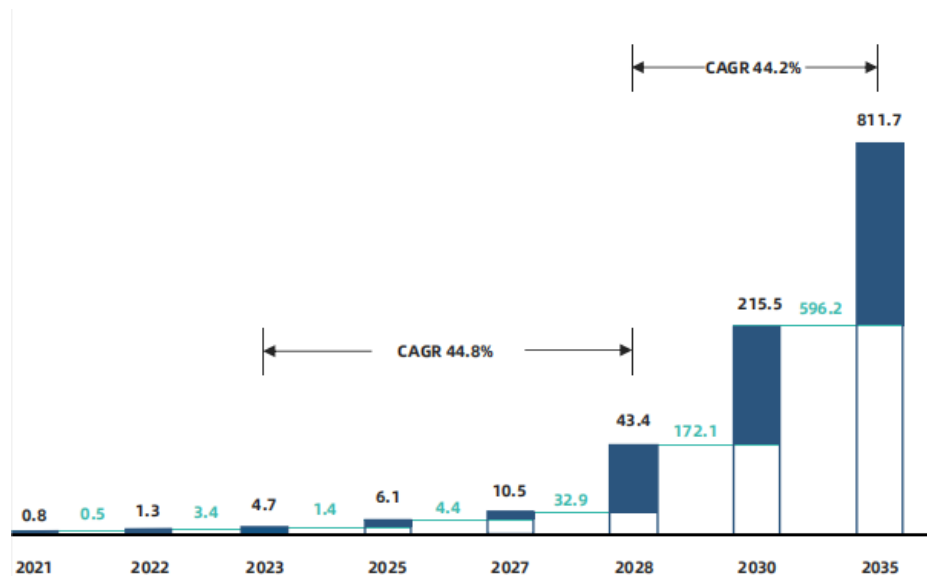
人工智能等多个领域，由于目前量子计算机都未达到实用化阶段，无法就现实问题提供算力支持，现阶段的各类应用合作尚处于早期探索阶段。在金融领域，量子计算的高速计算能力可用于风险分析和投资组合优化，提高决策效率与投资回报；在药物研发中，量子计算能够模拟分子行为，为新药设计提供关键数据支持，缩短研发周期；在材料科学里，量子计算助力科学家深入理解材料内部电子行为与相互作用，加速高性能电池、超导体和新型合金等新材料的开发。

图6：全球量子计算发展历程



资料来源：ICV，民生证券研究院

2023 年全球量子计算市场规模约 47 亿美元，预计 2035 年有望超过 8000 亿美元。据 ICV，随着量子计算技术的不断演进，以及 AI 技术等领域的快速发展，量子计算的应用边界被不断拓展，2023 年，全球量子产业规模达到 47 亿美元，2023 至 2028 年的年平均增长率（CAGR）达到 44.8%；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 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。

图7：全球量子计算产业规模（2021~2035）（单位：十亿美元）


资料来源：ICV，民生证券研究院

1.3 量子计算威胁加密系统，后量子密码构筑全新防线

强大计算性能打破传统密码学安全屏障，加密系统面临失效风险。随着量子计算技术在硬件、算法等层面不断取得突破性进展，其强大的计算能力正给传统密码体系带来前所未有的威胁。传统密码学基于大整数分解、离散对数等数学难题构建，依靠经典计算机在有限时间内难以破解这些难题来保障信息安全。然而，量子计算凭借独特的量子算法，打破了这一安全屏障。例如，RSA加密算法的安全性依赖于对两个大质数乘积进行分解的困难性，一旦量子计算机具备足够多的量子比特和稳定的运行环境，其独特的Shor算法能够利用量子计算的量子叠加和量子纠缠特性，在多项式时间内完成大整数分解，从而破解RSA密码体系。目前，超导量子计算原型机“祖冲之三号”、谷歌的“Willow”量子芯片等硬件成果在量子比特数量和计算性能上不断提升，为Shor算法的有效运行提供了更坚实的基础，这意味着在不久的将来，现有基于大整数分解的大量加密系统都可能面临被破解的风险。

量子计算的发展不仅威胁到加密算法本身，还对依赖传统密码技术的通信协议、数字签名等安全机制产生连锁反应。基于传统密码的安全通信协议在量子计算的冲击下，无法保障信息传输的机密性和完整性；数字签名体系也可能因量子计算破解密钥而失去可靠性，导致身份认证、数据不可抵赖等安全功能失效。

后量子算法保障未来信息安全，多种技术方案助力构建安全屏障。随着传统密码体系在量子算法的冲击下岌岌可危，后量子算法应运而生，成为保障未来信

息安全的重要手段。后量子密码技术（Post-Quantum Cryptography,PQC），也称为抗量子密码技术（Quantum-Resistant Cryptography,QRC），旨在构建能够抵御量子计算机攻击的新型密码体系，其核心目标是基于量子计算机难以快速解决的数学难题或物理特性，设计出安全可靠的加密、签名和密钥交换机制。后量子算法涵盖多种技术路线：

1) **基于格的密码算法**：利用格中最短向量问题和最近向量问题的困难性构建密码方案。这些问题在高维空间中具有极高的计算复杂度，即便量子计算机也难以在短时间内求解，从而为信息安全提供保障。

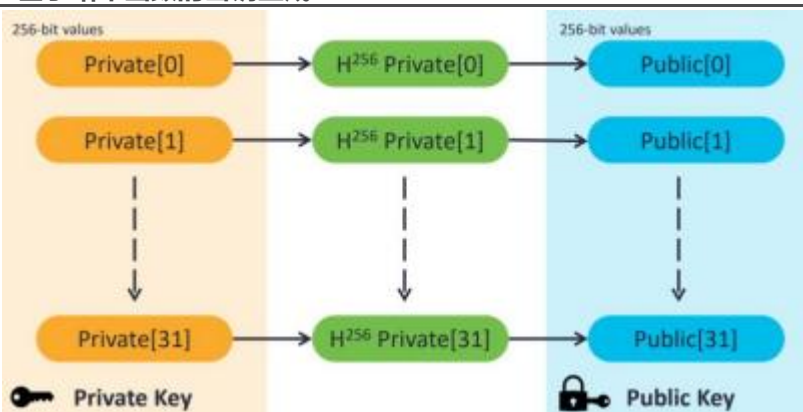
2) **基于哈希的后量子密码算法**：以哈希函数的单向性和碰撞阻力为核心，构建数字签名等密码机制，有效规避了传统密码算法在量子计算冲击下的安全风险。

3) **基于编码的密码算法**：以纠错码理论为基础，通过构造具有特定性质的纠错码来实现密码功能。由于解码随机线性码是一个NP-Hard问题，即使量子计算机也难以有效解决，使得基于编码的密码算法具备较强的抗量子攻击能力。

4) **基于多变量的后量子密码算法**：基于有限域上的多变量多项式方程组求解困难性设计密码方案。通过精心构造复杂的多变量多项式系统，使得攻击者在没有私钥的情况下，求解方程组变得极其困难。即便面对量子计算机，多变量密码算法所依赖的数学难题依然具有较高的安全性。

5) **基于同源的后量子密码算法**：基于代数几何中椭圆曲线或超椭圆曲线的同源问题构建密码方案，利用求解特定同源问题的计算困难性，为信息安全提供抵御量子攻击的坚实屏障。

图8：基于哈希函数的密钥生成



资料来源：东进技术《后量子密码技术白皮书》，民生证券研究院

1.4 后量子密码发展现状：美国全球领先，中国持续追赶

美国在后量子密码（PQC）领域的发展处于全球领先地位，体现在标准化进

程、政府战略部署、产业应用等多个层面。

1) **标准化进程：美国国家标准与技术研究院（NIST）主导，从技术研发到政策落地系统性布局。**2016 年 12 月，NIST 向全球发出后量子公钥密码算法“征集令”，意在遴选可抵御量子攻击的新一代算法，逐步替换现行易被量子计算破解的公钥加密体系。2024 年，首批后量子密码联邦信息处理标准（FIPS）正式发布，自此美国政府与产业界全面启动向后量子安全的系统性迁移，形成了一套环环相扣、全面且系统的推进体系。这一系列举措不仅有助于美国在量子计算时代抢占信息安全领域的战略高地，也为全球后量子密码技术的发展与应用提供了可复制的范例。目前，NIST 已确定的标准化算法包括两个密钥封装算法和三个签名算法，未来还将还将持续吸纳多元技术路线的签名方案，进一步丰富后量子密码“工具箱”。

表1：NIST 标准化后量子密码算法特性比较

NIST 算法	技术路线	公钥长度 (Byte)	签名/密文长度 (Byte)	签名/加密速度
ML-KEM	格密码	800 / 1184 / 1568	768 / 1088 / 1568	高
ML-DSA	格密码	1312 / 1952 / 2592	2420 / 3309 / 4627	中
SLH-DSA	哈希密码	32-64	7856-49856	极低
FN-DSA (待发布)	格密码	897/1345/1793	666/1019/1380	签名慢、验签快
HQC (待标准化)	编码密码	24576 / 36864 / 49152	1152 / 1728 / 2304	中

资料来源：东进技术《后量子密码技术白皮书》，民生证券研究院

2) **路线图：2030年前完成后量子密码标准迁移。**2021 年 10 月，NIST 发布了应对量子技术风险的路线图，以帮助企业保护其数据和系统，降低量子技术发展带来的风险。路线图提出 2024 年发布后量子密码算法标准，2030 年前迁移到后量子密码标准。美国政府安全机构与科技企业也积极推动后量子密码技术落地实践，纷纷抢在大型量子计算机问世前，加速部署抗量子算法。

图9：美国 2021 版应对量子技术风险路线图



资料来源：东进技术《后量子密码技术白皮书》，民生证券研究院

3) **产业推进：大型跨国公司和行业巨头加速构建产业生态。产品供给方面**，IBM 推出 QuantumSafe 整套解决方案，涵盖发现、观察和转换产品；微软推出开放量子安全项目 liboqs，成为最受欢迎的开源后量子密码项目；谷歌宣布与苏黎世联邦理工学院合作，成功创建了独特的 ECC/Dilithium 混合签名模式，首次实现开源量子弹性/抗量子 FIDO2 安全密钥。**应用方面**，2023 年 6

月，SandboxAQ 公司获得由美国国防信息系统局（DISA）提供的合同，以实施该公司端到端的后量子加密管理解决方案。2024 年 9 月，谷歌宣布更新其 Chrome 网络浏览器中的后量子加密技术，用完全标准化的 ML-KEM 算法取代实验性的 Kyber，以提升对量子计算潜在攻击的防御能力。

图10：量子安全产业发展周期



资料来源：光子盒研究院，民生证券研究院

国内后量子密码技术起步较晚，目前处于标准完善与产业试点阶段。

1) **标准化进程：国家标准化管理委员会启动规划与立项工作。**中国密码学会在 2019 年组织了全国密码算法设计竞赛，其中非对称算法部分征集到38个算法，经过形式审查、公开评议、检测评估和专家评选，竞赛最终评出14项优胜算法。2023 年，国家标准化管理委员会开展后量子密码标准的前瞻研究和规划布局。2024 年一些后量子密码方案已在我国密码行业标准化技术委员会立项。2025 年 2 月，商用密码标准研究院面向全球征集新一代公钥、杂凑、分组密码算法，明确要求算法需同时抵抗经典与量子攻击。

2) **产业推进：硬件研究+应用探索并行，加速追赶全球领先水平。**芯片研究方面，清华大学刘雷波教授团队设计了跨数学难题的抗量子密码芯片；华中科技大学研发的后量子密码芯片在 SMIC40nm 工艺下实现 Kyber 算法。**芯片供给方面**，目前市场上尚未出现公开发售的商业后量子密码芯片产品，一些密码厂商也 宣布推出了后量子密码软硬件产品，但总体仍处于内部测试或试点验证。**开源密码库方面**，郁昱教授团队开发和维护的 PQMagic 支持 FIPS 203-205 标准及国产Aegis 算法。**后量子密码应用试点方面**，华夏银行区块链试点

Dilithium-SM3 混合签名方案，交易验证时间控制在 300ms 内，较传统方案延迟增加约 20%，但安全性提升两个数量级。中国电信 5G 核心网部署“密流量量子盾”系统，集成Kyber、Dilithium 算法，实现量子安全漫游认证，密钥协商效率达 5000 次/秒。

图11：全球量子安全产业生态图谱



资料来源：光子盒研究院，民生证券研究院

2 聚焦未来技术变革，国内龙头企业加速布局

2.1 三未信安

密码芯片龙头，商用密码基础设施提供商。公司产品全面支持国产 SM1、SM2、SM3、SM4、SM7、SM9、ZUC 等密码算法及抗量子密码算法，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、密钥管理等密码服务。

自研抗量子全系列密码产品。三未信安自主研发的量子计算时代的密码产品，涵盖从密码芯片到密码板卡、密码整机、密码系统的全系列抗量子密码产品体系。抗量子全系列密码产品在兼容传统密码技术体系的基础上，具备对传统密码技术体系的抗量子加固功能，致力于为客户提供高安全、高性能的抗量子密码服务，抵御量子计算机带来的信息安全威胁。

抗量子密码产品全系支持 NIST 发布的四种标准抗量子密码算法，包括抗量子密码 SDK、抗量子 TLS 协议、抗量子密码芯片、抗量子 UKEY、抗量子密码板卡、抗量子密码机、抗量子网关、抗量子密码系统等软硬件产品和系统，可以实现用户抗量子密码需求的全场景覆盖。

图12：三未信安抗量子全系列密码产品



资料来源：三未信安官网，民生证券研究院

2.2 天融信

战略投资入局量子计算赛道，推动量子安全+网络安全有机融合。2018 年，天融信战略投资了安徽问天量子科技股份有限公司并与其达成合作，开始在量子计算领域进行投入和布局，并推出了量子网络密码机产品。目前，公司已将量子密码通信、量子密码认证、量子密码签名、量子密钥生成等研究成果应用于 VPN、堡垒机、服务器密码机、签名验签服务器等产品中，实现量子密码安全与网络安全的融合。此外，公司积极参与“宁苏量子干线”等国家级网络通信建设，积累了丰富的工程化经验。

国内首张芯片级后量子密码卡正式诞生，引领后量子安全产品全面升级。2025 年 7 月，安徽问天量子科技股份有限公司携手华中科技大学，成功研制出国内首颗后量子密码安全芯片及其配套密码卡，一举攻克后量子密码集成电路与应用落地的多项关键技术瓶颈。该密码卡采用“后量子密码 SoC + 量子随机数芯片”双芯同构架构，从微电子、密码学、软件工程、物理防护到侧信道攻防多维度系统化设计，兼容 NIST 候选算法体系与国密算法族，可一站式实现数字签名/验证、非对称/对称加解密、密钥生成等核心安全功能，为信息系统提供面向量子计算时代的全栈防护。多场景实测数据显示，该卡已在党政、金融、通信、能源等关键基础设施领域完成适配验证，性能、功耗、可靠性均达到规模化商用标准。而作为问天量子的战略股东，天融信有望凭借多年量子安全工程化经验，率先将该芯片集成至下一代防火墙、服务器密码机、VPN 等主力产品，推出“硬件 + 整机 + 系统”全栈后量子安全解决方案，持续引领行业升级。

图13：芯片级后量子密码卡实物图



资料来源：新浪财经，民生证券研究院

2.3 电科网安

深度布局后量子密码前沿领域研究，积极参与技术标准制定。作为以密码为核心的信息安全产品和系统的最大供应商之一，公司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，参与国家相关密码和安全技术标准的制定，并与高校、科研院所积极合作开展协同创新。

硬件+解决方案两翼齐飞，构建“芯片-设备-网络-云端”全链条安全生态。

1) **硬件**：公司大力发展以芯片为基础的核心密码能力，在抗量子技术领域实现了敏捷架构设计、全栈算法支持和高能效硬件加速等关键技术突破。2025年6月，公司正式发布了“量铠”抗量子密码系列产品。其中，量铠抗量子密码芯片作为信息安全的“底层地基”，实现了抗量子密码算法与传统密码算法的动态重构敏捷应用，其核心价值在于为整个信息安全体系提供从硬件层到应用层的全栈防护能力。该芯片具备从硬件到固件的多重防护设计，集成的抗量子密码算法引擎能以每秒数千次的速度完成密钥生成、加密、签名等运算，可作为公钥基础设施，参与数字安全基础设施建设，为金融交易、电力调度等高实时性场景提供高强度运算支持，确保数据在生成、传输、存储全生命周期的安全可控。

2) **应用创新**：公司基于理论、芯片、板卡、软件、整机、系统、平台、服务到解决方案的全产业链布局优势，面向后量子密码、同态加密、多方计算等前沿密码技术，以及5G、卫星互联网、工业互联网、车联网、物联网等新兴领域开展密码应用创新，形成了一站式、全覆盖的密评密改解决方案和行业整体解决方案。

3) **项目落地**：公司中标了中国移动研究院量子通信服务项目，成为中国移动量子密讯业务的重要安全支撑厂商，实现量子密钥管理及保密通信技术成果转化。

图14：“量铠”抗量子密码全栈产品矩阵



资料来源：电科网安微信公众号，民生证券研究院

2.4 吉大正元

积极推进抗量子密码迁移研究，实现从算法到应用的全栈创新。公司紧密围绕以“密码”为核心的战略，深入探索新型抗量子密码算法设计，成功将密码产品技术延展至量子密码和抗量子密码领域，构建了量子安全能力体系，确保产品在未来量子计算环境下的长期安全性，为企业在抗量子时代的密码应用提供了坚实保障。

1) 后量子 PKI 系统：兼容性与扩展性并重。吉大正元的后量子 PKI 系统采用模块化设计，将密码引擎、密钥管理等核心组件解耦，支持灵活集成新算法。其证书体系严格遵循 X.509v3 标准，兼容现有 PKI 生态，同时扩展了后量子双证书体系，增强安全性。这一设计为金融、政务等高安全需求场景提供了平滑升级路径。

2) 混合密钥协商与数字签名技术：LS 1.3 后量子混合密钥协商组件集成 NIST 标准后量子算法与传统算法，支持金融、政务等领域对 FIPS 认证的强制要求，适用于物联网、5G 通信等场景；多层默克尔树签名系统通过局部与全局认证路径设计，兼容标准证书链，减少企业迁移成本，已在敏感数据传输场景中验证有效性。

3) 产品矩阵：筑牢量子安全防线。吉大正元推出了多款后量子密码硬件设备，**后量子密码卡/密码机**集成国际主流后量子算法与国密算法，支持服务器、VPN 网关等设备的高效密码服务，可有效抵御量子攻击，为数据加密、数字签名和密钥交换等场景提供量子安全防护；**元密一体机**作为“密码安全+”底座，融合量子密钥与抗量子算法，提供动态密码算力调度、AI 赋能密码服务等能力，可满足中小型系统到大型平台的多样化需求，其超融合虚拟化能力支持密码服务与业务系统的一体化融合，显著降低运维复杂度。

4) 试点实践：从理论到落地的关键跨越。吉大正元联合中电信量子公司，通过 QKD（量子密钥分发）技术实现业务密钥的抗量子安全传输。该方案创新采用“量子密钥+后量子算法”的双重防护架构，既解决量子密钥远距离分发的技术瓶颈，又通过后量子密码机实现密钥使用环节的全生命周期保护，为金融业应对量子计算威胁提供了可复用的实施路径。

图15：吉大正元元密一体机



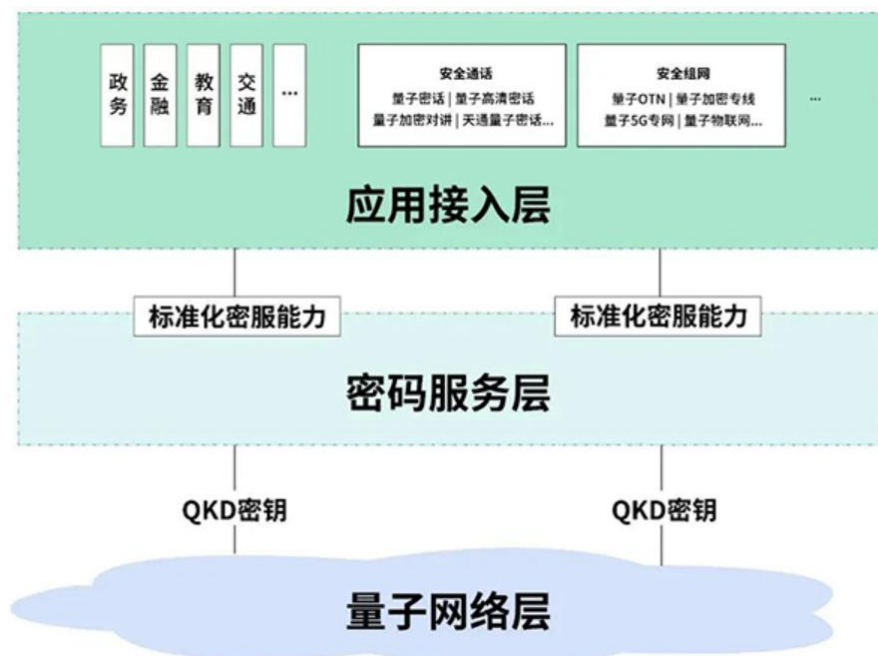
资料来源：吉大正元微信公众号，民生证券研究院

2.5 国盾量子

深耕量子技术产业化应用，完整产业链支撑后量子密码技术商业化落地。作为我国量子信息产业化的开拓者、实践者和引领者，国盾量子构建了涵盖量子通信、量子计算、量子精密测量领域的全产品矩阵。依托量子信息领域的深厚积淀，公司紧跟前沿科技攻关，不断推进国产化产业链发展，持续赋能后量子密码技术的探索

全球首个融合 QKD 和 PQC 的分布式密码体系正式发布，迈入规模化商用新纪元。2025 年 5 月，中电信量子携手国盾量子等单位，实现全球首例基于融合量子密钥分发（QKD）和后量子密码（PQC）的分布式密码体系，基于该体系的全局首例跨境量子密信电话在北京到合肥横跨 1000 公里距离成功接通，推动了“QKD+PQC”的量子安全解决方案从可行性验证走向规模化商用。“QKD+PQC”双保险的信息安全防线，可为用户提供端到端抗量子计算的密钥分发与密钥全生命周期管理，进一步推动了量子安全技术的广泛应用，构建数字时代抵御量子攻击的安全屏障。未来，国盾量子将持续探索“QKD+PQC”等量子安全技术的多元应用场景，切实助力我国构建未来自主可控的信息安全防线。

图16：融合 QKD 和 PQC 的分布式密码体系



资料来源：国盾量子官网，民生证券研究院

2.6 格尔软件

精研前沿技术，铸就新质生产力安全壁垒。格尔软件以技术研发作为核心推动力，以密码技术为核心，在研发端取得多项进展。在量子威胁逐渐显现的背景下，

公司提前布局，2024 年完成了全线密码产品抗量子能力的升级工作，不仅兼容美国 NIST 发布的抗量子算法，还完成了 CTRU/CNTR、LMS/HSS-SM3、Aigis-Sig 等中国抗量子算法的工程实现。在 2024 年 6 月召开的中国（上海）国际技术进出口交易会上，公司发布了量子安全 PKI 基础设施、量子安全密钥管理系统等一系列抗量子产品，格尔安全认证网关成为首家通过中国信息通信研究院抗量子技术验证的网关产品。通过持续的技术创新，公司已经构建了涵盖量子随机数生成、抗量子密码和量子密钥分发的全套产品体系，满足各行业用户的安全需求。

技术前瞻性+场景应用深度融合，抗量子迁移解决方案聚焦金融行业落地试点。

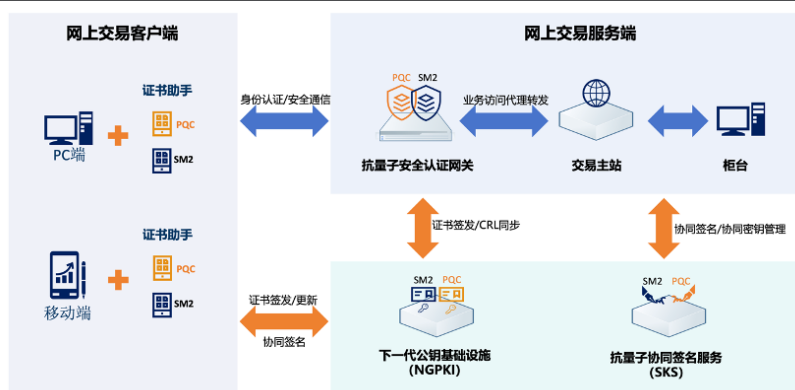
公司积极投身多项抗量子科研课题试点工作，已在银行、证券等行业的应用项目中立项，并成功通过相关权威机构验收。据格尔软件微信公众号，公司的抗量子解决方案为证券行业铸造量子安全时代的“数字护城河”，具备三大核心优势：

1) 算法兼容性突破：同步支持国际 FIPS 标准后量子算法 ML-KEM、ML-DSA、LSH-DSA、FN-DSA 及国内 AIGIS-SIG、CTRU/CNTR、LSS-SM3 等国密后量子算法。通过混合证书模式实现 SM2 算法与后量子密码的平滑过渡，既满足等保 2.0 合规要求，又构建量子安全防护层；

2) 迁移成本最优解：采用协同签名技术实现密钥生成、签名运算与证书管理的解耦设计，证券机构可在不改造或少改造现有业务系统的情况下，通过抗量子网关实现交易报文签名、投资者身份认证密钥等关键节点的量子安全升级；

3) 场景化防护体系：针对交易系统低延迟需求，方案可将签名时延控制在行业容忍阈值内；针对移动端身份认证场景，通过对称与非对称动态混合加密技术阻断量子中间人攻击；针对历史数据保护，创新采用“抗量子数字信封”技术，避免全量解密历史持仓数据、监管审计日志带来的数据暴露风险。

图17：证券抗量子迁移解决方案



资料来源：格尔软件微信公众号，民生证券研究院

2.7 国芯科技

聚焦于国产自主可控嵌入式 CPU 技术研发和产业化应用，推动量子技术 + 信创/信息安全芯片结合。作为中国国产嵌入式 CPU 的核心供应商，公司前瞻性

布局量子技术，通过与量子领域的知名企业开展量子技术合作，推动信创和信息安全芯片迭代升级。目前，公司已经与安徽问天量子科技股份有限公司、合肥硅臻芯片技术有限公司分别组建了量子芯片联合实验室，在物联网、云计算、先进存储、智能终端等领域，联合开展量子安全芯片的研发和产业化工作。公司多款产品已经被中电量子、问天量子等量子领域的头部企业实际采用和实现销售，成功应用于电力等关键领域中。

国芯科技于 5 月 6 日晚间发布公告，与参股公司郑州信大壹密科技有限公司合作研发的抗量子密码芯片 AHC001 于近日在公司内部测试中获得成功。该抗量子密码芯片的研发成功，实现了公司信息安全芯片产品的抗量子化提升，也进一步完善了公司信创与信息安全芯片产品的布局。

图18：国芯科技 CCUPHPQ01 抗量子密码卡



资料来源：财联社，民生证券研究院

3 投资建议

量子计算凭借指数级并行处理能力、全域协同特性与超低能耗优势，正从根本上颠覆传统计算架构，不仅成为破解 AI 算力瓶颈的颠覆性力量，也对传统密码体系的安全性构成严峻挑战。后量子密码技术旨在构建能够抵御量子计算机攻击的新型密码体系，成为保障未来信息安全的重要手段。当前，该技术的标准化进程加速推进，应用探索不断深入，国内外龙头企业亦纷纷加大布局力度，竞争态势日益凸显。建议关注天融信、电科网安、吉大正元、国盾量子、格尔软件、国芯科技等后量子密码技术标的，以及启明星辰、三未信安、科大国创、禾信仪器、神州信息、科华数据、中国长城、光迅科技、紫光国微、亨通光电等量子计算相关标的。

4 风险提示

1) 量子计算技术发展不及预期。当前量子计算技术仍处于起步阶段，技术路线较为复杂，无法判断量子计算的不同技术路线落地的确定性，若相关公司选择错误技术路线或面临产品竞争力下滑，进而对业绩产生不良影响。

2) 行业竞争加剧。量子计算或有较大蓝海市场，具备较强吸引力，若行业竞争加剧，或对相关公司利润率水平造成不良影响。

插图目录

图 1: 经典比特与量子比特对比.....	3
图 2: 量子计算与经典计算体系对比.....	4
图 3: 经典计算机与量子计算机运算能力对比.....	5
图 4: 量子计算产业生态与国内外代表性企业概况.....	6
图 5: 中国第三代自主超导量子计算机“本源悟空”.....	6
图 6: 全球量子计算发展历程.....	7
图 7: 全球量子计算产业规模（2021~2035）（单位：十亿美元）.....	8
图 8: 基于哈希函数的密钥生成.....	9
图 9: 美国 2021 版应对量子技术风险路线图.....	10
图 10: 量子安全产业发展周期.....	11
图 11: 全球量子安全产业生态图谱.....	12
图 12: 三未信安抗量子全系列密码产品.....	13
图 13: 芯片级后量子密码卡实物图.....	14
图 14: “量铠”抗量子密码全栈产品矩阵.....	15
图 15: 吉大正元元密一体机.....	16
图 16: 融合 QKD 和 PQC 的分布式密码体系.....	17
图 17: 证券抗量子迁移解决方案.....	18
图 18: 国芯科技 CCUPHPQ01 抗量子密码卡.....	19

表格目录

表 1: NIST 标准化后量子密码算法特性比较.....	10
-------------------------------	----

分析师承诺

本报告署名分析师具有中国证券业协会授予的证券投资咨询执业资格并登记为注册分析师，基于认真审慎的工作态度、专业严谨的研究方法与分析逻辑得出研究结论，独立、客观地出具本报告，并对本报告的内容和观点负责。本报告清晰准确地反映了研究人员的研究观点，结论不受任何第三方的授意、影响，研究人员不曾因、不因、也将不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

评级说明

投资建议评级标准	评级	说明
以报告发布日后的 12 个月内公司股价（或行业指数）相对同期基准指数的涨跌幅为基准。其中：A 股以沪深 300 指数为基准；新三板以三板成指或三板做市指数为基准；港股以恒生指数为基准；美股以纳斯达克综合指数或标普 500 指数为基准。	推荐	相对基准指数涨幅 15%以上
	谨慎推荐	相对基准指数涨幅 5% ~ 15%之间
	中性	相对基准指数涨幅-5% ~ 5%之间
	回避	相对基准指数跌幅 5%以上
公司评级	推荐	相对基准指数涨幅 5%以上
	中性	相对基准指数涨幅-5% ~ 5%之间
	回避	相对基准指数跌幅 5%以上
行业评级	推荐	相对基准指数涨幅 5%以上
	中性	相对基准指数涨幅-5% ~ 5%之间
	回避	相对基准指数跌幅 5%以上

免责声明

民生证券股份有限公司（以下简称“本公司”）具有中国证监会许可的证券投资咨询业务资格。

本公司境内客户使用。本公司不会因接收人收到本报告而视其为客户。本报告仅为参考之用，并不构成对客户的投资建议，不应被视为买卖任何证券、金融工具的要约或要约邀请。本报告所包含的观点及建议并未考虑获取本报告的机构及个人的具体投资目的、财务状况、特殊状况、目标或需要，客户应当充分考虑自身特定状况，进行独立评估，并应同时考量自身的投资目的、财务状况和特定需求，必要时就法律、商业、财务、税收等方面咨询专家的意见，不应单纯依靠本报告所载的内容而取代自身的独立判断。在任何情况下，本公司不对任何人因使用本报告中的任何内容而导致的任何可能的损失负任何责任。

本报告是基于已公开信息撰写，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、意见及预测仅反映本公司于发布本报告当日的判断，且预测方法及结果存在一定程度局限性。在不同时期，本公司可发出与本报告所刊载的意见、预测不一致的报告，但本公司没有义务和责任及时更新本报告所涉及的内容并通知客户。

在法律允许的情况下，本公司及其附属机构可能持有报告中提及的公司所发行证券的头寸并进行交易，也可能为这些公司提供或正在争取提供投资银行、财务顾问、咨询服务等相关服务，本公司的员工可能担任本报告所提及的公司的董事。客户应充分考虑可能存在的利益冲突，勿将本报告作为投资决策的唯一参考依据。

若本公司以外的金融机构发送本报告，则由该金融机构独自为此发送行为负责。该机构的客户应联系该机构以交易本报告提及的证券或要求获悉更详细的信息。本报告不构成本公司向发送本报告金融机构之客户提供的投资建议。本公司不会因任何机构或个人从其他机构获得本报告而将其视为本公司客户。

本报告的版权仅归本公司所有，未经书面许可，任何机构或个人不得以任何形式、任何目的进行翻版、转载、发表、篡改或引用。所有在本报告中使用的商标、服务标识及标记，除非另有说明，均为本公司的商标、服务标识及标记。本公司版权所有并保留一切权利。

民生证券研究院：

上海：上海市虹口区杨树浦路 188 号星立方大厦 7 层； 200082

北京：北京市东城区建国门内大街 28 号民生金融中心 A 座 18 层； 100005

深圳：深圳市福田区中心四路 1 号嘉里建设广场 1 座 10 层 01 室； 518048