

2026 年 09 月 30 日

中小盘研究团队

量子科技系列（四）：后量子时代将至，量子安全蓄势起航

——中小盘主题

周佳（分析师）

zhoujia@kysec.cn

证书编号：S0790523070004

● 后量子时代将至，量子安全重要性凸显

随着量子计算技术的迅猛发展，其潜在的密码破解能力将对现行公钥密码体系构成系统性威胁，由此催生了对量子安全的需求。具体而言，大规模可容错通用量子计算机运行 Shor 算法，可高效破解基于大数分解和离散对数问题的 RSA、ECC 等公钥密码核心算法，不仅会危及数字空间身份与行为信息真实性、敏感数据传输的机密性与完整性，更会对需长期保密的信息形成“先截获，后破解”的追溯性风险。因此，随着后量子时代将近，量子安全愈发受到重视。据麦肯锡数据，2023 年量子通信市场（涵盖安全与网络，安全占较大比例）总规模为 9 亿至 10 亿美元，预计到 2035 年将达到 105 亿至 149 亿美元，复合年增长率为 23-25%。

● 量子安全的主要方案包括量子保密通信与抗量子加密

基于量子密钥分发（QKD）等物理学方案实现量子保密通信，以及基于格加密、纠错编码等新型数学难题，构建抗量子计算破解的新型公钥密码，即抗量子加密（PQC），是应对量子计算破解公钥密码安全威胁的两种主要方案。其中，量子保密通信的代表性技术方向 QKD 是一种通信双方通过传输量子态来建立密钥的协议，其目的是使通信双方获得一串只有他们两个知道的由经典随机比特构成但用量子方式建立的量子密钥，其在理论协议层面具备信息论安全性。PQC 则是指在量子计算机时代仍能保持安全的新型密码学技术，旨在设计和实现能够在面对量子计算机攻击时仍然有效的加密算法。这些算法通常基于数学问题，而这些问题在经典计算机和量子计算机上都难以解决，从而确保了即使在量子计算机普及的情况下，数据的安全性也能得到保障。

● QKD 与 PQC 各有优劣，二者将长期并行发展

目前，QKD 与 PQC 在安全性、部署复杂度、应用场景等方面存在显著差异，各有优劣，二者均将长期作为应对量子计算威胁的重要技术。首先，在安全性方面，QKD 基于量子力学原理，即量子态的不可克隆性和测量的扰动特性，在物理层面保证了理论上“无条件安全”，任何窃听都会被发现。不过，QKD 缺乏对 QKD 传输源的身份认证机制，无法提供完整通信安全，且用于实施 QKD 的具体硬件本身可能引入漏洞。PQC 可提供认证、加密功能，但其安全性是“计算安全性”，如果作为技术基础的复杂数学问题被破解，安全性就无法保证。部署复杂度方面，QKD 需要专用的量子信道和设备，部署成本较高。而 PQC 的大多数实现仅需软件即可完成，能基于现有网络架构进行迁移和部署，成本较低。应用场景方面，QKD 适合政府、金融等高安全性需求场景；PQC 广泛的通用性使其更适配互联网、物联网、工业控制等场景。

● **风险提示：**技术研发与迭代不及预期、产业落地进度不及预期、下游应用场景需求不及预期。

相关研究报告

《量子科技系列报告（三）：量超融合加速落地，开启下一代算力周期——中小盘主题》-2026.9.25

《碳市场专题：2026 年 CCER 供需缺口进一步扩大——中小盘策略专题》-2026.9.21

《国内检验检测优质公司，外延并购打开增长空间——中小盘首次覆盖报告》-2026.9.17

特别声明

《证券期货投资者适当性管理办法》、《证券经营机构投资者适当性管理实施指引（试行）》已正式实施。根据上述规定，开源证券评定此研报的风险等级为R3（中风险），因此通过公共平台推送的研报其适用的投资者类别仅限定为专业投资者及风险承受能力为C3、C4、C5的普通投资者。若您并非专业投资者及风险承受能力为C3、C4、C5的普通投资者，请取消阅读，请勿收藏、接收或使用本研报中的任何信息。因此受限于访问权限的设置，若给您造成不便，烦请见谅！感谢您给予的理解与配合。

分析师声明

本研究报告的署名人员具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，以勤勉的职业态度，独立、客观地出具本报告，并对内容和观点负责。本报告清晰准确地反映了署名人员的研究观点，所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。本报告署名人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中具体的推荐意见或观点有直接或间接的联系。

股票投资评级说明

	评级	说明
证券评级	买入（Buy）	预计相对强于市场表现 20%以上；
	增持（Outperform）	预计相对强于市场表现 5%~20%；
	中性（Neutral）	预计相对市场表现在-5%~+5%之间波动；
	减持（Underperform）	预计相对弱于市场表现 5%以下。
行业评级	看好（Overweight）	预计行业超越整体市场表现；
	中性（Neutral）	预计行业与整体市场表现基本持平；
	看淡（Underperform）	预计行业弱于整体市场表现。

备注：评级标准为以报告日后的 6~12 个月内，证券相对于市场基准指数的涨跌幅表现，其中 A 股基准指数为沪深 300 指数（北交所基准指数为北证 50 指数）、港股基准指数为恒生指数、新三板基准指数为三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）、美股基准指数为标普 500 或纳斯达克综合指数。我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。

法律声明

开源证券股份有限公司是经中国证监会批准设立的证券经营机构，已具备证券投资咨询业务资格。

本报告仅供开源证券股份有限公司（以下简称“本公司”）的客户使用。本公司不会因接收人收到本报告而视其为客户。本报告是发送给开源证券客户的，属于商业秘密材料，只有开源证券客户才能参考或使用。

本报告是基于本公司认为可靠的已公开信息，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、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他金融工具的邀请或向人做出邀请。本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可能会波动，过往的业绩表现不应作为其日后表现的预示。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。客户应当考虑到本公司可能存在可能影响本报告客观性的利益冲突，不应视本报告为做出投资决策的唯一因素。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。本公司未确保本报告充分考虑到个别客户特殊的投资目标、财务状况或需要。本公司建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议。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所引致的任何损失负任何责任。若本报告的接收人非本公司的客户，应在基于本报告做出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。投资者应自主作出投资决策并自行承担投资风险，任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。

开源证券在法律允许的情况下可参与、投资或持有本报告涉及的证券或进行证券交易，或向本报告涉及的公司提供或争取提供包括投资银行业务在内的服务或业务支持。开源证券可能与本报告涉及的公司之间存在业务关系，并无需事先或在获得业务关系后通知客户。

本报告的版权归本公司所有。本公司对本报告保留一切权利。未经本公司事先书面授权，本报告的任何部分均不得以任何方式制作任何形式的拷贝、复印件或复制品，或再次分发给任何其他人，或以任何侵犯本公司版权的其他方式使用。所有本报告中使用的商标、服务标记及标记均为本公司的商标、服务标记及标记。

开源证券研究所

上海

地址：上海市浦东新区世纪大道1788号陆家嘴金控广场1号楼3层
邮编：200120
邮箱：research@kysec.cn

深圳

地址：深圳市福田区金田路2030号卓越世纪中心1号楼45层
邮编：518000
邮箱：research@kysec.cn

北京

地址：北京市西城区西直门外大街18号金贸大厦C2座9层
邮编：100044
邮箱：research@kysec.cn

西安

地址：西安市高新区锦业路1号都市之门B座5层
邮编：710065
邮箱：research@kysec.cn