

计算机

信安世纪：金融量子密码的领军者

1、中美量子科技竞赛，传统密码技术受到巨大安全性挑战

2023年12月，IBM推出了第一台拥有1000多个量子位的量子计算机，相当于普通计算机中的数字位。2024年4月4日，量子计算公司Quantinuum与科技巨头微软宣布，在实现容错量子计算方面取得重大突破。从国内来看，2016年中国在“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年中国提出了新的“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。信安世纪表示，随着量子计算的不断突破，现阶段部署的一些经典密码算法（特别是公钥密码算法）将受到巨大的安全性挑战，进而影响国家安全和社会公共利益。我们认为，金融行业作为国民经济重要领域，或率先迁移替换为PQC算法密码。

2、美国2023年加速PQC算法标准草案，中国后量子密码试点在即

根据中国科学院网站消息，2023年8月24日，美国NIST正式公布三种后量子密码（PQC）算法标准草案，并表示其将于2024年投入使用，第四种算法的标准草案也将在2024年向公众发布。信安世纪官网显示，2023年11月，中国信通院CPII“密码+应用推进计划”联合产业各方编制并发布《后量子密码应用研究报告（2023年）》，公司受邀参与了报告编制工作。根据信安世纪公众号，2023年12月美国国家标准与技术研究所（NIST）发布了《量子准备：密码发现》和《量子准备：测试互操作性和性能标准草案》两份出版物草案。我们认为，为应对美国的量子计算发展带来的安全性挑战，国内后量子密码研发及试点或将加速，以替代经典密码算法。

3、信安世纪前瞻布局后量子密码，推进算法研究、迁移、行业融合工作

公司作为商密领军企业，积极推进后量子密码算法研究、迁移及行业融合工作。1)在后量子算法研究，公司已成功将NIST公布的KYBER、DILITHI-UM、SPHINCS+、FALCON四种后量子算法融入公司数字认证、签名服务器、应用安全网关等安全产品当中，为各行业面对未来的后量子攻击风险提供安全保障；2)后量子算法迁移领域，针对不同场景、不同应用系统、存量算法、性能影响等方面，综合设计后量子密码的迁移规划及落地实践，助力各行业从传统密码体系平滑过渡到后量子密码体系；3)后量子算法行业融合领域，公司已与多家机构建立后量子密码联合实验室，搭建后量子密码运行测试环境，共同开展后量子密码实验课题的研究。

风险提示：量子计算研发进展不及预期、后量子密码应用落地不及预期、技术发展不及预期

证券研究报告

2024年04月08日

投资评级

行业评级

强于大市(维持评级)

上次评级

强于大市

作者

缪欣君

分析师

SAC执业证书编号：S1110517080003

miaoxinjun@tfzq.com

行业走势图

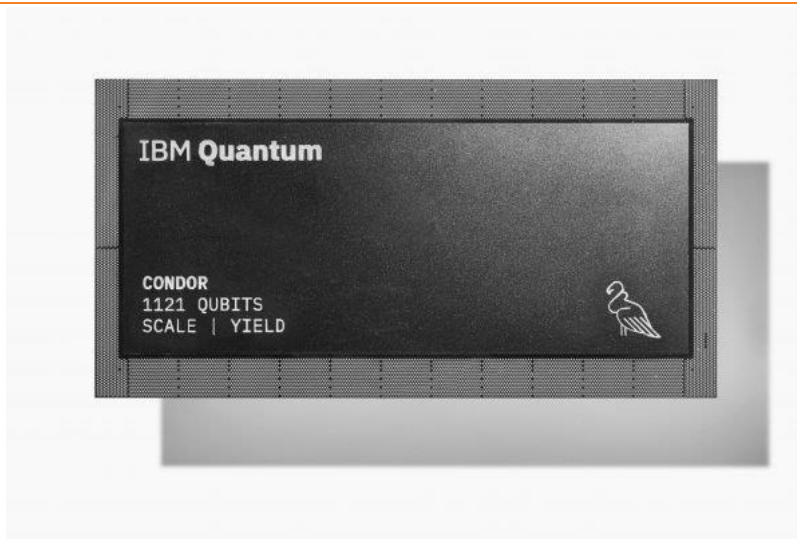


资料来源：聚源数据

相关报告

- 《计算机-行业点评:央企引领新质生产力，聚焦三大主线》2024-03-31
- 《计算机-行业点评:Kimi：出海或加速，产品力提升有望带来用户快速增长》2024-03-29
- 《计算机-行业点评:顶层文件发布，低空经济建设进入快车道》2024-03-28

图 1：拥有 1121 个超导量子位的 Condor 处理器



资料来源：EDN China、天风证券研究所

图 2：NIST 发布《量子准备：密码发现》和《量子准备：测试互操作性和性能标准草案》出版物草案



资料来源：信安世纪公众号、天风证券研究所

图 3：信安世纪前瞻布局后量子密码



资料来源：信安世纪公众号、天风证券研究所

分析师声明

本报告署名分析师在此声明：我们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，本报告所表述的所有观点均准确地反映了我们对标的证券和发行人的个人看法。我们所得报酬的任何部分不曾与，不与，也将不会与本报告中的具体投资建议或观点有直接或间接联系。

一般声明

除非另有规定，本报告中的所有材料版权均属天风证券股份有限公司（已获中国证监会许可的证券投资咨询业务资格）及其附属机构（以下统称“天风证券”）。未经天风证券事先书面授权，不得以任何方式修改、发送或者复制本报告及其所包含的材料、内容。所有本报告中使用的商标、服务标识及标记均为天风证券的商标、服务标识及标记。

本报告是机密的，仅供我们的客户使用，天风证券不因收件人收到本报告而视其为天风证券的客户。本报告中的信息均来源于我们认为可靠的已公开资料，但天风证券对这些信息的准确性及完整性不作任何保证。本报告中的信息、意见等均仅供客户参考，不构成所述证券买卖的出价或征价邀请或要约。该等信息、意见并未考虑到获取本报告人员的具体投资目的、财务状况以及特定需求，在任何时候均不构成对任何人的个人推荐。客户应当对本报告中的信息和意见进行独立评估，并应同时考量各自的投资目的、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。对依据或者使用本报告所造成的一切后果，天风证券及/或其关联人员均不承担任何法律责任。

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，天风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。天风证券的销售人员、交易人员以及其他专业人士可能会依据不同假设和标准、采用不同的分析方法而口头或书面发表与本报告意见及建议不一致的市场评论和/或交易观点。天风证券没有将此意见及建议向报告所有接收者进行更新的义务。天风证券的资产管理部门、自营部门以及其他投资业务部门可能独立做出与本报告中的意见或建议不一致的投资决策。

特别声明

在法律许可的情况下，天风证券可能会持有本报告中提及公司所发行的证券并进行交易，也可能为这些公司提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。因此，投资者应当考虑到天风证券及/或其相关人员可能存在影响本报告观点客观性的潜在利益冲突，投资者请勿将本报告视为投资或其他决定的唯一参考依据。

投资评级声明

类别	说明	评级	体系
股票投资评级	自报告日后的 6 个月内，相对同期沪深 300 指数的涨跌幅	买入	预期股价相对收益 20%以上
		增持	预期股价相对收益 10%-20%
		持有	预期股价相对收益 -10%-10%
		卖出	预期股价相对收益 -10%以下
行业投资评级	自报告日后的 6 个月内，相对同期沪深 300 指数的涨跌幅	强于大市	预期行业指数涨幅 5%以上
		中性	预期行业指数涨幅 -5%-5%
		弱于大市	预期行业指数涨幅 -5%以下

天风证券研究

北京	海口	上海	深圳
北京市西城区德胜国际中心 B 座 11 层	海南省海口市美兰区国兴大道 3 号互联网金融大厦 A 栋 23 层 2301 房	上海市虹口区北外滩国际客运中心 6 号楼 4 层	深圳市福田区益田路 5033 号平安金融中心 71 楼
邮编：100088	邮编：570102	邮编：200086	邮编：518000
邮箱：research@tfzq.com	电话：(0898)-65365390 邮箱：research@tfzq.com	电话：(8621)-65055515 传真：(8621)-61069806 邮箱：research@tfzq.com	电话：(86755)-23915663 传真：(86755)-82571995 邮箱：research@tfzq.com