国投证券 SDIC SECURITIES

2024 年 08 月 19 日
计算机

行业周报

证券研究报告

NIST 发布全球首个抗量子密码算法标准

投资评级 领先大市-A
维持评级

首选股票	目标价（元）	评级

行业表现

资料来源：Wind 资讯

升幅%	1M	3M	12M
相对收益	-1.2	-6.7	-22.3
绝对收益	-5.6	-14.8	-34.7

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

相关报告

把握产业发展趋势，关注自主可控三大方向	2024-08-12
海外科技巨头迎来财报披露密集期，加码 AI 仍是一致方向	2024-08-05
卫星互联网与商业航天迎来新一轮投资机会	2024-07-29
DRG/DIP 付费 2.0 版出台，医保支付改革提速	2024-07-23
24Q2 板块持仓复盘及三中全会《决定》解读	2024-07-22

NIST 发布抗量子密码算法标准，量子科技产业再进一步

8 月 13 日，美国商务部国家标准与技术研究院（NIST）正式发布了抗量子密码学联邦信息处理标准。这一里程碑事件不仅标志着密码学领域的新突破，也为未来量子计算带来的安全威胁提供了应对之道。

新标准包含三种算法：1）FIPS 203：基于 Kyber 算法的标准，旨在用于传输层安全协议。尽管该算法生成的公钥和密文较大，但其快速性能使其成为传统方法的有效替代品。2）FIPS 204：基于 Dilithium 算法，专为数字签名设计。该标准在验证速度方面表现优越，适用于需要更大签名和公钥的应用场景。3）FIPS 205：基于 SHA-2 或 SHA-3 的安全性，提供了 32 字节的小公钥和约 7KB 的大签名，适用于需要快速验证的固件更新等应用。

应对量子计算攻击，抗量子密码改造蓄势待发

量子计算的发展对密码学带来了巨大威胁。1994 年 Shor 提出的量子算法，可以在多项式时间内快速分解大整数以及求解离散对数，理论上 Shor 算法可以彻底破解当前广泛应用的 RSA 和椭圆曲线公钥密码算法，因它们的安全基础分别为大整数分解和椭圆曲线离散对数问题。1996 年 Grover 提出的量子算法，对无序集中的搜索复杂度有开平方量级的降低，理论上也可以使对称密码算法的安全强度减半。

抗量子密码技术成为重要应对措施。“后量子密码”或“抗量子密码”，是指能够抵御量子计算机攻击的新型密码算法，是量子信息时代维护网络安全的关键技术。当前全球各个国家都在通过政策和标准的形式，推动抗量子密码的算法演进和产业布局。

从迁移进度来看，2023 年 8 月，美国网络安全和基础设施安全局（CISA）、国家安全局（NSA）与国家标准与技术研究院（NIST）联合发布《量子准备：向后量子密码迁移》指南，此前 NSA 发布了《商业国家安全算法（CNSA）2.0》，提出美国政府将在 2033 年之前完成其信息系统中的后量子迁移。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。

抗量子密码算法标准发布，关注产业跟进和密码替换机会。我们认为此次 NIST 发布全球首个抗量子密码算法标准，后续有望获得包括美国政府以及全球科技巨头的持续跟进，从美国迁移进度来看，后续含有加密和数字证书的信息系统均有望向抗量子密码迁移，有望带来密码产业的新机遇。关注格尔软件、信安世纪、吉大正元、三未信安、电科网安、中孚信息等密码企业。

风险提示：1）技术创新不及预期；2）政策支持力度不及预期。

内容目录

1. 本周行业观点 3
2. 市场行情回顾 4
2.1. 本周板块指数涨跌幅 4
2.2. 本周计算机个股表现 5
3. 重要行业新闻 6
3.1. 数字经济 6
3.2. 新兴技术与硬科技 6
3.3. 低空经济 6
3.4. 医疗信息化 6
4. 重点公司动态 7
4.1. 基础软硬件 7
4.2. 工业软件 7
4.3. 网络安全 7
4.4. AI 大数据应用 7
4.5. 智能网联车 8

图表目录

图 1. 本周各行业涨跌幅统计 4

表 1： 本周板块指数涨跌幅统计 4
表 2： 本周计算机个股涨跌幅统计 5

1. 本周行业观点

NIST 发布抗量子密码算法标准，量子科技产业再进一步

8 月 13 日，美国商务部国家标准与技术研究院（NIST）正式发布了抗量子密码学联邦信息处理标准。这一里程碑事件不仅标志着密码学领域的新突破，也为未来量子计算带来的安全威胁提供了应对之道。

新标准包含三种算法：1）FIPS 203：基于 Kyber 算法的标准，旨在用于传输层安全协议。尽管该算法生成的公钥和密文较大，但其快速性能使其成为传统方法的有效替代品。2）FIPS 204：基于 Dilithium 算法，专为数字签名设计。该标准在验证速度方面表现优越，适用于需要更大签名和公钥的应用场景。3）FIPS 205：基于 SHA-2 或 SHA-3 的安全性，提供了 32 字节的小公钥和约 7KB 的大签名，适用于需要快速验证的固件更新等应用。

应对量子计算攻击，抗量子密码改造蓄势待发

量子计算的发展对密码学带来了巨大威胁。1994 年 Shor 提出的量子算法，可以在多项式时间内快速分解大整数以及求解离散对数,理论上 Shor 算法可以彻底破解当前广泛应用的 RSA 和椭圆曲线公钥密码算法，因它们的安全基础分别为大整数分解和椭圆曲线离散对数问题。1996 年 Grover 提出的量子算法，对无序集中的搜索复杂度有开平方量级的降低，理论上也可以使对称密码算法的安全强度减半。

抗量子密码技术成为重要应对措施。“后量子密码”或“抗量子密码”，是指能够抵御量子计算机攻击的新型密码算法，是量子信息时代维护网络安全的关键技术。当前全球各个国家都在通过政策和标准的形式，推动抗量子密码的算法演进和产业布局。

从迁移进度来看，2023 年 8 月，美国网络安全和基础设施安全局（CISA）、国家安全局（NSA）与国家标准与技术研究院（NIST）联合发布《量子准备：向后量子密码迁移》指南，此前 NSA 发布了《商业国家安全算法（CNSA）2.0》，提出美国政府将在 2033 年之前完成其信息系统中的后量子迁移。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。

抗量子密码算法标准发布，关注产业跟进和密码替换机会。我们认为此次 NIST 发布全球首个抗量子密码算法标准，后续有望获得包括美国政府以及全球科技巨头的持续跟进，从美国迁移进度来看，后续含有加密和数字证书的信息系统均有望向抗量子密码迁移，有望带来密码产业的新机遇。关注格尔软件、信安世纪、吉大正元、三未信安、电科网安、中孚信息等密码企业。

2. 市场行情回顾

2.1. 本周板块指数涨跌幅

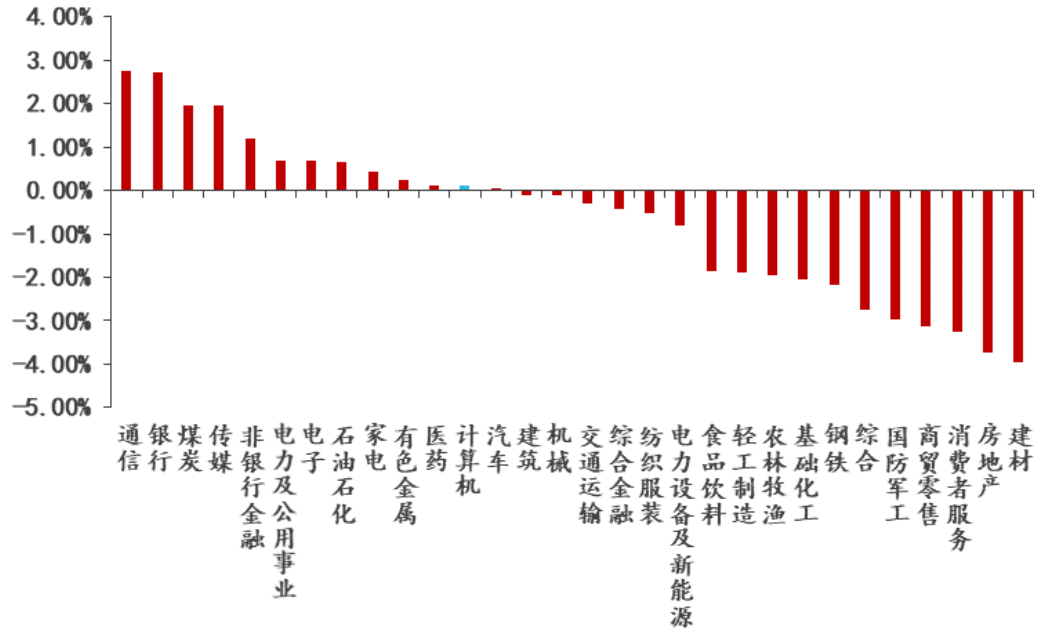
本周深证成指下跌 0.52%，创业板指下跌 0.26%，计算机行业上涨 0.11%，跑赢深证成指 0.63%，跑赢创业板指 0.37%。横向来看，本周计算机行业指数在中信 30 个行业指数中排名第 12，在 TMT 四大行业（电子、通信、计算机、传媒）中排名第 4。

表1：本周板块指数涨跌幅统计

指数名称	周涨跌幅%	年初至今涨跌幅%	周相对涨跌幅	年初至今相对涨跌幅
计算机（中信）	0.11%	-28.01%	——	——
上证综指	0.60%	-3.21%	-0.49%	-24.80%
深证成指	-0.52%	-12.33%	0.63%	-15.68%
创业板指	-0.26%	-15.86%	0.37%	-12.15%
沪深 300	0.42%	-2.49%	-0.31%	-25.52%
云计算指数	0.31%	-29.03%	-0.20%	1.02%
网络安全指数	-0.34%	-32.24%	0.45%	4.23%
车联网指数	0.99%	-16.07%	-0.88%	-11.94%

资料来源：Wind，国投证券研究中心

图1. 本周各行业涨跌幅统计



资料来源：Wind，国投证券研究中心

2.2. 本周计算机个股表现

从涨跌幅情况来看，本周计算机板块整体表现一般。展望 2024 年，我们仍建议关注景气度向上的人工智能、低空经济、智能网联车和信创等产业的投资机会。

表2：本周计算机个股涨跌幅统计

周涨幅前十		周跌幅前十		周换手率前十	
股票名称	周涨跌幅（%）	股票名称	周涨跌幅（%）	股票名称	周换手率（%）
优博讯	18.31%	任子行	-24.43%	启明信息	108.23%
安博通	17.46%	威创股份	-22.41%	天迈科技	63.47%
雷柏科技	16.67%	汇金股份	-10.80%	金溢科技	60.16%
GQY 视讯	16.07%	彩讯股份	-10.50%	京天利	53.83%
朗科科技	15.95%	航天宏图	-9.77%	天利科技	53.83%
博睿数据	12.09%	金溢科技	-9.59%	GQY 视讯	49.74%
世纪瑞尔	11.58%	吉大正元	-9.00%	四维图新	43.54%
东方中科	10.96%	易联众	-8.78%	浩云科技	43.00%
卓易信息	10.55%	航天长峰	-7.88%	万集科技	42.26%
丝路视觉	10.34%	银江股份	-7.83%	思创医惠	40.76%

资料来源：Wind，国投证券研究中心

3. 重要行业新闻

3.1. 数字经济

2024 年，国务院国资委开展了“AI+专项行动”，通过人工智能技术推动产业焕新。该行动要求中央企业深化 AI 技术的应用，特别是在重点行业，以及构建多模态优质数据集，并打造大模型赋能产业生态。为响应国务院国资委“AI+专项行动”，中国企业联合会、中国经济改革研究基金会牵头《人工智能 数据资产流通管理指南》团体标准立项，中国资产评估协会等专业机构和多家央企作为重要参编单位。首部“AI+数据资产”交叉领域标准，将为央国企“AI+”场景牵引赋能千行百业，提供数据资产流通管理指引。数据要素社联合中国企业联合会、中国经济改革研究基金会，将持续举办“AI+数据资产”专家工作坊，推动标准编制，服务央国企 AI 应用场景创新。（来源：数据要素社）

3.2. 新兴技术与硬科技

8 月 14 日，为加强新能源汽车废旧动力电池综合利用行业管理，推动行业高质量发展，工信部修订形成了《新能源汽车废旧动力电池综合利用行业规范条件(2024 年本)》，现向社会公开征求意见。《条件》对企业布局与项目选址、厂区条件、设施设备、技术工艺、溯源能力、资源利用、能源消耗、产品质量、环境保护等进行了要求。另外，上述规范对梯次利用企业和再生利用企业均进行了不同要求。比如，梯次利用企业的年梯次利用的废旧动力电池量，应不低于实际废旧动力电池回收量的 60%（其中利用量和回收量均按重量计算）；自建或与用户共建梯次产品在线监测平台，监测产品运行状态和流向。（来源：semi 产业网）

3.3. 低空经济

8 月 12 日，湖北省政府召开了低空经济发展推进会。会议强调，要深入贯彻落实党的二十届三中全会精神和习近平总书记关于低空经济发展的重要论述，加快打造具有全国影响力的低空经济发展高地。湖北省省长王忠林指出，低空经济是国家战略性新兴产业，是湖北省的重要新增长点。会议提出，要以设施建设、研发制造、拓展应用为核心，完善低空经济的基础设施和全产业链，推动低空经济融入各行各业。近日，湖北省发改委还发布了《湖北省加快低空经济高质量发展行动方案（2024—2027 年）》，提出到 2027 年全省低空经济产业规模要突破 1000 亿元，建成 30 个以上通用机场，并全面推进相关配套设施和应用场景的建设。（来源：湖北省政府网）

苏州市交通运输局于 8 月 12 日发布公告，就《苏州市低空经济产业发展促进条例（征求意见稿）》公开征求意见，时间为 2024 年 8 月 12 日至 9 月 11 日。《条例》共 7 章三十九条，涵盖低空经济产业的发展、基础设施建设、科技创新、应用场景推广、安全保障等方面内容，旨在推动苏州市低空经济高质量发展。《条例》明确了各方职责和体制机制，重点关注政策扶持、企业培育、基础设施规划、科技创新和安全保障等关键领域，强调低空产业发展必须坚持安全第一的原则。（来源：苏州市政府网）

3.4. 医疗信息化

8 月 10 日，国家卫生健康委办公厅、国家医保局办公室发布《关于印发长期处方管理规范（试行）的通知》。《规范》明确了长期处方的适用对象、开具长期处方的医疗机构等实施主体以及开具的主要流程等，根据患者诊疗需要，长期处方的处方量一般在 4 周内；根据慢性病特点，病情稳定的患者适当延长，最长不超过 12 周。《通知》从多角度提出要加强互联网技术在长处方管理规范中的应用，比如基层卫生医疗机构可通过互联网复诊等途径在医联体内具备条件的上级医疗机构指导下开具、互联网医院提供长期处方服务等。（来源：国家卫生健康委）

4. 重点公司动态

4.1. 基础软硬件

【中科曙光】业绩快报：上半年公司预计实现营业总收入 57.12 亿元，同比增长 5.77%；归属于上市公司股东净利润 5.58 亿元，同比增长 2.43%；归属于上市公司股东的扣除非经常性损益的净利润 3.54 亿元，同比增长 15.93%。（来源：同花顺）

【海光信息】半年报：公司实现营业总收入 37.63 亿元，同比增长 44.08%；归属于上市公司股东净利润 8.53 亿元，同比增长 25.97%；归属于上市公司股东的扣除非经常性损益的净利润 8.18 亿元，同比增长 32.09%。（来源：同花顺）

【工业富联】半年报：上半年公司实现营业收入 2660.91 亿元，同比增长 28.69%；归母净利润盈利 87.39 亿元，同比增长 22.04%；扣非归母净利润盈利 85.33 亿元，同比增长 13.23%。（来源：同花顺）

4.2. 工业软件

【中望软件】半年报：上半年公司实现营业收入 3.08 亿元，同比增长 11.79%；归母净利润盈利 597.62 万元，扭亏为盈；扣非归母净利润亏损 8396.78 万元。（来源：同花顺）

【北路智控】半年报：本报告期营业收入 4.97 亿元，同比上涨 17.14%，归属于上市公司股东的净利润 8314.93 万元，同比下降 16.81%；扣非归母净利润为 6895.49 万元，同比下降 25.84%。（来源：同花顺）

【龙软科技】半年报：上半年，公司实现营业总收入 1.40 亿元，同比增长 0.86%；归属于上市公司股东净利润 0.36 亿元，同比减少 6.90%，归属于上市公司股东的扣除非经常性损益的净利润 0.35 亿元，同比减少 6.16%。（来源：同花顺）

【普联软件】半年报：上半年，公司实现营业总收入 1.92 亿元，同比增长 25.93%；归母净利润 1339.1 万元，同比增长 142.17%；扣非归母净利润 790.23 万元，同比增长 121.4%。（来源：同花顺）

4.3. 网络安全

【山石网科】股权激励：公司同意本激励计划的授予日为 2024 年 8 月 13 日，并同意以 8.59 元/股的授予价格向符合条件的 159 名激励对象授予 992.00 万股限制性股票。（来源：同花顺）

【天融信】半年报：公司实现营业总收入 8.73 亿元，同比下降 13.07%；归属于上市公司股东净利润-2.06 亿元，归属于上市公司股东的扣除非经常性损益的净利润-2.16 亿元。（来源：同花顺）

4.4. AI 大数据应用

【海天瑞声】首次回购股份：2024 年 8 月 13 日，公司通过上海证券交易所交易系统以集中竞价交易方式首次回购股份 19,824 股，占公司总股本 6032.52 万股的比例为 0.0329%，回购成交的最高价为 43.50 元/股，最低价为 43.10 元/股，支付的资金总额为人民币 85.87 万元（不含交易费用）。（来源：同花顺）

【万兴科技】半年报：上半年，公司实现营业总收入 7.05 亿元，同比下降 1.80%；归属于上市公司股东净利润 0.24 亿元，同比下降 43.99%，归属于上市公司股东的扣除非经常性损益的净利润 1.57 亿元，同比下降 54.58%。（来源：同花顺）

【海康威视】半年报：上半年，公司实现营业收入 412.09 亿元，同北增长 9.68%；归母净利润盈利 50.64 亿元，同比下降 5.13%；扣非归母净利润盈利 52.43 亿元，同比增长 4.11%。（来源：同花顺）

4.5. 智能网联车

【光庭信息】半年报：公司实现营业总收入 2.17 亿元，同比减少 20.06%；归属于上市公司股东净利润亏损 1339.28 万元；归属于上市公司股东的扣除非经常性损益的净利润亏损 1790.82 万元。（来源：同花顺）

【万集科技】半年报：上半年，公司实现营业总收入 3.78 亿元，同比增长 17.28%；归母净利润亏损 1.5 亿元，扣非归母净利润亏损 1.58 亿元。（来源：同花顺）

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：深圳市福田区福田街道福华一路 119 号安信金融大厦 33 楼
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