证券研究报告

行业报告：行业深度研究

2024年04月29日

计算机

量子加密，一片新蓝海

作者：

分析师 缪欣君 SAC执业证书编号：S1110517080003

天风证券 TF SECURITIES

行业评级：强于大市（维持评级）

上次评级：强于大市

核心观点

1、量子科技竞赛加速，经典密码有必要考虑向PQC迁移（量子软加密）：2023年12月IBM 推出1000 多个量子位的量子计算机。2024年4月初，微软也跟量子计算合作，在容错方面取得了较大突破。当前密码大量应用于国家保密系统和大型国防装备，一旦量子计算机问世，现代密码学或会被直接攻破，威胁到党政军民领域的网络信息安全。

2、QKD硬加密适用特定场景，PQC（量子软加密）有望实现广泛覆盖：QKD量子密钥分发是一种密钥的安全传输方式，基于物理原理，需要专用的物理设备，可以在两个相距遥远的通信端之间进行密钥的发送；PQC是能够抵抗量子计算对现有密码算法攻击的新一代密码算法，研究密码算法在量子环境下的安全性，并设计在经典和量子环境下均具有安全性的密码系统。

3、美国PQC（量子软加密）加速标准2024年已建立，要求2023年前完成密码体系迁移：美国NIST去年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年批准，第四种算法的标准草案也将在2024年向公众发布，且NIST要求2024~2030年必须升级到PQC算法。此外，欧洲及日韩在PQC迁移及标准建立均有相关的研究与进展，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。**从替换节奏看，金融行业尤其是银行作为国民经济重要领域**，涉及大量的核心数据和交易信息，相比于其他行业有望更早地采取相应的措施过渡到后量子密码体系。

4、替换加速，预计2029年市场规模约700亿元。参考美国替换进度，中国过去数年投入的密码产品可能在未来五年重新替换为PQC量子加密产品。根据Inside Quantum Technology测算，预计到2029年后量子密码软件和芯片市场规模将达到95亿美元，约合人民币689亿元（截至2024年4月21日汇率）。

5、量子产业或成为全球科技竞赛的下一站，建议关注三大方向：量子安全、量子计算、量子测量。建议关注：

1）量子加密：信安世纪、国盾量子、神州信息、格尔软件、三未信安、天融信、吉大正元

2）量子计算：国盾量子、普源精电、科华数据（通信&电新联合覆盖）、腾景科技

3）量子测量：科大国创、天奥电子

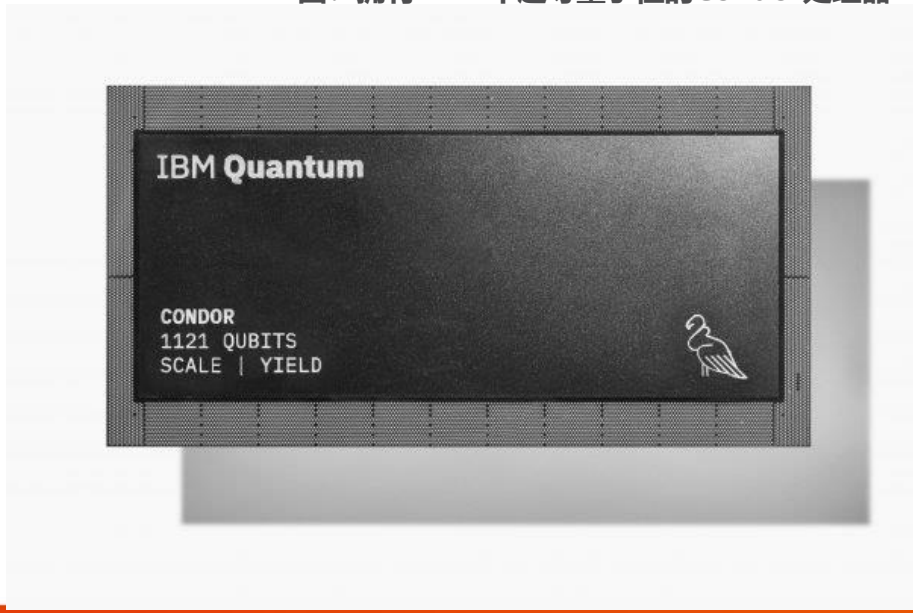
风险提示：政策落地不及预期、量子计算研发进展不及预期、后量子密码应用落地不及预期

1、量子科技竞赛加速，经典密码体系有必要向PQC迁移

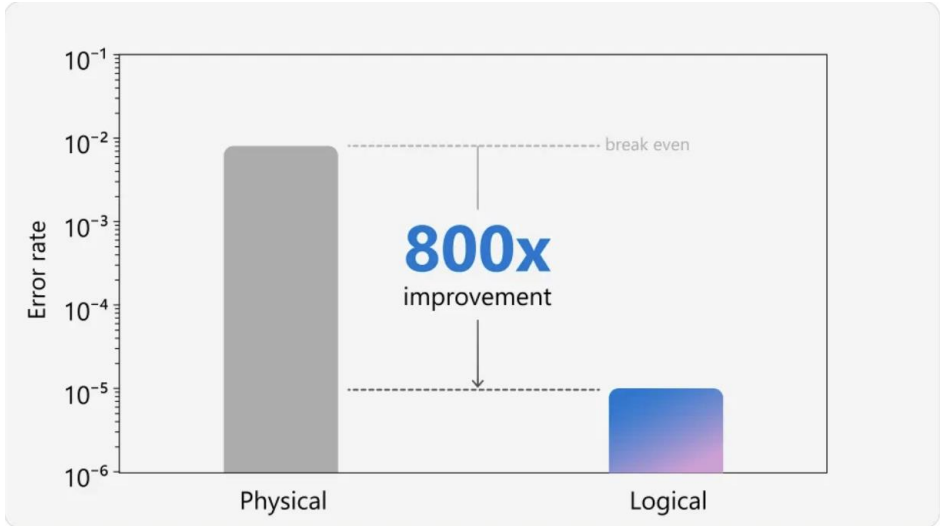
量子科技竞赛加速，经典密码体系有必要考虑向PQC迁移（后量子密码，又称抗量子密码）：

- **美国量子计算不断突破，NIST要求2030前必须升级到PQC算法**：2023年12月IBM 推出1000 多个量子位的量子计算机。2024年4月初，微软也跟量子计算合作，在容错方面取得了较大突破。此外，NIST要求2024~2030年必须升级到PQC算法。
- **经典密码体系有必要考虑向量子密码解决方案迁移：**当前密码大量应用于国家保密系统和大型国防装备，一旦量子计算机问世，现代密码学基于大整数分解、离散对数问题设计的公钥密码或会被直接攻破，威胁到党政军民领域的网络信息安全。

图：拥有1121个超导量子位的Condor处理器



图：微软与量子公司合作，量子计算可靠性提升800倍

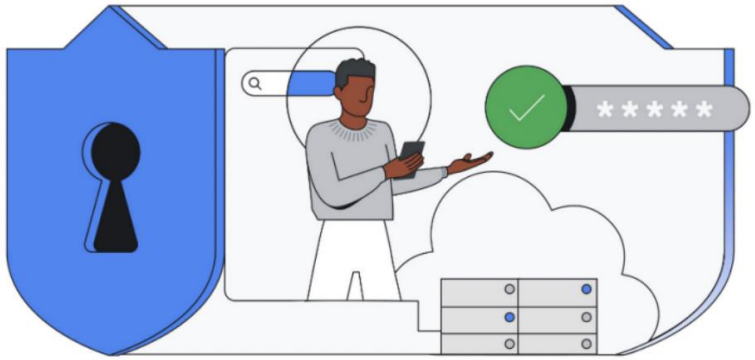


来源：电子技术设计、微软加速器公众号、天风证券研究所

2、密码体系或迎全面变革，预计2029年约700亿市场规模

- **参考美国替换进度，中国过去数年投入的密码产品可能在未来五年重新替换为PQC量子加密产品。**根据Inside Quantum Technology测算，预计到2029年后量子密码软件和芯片市场规模将达到95亿美元，**约合人民币689亿元（截至2024年4月21日汇率）。**
- **IBM、微软和谷歌等国际ICT巨头在PQC领域取得了显著成果。**2022年11月19日，谷歌宣布，Google Cloud已经在内部ALTS协议上启用了PQC以确保公司内部基础设施组件相互通信，并确保通信经过认证和加密。

图：谷歌内部加密传输协议应用层传输安全(ALTS):启用抗量子密码



图：量子安全OTN专线六大核心优势

来源：安全内参、中国电信浙江政企服务号公众号、天风证券研究所

3、量子算法或将击破经典密码体系

量子计算在某些问题上具有比传统计算更高的计算速度和效率：

- **Shor算法：**于1994年提出的一种大数质因子分解的量子多项式算法。这一算法将NP问题变为了P问题,利用数论中的一些定理将大数因子分解转化为求某个函数的周期，由于在量子环境下可以提高傅立叶变换效率，从而可以对大数质因子进行化简。我们认为，一旦可以运行Shor算法的量子计算机出世，现行的RSA公钥密码体制或受到威胁。
- **Grover算法：**针对对称（私钥）加密，如AES加密算法，只能进行暴力破解，而传统计算机的破解时间为指数时间，更准确地说，是依据其中密钥的长度。而量子计算机可以利用Grover算法进行更优化的暴力破解，其效率更高，量子计算机暴力破解AES-256加密的效率跟传统计算机暴力破解AES-128是一样的。

图：RSA实现原理，Shor算法可以高效破解RSA

两质数相乘容易，但是反过来，分解非常困难。

易	$104322269 \times 1998585857 = 208497011393549533$
难	$208497011393549533 = 104322269 \times 1998585857$

4、QKD（量子密钥分发）或 PQC（量子软加密），技术与迁移

目前能够实现量子安全的有两种方案：

- **QKD量子密钥分发：**是一种密钥的安全传输方式，基于物理原理，需要专用的物理设备，可以在两个相距遥远的通信端之间进行密钥的发送。在保密通信的过程中，需要用密钥加密解密信息，密钥的安全性保证了信息的安全性。
- **PQC算法：**为了应对量子计算对公钥密码算法的威胁，PQC应运而生。PQC是能够抵抗量子计算对现有密码算法攻击的新一代密码算法，旨在研究密码算法在量子环境下的安全性，并设计在经典和量子环境下均具有安全性的密码系统。

图：量子安全与经典密码对比

保密类型	技术基础	专用设备	出发点	关注点	安全性	现存问题
经典密码	数学原理	无需专用硬件设备	解析数学难题	密钥的保密性	不能抵御量子计算机攻击	不能抵御量子计算机攻击
QKD	物理原理	需专用硬件设备	一次一密加密体制	解决密钥分配问题	量子环境下，理论绝对安全	成本高、有硬件要求、应用场景有限
PQC	数学原理	无需专用硬件设备	解析数学难题	非对称密码系统	量子环境下，理论绝对安全	未经过充分验证

来源：光子盒公众号、天风证券研究所

5、PQC（量子软加密）的五种方案，格密码研究活跃

PQC的五种主流方案：

- 基于哈希的后量子密码算法：利用哈希函数的特性来创建数学签名，如XMSS和SPHINCS+，它们在后量子密码标准化中表现出色，以高效率和模块化设计为优势。
- 基于编码的后量子密码算法：依赖于纠结码的复杂性，尽管具有快速加密的优势，但较大的公钥尺寸限制了它们的应用范围。
- 基于多变量的后量子密码算法：构建在求解多变量方程组的困难性上，它们以快速运算和较小的签名尺寸为特点，但公钥尺寸和安全性问题仍需进一步研究。
- 基于格的后量子密码算法：以解决格中的困难问题位基础，如最短向量问题，因其良好的安全性和实用性被认为是后量子密码学中最有前景的方向。
- 基于曲线同源的后量子密码算法：围绕椭圆曲线间的同源映射，尽管SIKE算法被破解，但同源问题本身未被完全解决，相关研究仍在进行中，以小尺寸参数为特点。

类型	公钥尺寸	计算速度	功能多样性
格	小	快	很好
编码	大	快	较好
多变量	大	较快	较好
哈希函数	小	较快	有限
同源密码	极小	慢	较好

图：PQC的五种主流方案技术特点非定量对比

来源：安全内参官网、天风证券研究所

6、全球PQC（量子软加密）加速标准建立

表：多个国家地区开始对PQC展开研究并且加速标准制定

国家/地区	日期	事件
美国	2016	美国国家标准与技术研究院（NIST）在2016年就启动了PQC标准化工作，通过提名、会议研讨、四轮遴选，面向全球征集PQC算法。
	2021.10	国土安全部与NIST合作发布了应对量子技术风险的路线图，旨在帮助企业保护其数据和系统，降低量子技术发展相关的风险。同时，美政府力邀亚马逊，微软，谷歌等科技型龙头企业现有系统向PQC迁移。
	2023.08	NIST发布CRYSTALS-Kyber、CRYSTALS-Dilithium和SPHINCS+三种算法的标准草案，经过公众审查后预计于2024年正式批准。
		谷歌Chrome浏览器启用抗量子密码Kyber-768，对共享网络连接进行对称加密保护。
	2024	预计FALCON算法标准草案将向社会公布。
欧盟	2022	美拜登政府通过国家安全备忘录，和G7集团联合签署协议，要求欧盟快速推进PQC迁移工作，加快PQC发展进程。一方面，以项目形式深入PQC建设，如SafeCrypto项目采取基于格的密码学算法（抗量子密码四大主流算法之一），实现加密、数字签名、密钥交换、属性加密、函数加密、等公钥加密方案。另一方面，呼吁企业入局PQC应用，瑞士IDQ与PQC公司合作，为手机用户提供量子通信解决方案，应用于政府、企业等特定人群的敏感通信。
		德国英飞凌推出全球首款PQC固件保护更新可信平台模块，可抵消量子计算机攻击者损坏固件的威胁。
		芬兰Xiphera公司推出应用PQC算法的系列产品。该产品提供全面的量子安全密钥交换和数字签名集合。
日韩	近年	日本情报通信研究机构与合作方开发了基于PQC技术的IC卡，应用于医务人员IC卡认证和电子病历数据在长期安全数据存储和交换系统中的访问控制。
		韩国移动运营商LG U+于2022年推出韩国首个PQC商业服务，可防御量子计算机的黑客攻击，是世界上第一个PQC专线服务。
		韩国移动运营商SK Telecom和SKB将抗量子密码拓展到全球虚拟网络，进一步提高其国际网络安全等级。
中国	2019	中国密码学会自2019年起举办全国抗量子密码算法竞赛，该竞赛仅面向中国的密码学者，是我国PQC算法标准制定的基础。
	2021	新的“十四五”规划提出这 5 年是中国量子技术实现“弯道超车”的关键时期。
	2023	信通院联合行业内各个量子及密码龙头厂商发布了《后量子密码应用研究报告》，为我国开展后量子密码研究、迁移提供了指导思路。

来源：天翼智库公众号、标准化战略研究公众号、九州量子公众号、信息安全与通信保密杂志社公众号、天风证券研究所

7、金融行业尤其银行有望成为最先迁移到PQC（量子软加密）体系

- 对于金融行业乃至整个工业界而言，布局后量子密码安全技术，最重要的工作便是将现有的密码安全体系分阶段平稳过渡到后量子密码安全标准体系，即“后量子迁移”。
- 近年来，西方的多个国家，如德国、英国和法国，都已明确表示他们对后量子迁移的关注，而美国在这一领域已经走在了前列。
- **我们认为，目前党政军及关基行业或最先面临风险，从迁移速度来讲，金融行业尤其是银行作为国民经济重要领域，涉及大量的核心数据和交易信息，相比于其他行业或更早地采取相应的措施过渡到后量子密码体系**

表：应用公钥密码的金融应用场景

文件传输类	批量数据文件交换 代收付数据文件交换 与第三方文件交换，银联/央行等
传输通道类	网银 手机银行 员工远程办公
密钥管理CA类	内部CA;服务器证书（以文件证书存储私钥） 央行、EMV IC卡证书； 申请外部证书；比如CFCA等； USB KEY；网银盾；密码机管理 加密机设备主密钥证书
签名验签交易类	央行大平台交易 IC卡 网银盾签名验签 电子签章 卡组织交易

来源：金融电子化公众号、天风证券研究所

8、建议关注

量子产业或成为全球科技竞赛的下一站，建议关注三大方向：量子安全、量子计算、量子测量。建议关注：

1）**量子安全：**信安世纪、国盾量子、神州信息、格尔软件、三未信安、天融信、吉大正元

2）**量子计算：**国盾量子、普源精电、科华数据（通信&电新联合覆盖）、腾景科技

3）**量子测量：**科大国创、天奥电子

风险提示

1）政策落地不及预期：若量子科技相关政策落地不及预期，会对相关公司造成一定的影响；

2）量子计算研发进展不及预期：量子密码离不开量子计算，若量子计算研发进展不及预期，或对相关公司造成一定的影响；

3）后量子密码应用落地不及预期：后量子密码应用处于早期阶段，若推广不及预期，会对相关公司造成一定的影响。

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

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

THANKS