

苏州国芯科技股份有限公司

2025 年 7 月 30 日投资者关系活动记录表

证券简称：国芯科技

证券代码：688262

编号：2025-019

投资者关系活动类别	☒ 特定对象调研 ☐ 媒体采访 ☐ 新闻发布会 ☐ 现场参观 ☐ 分析师会议 ☐ 业绩说明会 ☐ 路演活动 ☐ 其他（请文字说明其他活动内容）
参与单位名称	兴业证券
时间	2025 年 7 月 30 日
地点	现场交流
上市公司参加人员姓名	董事长：郑茫 董事会秘书：龚小刚
投资者关系活动主要内容介绍	1、请介绍一下公司在抗量子密码技术和产品上的研发进展情况？ 答：国芯科技针对 NIST 公布的基于格原理、哈希原理和编码原理 3 种类型的 5 个抗量子密码算法，已开展从抗量子密码算法理论研究、算法硬件架构设计、算法软硬件实现、算法侧信道安全等多层次和多维度的深入研究。 目前已完成了 NIST FIPS 203 (ML-KEM)、FIPS 204 (ML-DSA)、FIPS 205 (SLH-DSA) 三个算法模块的硬件设计，其中 ML-KEM 和 ML-DSA 是基于格原理的抗量子密码算法，SLH-DSA 是基于哈希原理的抗量子密码算法。同时还提交了 5 个抗量子密码算法硬件设计及侧信道防护相关的专利申请。ML-KEM/ML-DSA/ SLH-DSA 三个抗量子密码算法 IP 已成功应用在公司的抗量子密码产品中。

	正在进行 NIST FIPS 206 (FN-DSA) 的算法硬件设计以及 NIST HQC 算法的理论研究及算法硬件架构设计，其中 FN-DSA 是基于格原理的抗量子密码算法，HQC 是基于编码原理的抗量子密码算法。 在抗量子密码芯片方面，公司通过与信大壹密合作开发，推出了抗量子密码芯片 AHC001。AHC001 是基于国产 28nm 工艺制程，并采用国芯科技自主可控 CPU 内核设计的一款可重构低功耗抗量子密码算法芯片，典型工作功耗和静态低功耗可分别低至 350mW 和 0.13mW 左右。芯片内集成了抗量子密码算法引擎、ECC 引擎以及对称密码处理器。抗量子密码算法引擎采用可重构电路技术实现，具备低功耗、算法可重构、高安全性以及高扩展性特点，可用于多种应用领域产品的高安全防护，适用于今后对安全要求较高的各种端和边缘侧设备场合。公司已完成抗量子 POS 芯片的开发，目前该芯片产品已在流片生产中。 同时，公司在今年 6 月成功研制了抗量子密码卡 CCUPHPQ01，该抗量子密码卡是一款基于抗量子密码算法与经典国密算法相结合，以公司自主设计研发的 CCP1080T 安全芯片为主控芯片，外加一颗国产 FPGA 芯片而设计完成的高性能密码安全产品。该产品遵循国家密码管理局关于密码模块、PCIe 密码卡等相关技术规范，支持 SM1、SM2、SM3、SM4 等国密算法，同时支持主流的抗量子密码算法，如 Kyber512/Kyber768/Kyber1024 加密算法、Dilithium2/Dilithium3/Dilithium5 数字签名算法等，其中：抗量子密码算法 Kyber512 密钥生成速度达到 2700 次/s，加密速度达到 2300 次/s，解密速度可达到 1800 次/s；Dilithium2 算法密钥生成速度达到 860 次/s，签名速度达到 190 次/s，验签速度达到 600 次/s。该产品支持抗量子密码算法更新，能够很好地跟进抗量子密码算法的迭代及标准化推进过程。该新产品的随机源采用 CQWNG10 量子随机数芯片，该随机数芯片的随机性源自于量子物理原理，并可采用物理熵理论严格证明其随机性，具有更高的安全性和更快的随
--	---

	机数生成速度。该抗量子密码卡新产品可以同时支持抗量子密码算法和传统密码算法应用，采用抗量子密码卡的安全产品或设备可以通过抗量子密码算法和传统密码算法共存方式，逐步进行抗量子密码算法应用迁移，在保障原有业务不受影响的情况下开展抗量子密码算法在新业务中应用，既满足现有业务系统密码应用，又能有效抵御量子计算攻击，进而增强了安全产品或设备抗量子计算攻击的能力。该抗量子密码卡新产品能够为各类安全平台提供多线程、多进程处理的高速密码运算服务，满足其对数字签名/验证、非对称/对称加解密、数据完整性校验、真随机数生成、密钥生成和管理等功能的要求，保证敏感数据的安全性、真实性、完整性和抗抵赖性。该抗量子密码卡产品可以适配龙芯、飞腾、海光等主流平台，支持UOS、麒麟、Linux等主流操作系统，可广泛应用于金融、通信、电力、物联网等领域以及签名/验证服务器、安全网关/防火墙等有高安全要求的信息安全设备中。 说明：对于已发布的重复问题和内容，本表不再重复记录，更多关于公司的情况敬请查阅公司在《中国证券报》《上海证券报》《证券时报》《证券日报》和上海证券交易所网站上披露的定期报告、临时报告及公司在上证E互动平台“上市公司发布”栏目刊载的各期《投资者关系活动记录表》。
附件清单 (如有)	无
日期	2025 年 7 月