证券代码：688262　　证券简称：国芯科技　　公告编号：2025-044

苏州国芯科技股份有限公司

关于自愿披露公司与参股公司郑州信大壹密科技有限公司合作研发的抗量子密码芯片新产品内部测试成功的公告

本公司董事会及全体董事保证本公告内容不存在任何虚假记载、误导性陈述或者重大遗漏，并对其内容的真实性、准确性和完整性依法承担法律责任。

苏州国芯科技股份有限公司（以下简称“公司”或“国芯科技”）与参股公司郑州信大壹密科技有限公司(以下简称“信大壹密”)合作研发的抗量子密码芯片AHC001新产品于近日在公司内部测试中获得成功。现将相关事项公告如下：

一、新产品的基本情况

公司与信大壹密合作的抗量子密码芯片AHC001是基于国产28nm工艺制程进行研发，采用公司自主CPU内核设计的一款可重构低功耗抗量子密码算法芯片。该芯片的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，通过可重构指令可以定制不同的抗量子密码算法，该引擎模块支持ML-KEM-512/ML-KEM-768/ML-KEM-1024密钥对生成算法、密钥封装/解封装算法、加密/解密算法；支持ML-DSA-44/ML-DSA-65/ML-DSA-87密钥对生成算法、签名算法和验签算法；支持256/512/1024/4096点NTT/INTT/DWT/IDWT运算，并支持4路并行NTT高性能计算；同时，还支持中心二项分布采样/拒绝采样等常用的采样算法；可以灵活地支持主流基于格原理的抗量子密码算法，如Kyber512/Kyber768/Kyber1024加密算法、Dilithium2/Dilithium3/Dilithium5数字签名算法，其中：抗量子密码算法Kyber512密钥生成速度达到3600次/s、加密速度达到2600次/s和解密速度可达到 1300次/s；Dilithium2算法密钥生成速度达到990次/s、签名速度达到300次/s和验签速度达到500次/s。同时，AHC001芯片集成的ECC引擎支持实现国密SM2算法，对称密码处理器可以采用可重构指令方式实现国密算法SM3/SM4等算法和国际通用算法DES/AES/SHA等算法。AHC001

芯片内置真随机数发生器，并具有电压检测、温度检测、频率检测、电源毛刺检测、光检测和金属防护网等多种安全防护设计。AHC001芯片支持USB3.0接口、SD3.0/EMMC5.0接口、百兆以太网接口、SSI/SPI接口以及UART、ISO7816、I2C等必要的低速外设。AHC001芯片具备低功耗、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的产品高安全防护，适用于今后对安全要求较高的各种端和边缘侧设备场合。

抗量子密码芯片AHC001可以同时支持抗量子密码算法和传统密码算法应用，采用AHC001芯片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，增强安全产品或设备抗量子计算攻击的能力，本芯片可以广泛应用于金融、通信、电力、物联网等有高安全要求的信息安全设备中。

二、对公司的影响

公司与信大壹密对上述芯片产品共同拥有知识产权。本次抗量子密码芯片新产品研发成功，是公司在量子安全领域长期坚持创新驱动的结果，实现了公司安全芯片产品的抗量子化提升，进一步完善了公司信创与信息安全芯片产品的布局，将为信息安全领域抗量子密码技术的迁移提供技术支撑，对公司未来市场拓展和业绩成长性预计都将产生积极的影响。

三、风险提示

本次测试目前是公司内部测试成功，尚未完成第三方机构检测测试。本次公司与合作方信大壹密共同推出抗量子密码芯片 AHC001 新产品尚处于市场导入初期，尚未实现规模化销售，存在市场推广与客户开拓不及预期、客户验证失败等风险，将对公司收入及盈利带来不确定性，公司将及时根据后续进展履行信息披露义务，敬请广大投资者注意投资风险。

特此公告。

苏州国芯科技股份有限公司

董事会

2025 年 5 月 7 日