网络安全与后量子密码迁移白皮书

White Paper on Cybersecurity and Post-Quantum Migration

正式研究展示文件

本文件讨论数字科学组织和技术项目在网络安全、密码体系更新、后量子迁移准备度和安全评审方面的共性问题。内容强调阶段性评估、资产梳理和风险沟通，不以夸张的威胁叙事替代专业分析。

发布日期：2025年09月20日
发布机构：数字科学促进与研究协会（ADSPR） / 数智研究院（DSRI）

一、背景说明

后量子密码迁移不是一次性替换算法，而是涉及资产识别、协议兼容、系统验证、供应链管理和长期维护的综合工作。数字科学项目越依赖数据协作和平台化工具，越需要提前规划安全基础。

二、迁移准备度维度

资产清单

识别系统中使用的加密算法、证书、密钥管理方式和外部依赖。

兼容验证

评估新旧算法并行、性能影响和业务连续性。

风险沟通

对管理层、研究团队和技术维护人员说明迁移原因、时间表和限制条件。

阶段	目标	说明材料
识别	建立加密资产视图	算法、证书、接口清单
试点	验证兼容与性能	测试记录、影响分析
切换	降低迁移风险	时间表、回退方案

三、评审关注点

DSRI 在网络安全相关成果评审中关注技术有效性、攻防模型、实验环境、边界条件和可复核记录。对后量子迁移方案，应重点检查算法选择依据、替换路径和回退方案。

四、建议路线

建议组织采用“识别—分级—试点—并行—切换—复盘”的路线推进迁移。对于研究型项目，可以先完成风险清单和小范围验证，再进入更完整的工程规划。