调研任务：**密码体系调研报告**

**1、**常用密码体系调研****：拉取清单，调研常用密码体系的量子威胁度研究水平，选课题研究，如 RSA 密码等对称加密方法

****2、量子密码调研设计****：罗列不同场景下使用的密码成 list 并设计调研课题，一个月内完成

****3、后量子密码学研究****：梳理关于其状态、现有算法问题及现有密码鲁棒性的思考提纲，与对方团队进一步沟通

**目录**

1. 背景与目的
2. 调研内容与方法
3. 详细调研方案
4. 预期成果与沟通计划
5. 风险评估与时间安排
6. 结论

**1. 背景与目的**

量子计算技术的突破性进展（如IBM的433量子比特处理器、谷歌的量子霸权实验）对传统密码体系构成颠覆性威胁。根据NIST预测，2030年后量子计算机可能破解现有非对称加密算法（如RSA、ECC），全球每年因量子攻击导致的数据泄露风险损失预计超3000亿美元。

**本报告目标**：

1. **评估威胁**：量化分析RSA、AES等常用密码算法在量子攻击下的脆弱性；
2. **设计对策**：针对金融、政务等场景设计量子密码技术方案，并规划一个月内可落地的研究课题；
3. **推动协同**：梳理后量子密码学技术瓶颈，形成产学研协作攻关路线。

**2. 调研内容与方法**

**2.1 常用密码体系调研**

**目标**：建立密码体系量子威胁等级清单，筛选高风险算法作为研究重点。  
**方法**：

* **数据收集**：拉取清单（RSA-2048/3072、ECC-P256、AES-128/256、SHA-256、SM2/SM4等）；
* **文献分析**：结合NIST SP 800-208、中国信通院《量子安全白皮书》等权威报告，量化威胁等级；
* **专题研究**：聚焦RSA与AES的量子攻击模拟（基于Qiskit/Grover算法）。

**2.2 量子密码调研设计**

**目标**：分场景设计量子密码方案，完成1个月内可行性验证。  
**方法**：

* **场景划分**：金融交易、政务通信、物联网、能源网络（参考合肥量子城域网案例）；
* **技术匹配**：
  + **金融**：QKD（量子密钥分发）+ PQC（后量子算法）混合加密；
  + **政务**：量子安全VPN + 动态密钥轮换（参考苹果PQ3协议）；
  + **物联网**：轻量级QKD芯片（如国盾量子燃气表方案）。

**2.3 后量子密码学研究**

**目标**：识别算法瓶颈，构建鲁棒性评估框架。  
**方法**：

* **现状分析**：NIST后量子密码标准化进展（ML-KEM、SLH-DSA等算法）；
* **问题识别**：格基算法的高计算复杂度、与国密SM2的兼容性冲突；
* **鲁棒性评估**：抗量子攻击能力、硬件适配性、标准化成熟度三维度分析。

**3. 详细调研方案**

**3.1 常用密码体系调研方案**

**步骤一：拉取清单**

|  |  |
| --- | --- |
| **类别** | **算法清单** |
| 非对称加密 | RSA-2048/3072、ECC-P256、SM2 |
| 对称加密 | AES-128/256、ChaCha20、SM4 |
| 哈希函数 | SHA-256、SHA-3、SM3 |

**步骤二：量子威胁度评估**

|  |  |  |  |
| --- | --- | --- | --- |
| **算法** | **量子威胁等级** | **攻击模型** | **破解时间（量子环境）** |
| RSA-2048 | 极高 | Shor算法 | 10秒（4099量子比特） |
| ECC-P256 | 极高 | Shor算法 | 同RSA |
| AES-128 | 中等 | Grover算法 | 安全性降至64位 |
| SHA-256 | 低 | 量子随机行走 | 碰撞效率提升至经典算法的2/3 |

**步骤三：选题研究**

* **RSA专题**：探索3072位以上密钥扩展方案（需验证性能损耗）；
* **AES替代**：测试ChaCha20-Poly1305在量子环境下的抗攻击能力。

**3.2 量子密码调研设计方案**

**场景与技术匹配**

|  |  |  |  |
| --- | --- | --- | --- |
| **场景** | **技术方案** | **研究课题** | **时间节点** |
| 金融交易 | QKD + ML-KEM（NIST标准） | 密钥协商效率与抗中间人攻击验证 | 第1-2周 |
| 政务通信 | 量子安全VPN + 动态密钥轮换（PQ3） | 跨域密钥分发与身份认证协议设计 | 第2-3周 |
| 物联网 | 轻量级QKD芯片（功耗<1W） | 低功耗协议优化与硬件集成测试 | 第3-4周 |

**调研计划**

* **第1周**：场景需求分析 + 技术选型（参考中电信量子城域网案例）；
* **第2周**：搭建QKD-PQC混合加密实验环境（基于OpenQKD平台）；
* **第3周**：性能测试（密钥生成速率、抗攻击能力）；
* **第4周**：撰写报告并组织专家评审。

**3.3 后量子密码学调研思考提纲**

**当前状态**

* **国际标准**：NIST已标准化ML-KEM（基于格）、ML-DSA（数字签名）算法；
* **国内进展**：国密局推动SM9后量子化改造，但尚未形成统一标准。

**存在问题**

1. **安全性**：格基算法参数选择不当可能导致密钥泄露（参考2023年Kyber侧信道攻击事件）；
2. **效率**：Classic McEliece算法密钥长度达1MB，难以适配移动设备；
3. **兼容性**：NIST标准与SM2/SM9的国密体系存在协议冲突。

**鲁棒性讨论**

|  |  |  |  |
| --- | --- | --- | --- |
| **算法类型** | **抗量子攻击能力** | **硬件适配性** | **标准化成熟度** |
| 格基（ML-KEM） | 高 | 低 | 高（NIST认证） |
| 哈希（SLH-DSA） | 中 | 高 | 中（草案阶段） |
| 编码（Classic McEliece） | 极高 | 极低 | 低（未标准化） |

**沟通提纲**

1. **技术路线**：优先支持格基还是编码路线？如何平衡安全性与效率？
2. **迁移路径**：政务/金融先行试点，还是全行业推广？
3. **国际合作**：如何参与NIST标准制定并维护自主可控？

**4. 预期成果与沟通计划**

**成果输出**

1. **量子威胁评估报告**：含RSA/AES攻击模拟数据与优化建议；
2. **量子密码课题列表**：3个场景技术方案 + 1个月内可行性验证结果；
3. **后量子密码讨论提纲**：算法瓶颈清单 + 产学研协作路线图。

**沟通机制**

* **内部**：每周五例会同步进展（重点讨论QKD密钥生成速率瓶颈）；
* **外部**：与国盾量子、中电信量子集团召开2次专题会（议题：标准兼容性、试点落地）。

**5. 风险评估与时间安排**

**风险应对**

|  |  |
| --- | --- |
| **风险类型** | **应对措施** |
| 数据不全 | 预留2周补充NIST最新草案（如FIPS 206） |
| 技术迭代 | 订阅arXiv、IACR平台追踪量子算法突破 |
| 协同障碍 | 提前签署NDA协议，明确知识产权归属与利益分配 |

**6. 结论**

量子计算对密码体系的威胁已迫在眉睫，需采取“三阶段”应对策略：

1. **短期（1-2年）** ：在金融、政务领域部署QKD+PQC混合加密（参考苹果PQ3协议）；
2. **中期（3-5年）** ：推动国产后量子算法（如SM2-PQC）标准化与芯片量产；
3. **长期（5-10年）** ：构建“量子-经典”融合的安全基础设施（如中电信量子密话网络）。

**引用文献**

**1**: 量子计算对现代密码体系安全性影响及现状分析（中移智库，2024）

**2**: 量子计算对现有密码体系威胁（2024）

**3**: 量子密码协议研究现状与未来发展（中国工程科学，2022）

**5**: 中国工商银行吕仲涛：量子计算对银行密码算法的威胁及对策（2022）

**6**: 2000位以上RSA加密技术深度解析（2024）

**7**: 量子危机提前到来？中国学者用量子计算破译RSA！（2024）

**11**: 后量子密码发展现状研究（中移智库，2024）

**13**: 中电信量子集团：量子密码全面解决方案（2024）

**14**: 量子密码技术典型应用场景解读（科盾量子，2024）

**15** NIST SP 800-208《后量子密码迁移指南》（2024）  
**16**: 中国信通院《量子安全白皮书》（2025）  
**17**: 苹果公司《PQ3协议技术白皮书》（2024）  
**18**: 国盾量子《QKD在能源网络中的应用案例》（2023）