通信网密码敏捷技术体系研究

随着 6G 网络向“通感算智安”深度融合、空天地一体化泛在连接演进，以及量子计算等技术的快速发展，通信网密码应用面临三大挑战：新场景对密码应用提出低时延、轻量化、跨域信任传递等多样化新需求；量子计算对传统公钥密码体系构成颠覆性威胁，带来后量子密码迁移难题；网络技术演进引入新型攻击面，静态密码体系需变革以应对动态风险。

针对上述问题，本文提出通信网密码敏捷技术体系，以弹性安全与智能化为核心目标，构建由密码敏捷管理和敏捷密码资源组成的技术体系，建议未来在加快国产 PQC 标准研制、推动敏捷技术产品化、建立评估认证体系的同时，可依托试验网开展大规模验证，为 6G 网络在量子时代构建高弹性、可迭代的安全韧性。

1. 通信网密码应用安全面临新挑战

（一）6G 新场景对密码应用提出多样化需求

国际电信联盟（ITU）定义的 AI 与通信融合、感知与通信融合、泛在连接等 6G 六大应用场景，对安全提出了多样化新需求。工业控制、远程交互场景需要低时延、轻量化密码协议，避免加密认证造成业务时延超标；海量物联网终端算力、功耗受限，亟须轻量化密码算法与低开销协商机制；空天地一体化跨域通信场景，对跨域信任传递、动态密钥协同、异构协议适配提出硬性要求。此外，6G 新业务迭代速度快，安全需求动态演变，要求密码体系具备快速适配、动态切换、按需调度的敏捷能力，传统固定不变的密码应用模式难以适配应用场景持续迭代的发展趋势。

（二）量子计算对传统密码体系构成安全威胁

量子计算能够在短时间内破解基于大整数分解、离散对数等数学难题实现的传统密码算法，对当前广泛使用的公钥密码体系构成颠覆性威胁，已成为全球密码学界与安全行业共同关注的焦点，催生经典密码体系向后量子（PQC）密码体系迁移。因此，6G 网络从架构设计之初即需纳入后量子安全的考量。同时，PQC 算法标准正逐步走向成熟，这为 6G 网络提供了主动构建算法弹性支持的契机——以快速、低成本的敏捷更新能力，从容应对未来密码算法的持续演进。

（三）通信网技术演进引入新型攻击面

通信网的全面升级，极大拓展了网络攻击面，催生了新型密码安全风险。6G 深度融合 AI、通感一体化、数字孪生、边缘计算等技术，网络架构呈现异构化、动态化、开放化特征，传统封闭的安全边界彻底瓦解，网络节点、交互链路、数据交互模式愈发复杂，衍生出新型攻击手段，密码安全防护难度大幅提升。同时，攻击手段迭代加速、密码技术更新周期大幅缩短，被动式、静态化的传统防护模式已无法适配动态多变的安全风险，亟需构建高弹性、可迭代、主动防御的密码敏捷体系。

2. 通信网密码敏捷技术体系

（一）安全目标

在弹性安全方面，支持密码算法、协议的快速动态升级，实现适用性算法的自动优化选择、实体间敏捷协商与互操作。

在智能化方面，实现 AI 与密码技术深度融合，具备感知、决策与自优化能力，通过大模型和大数据驱动特征分析、威胁感知和动态响应。

（二）体系框架

面向通信网密码敏捷需求，结合弹性安全与智能化的设计目标，形成由密码敏捷管理和具备密码敏捷性的密码资源组成的技术体系，包含多个关键模块，模块间相互协作，横向拉通资源，形成从风险分析、敏捷响应到资源智能调度的完整闭环，共同构建起灵活、高效、安全的密码敏捷技术体系。

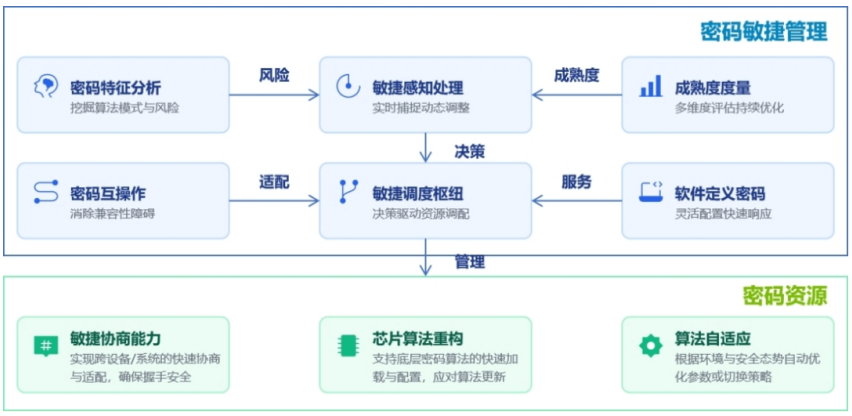

图 1　通信网密码敏捷体系框架图

3.通信网密码敏捷关键技术

（一）基于 AI 的密码特征分析

在技术需求方面，利用 AI 技术对密码使用模式、安全属性和潜在风险进行探测发现与深度挖掘。

技术原理为监测加密通信的行为指纹，识别网络攻击，分析隐藏于加密数据中的异常、威胁或潜在信息，实现加密环境下的威胁识别、异常监测、流量分类与合规审计。采用 AI 模型分析加密数据的特征、协议交互模式或计算行为，判断所使用的密码算法类型及其参数配置，破解加密通信的“黑箱”状态，识别老旧弱密码算法、未授权算法或后门风险，支撑漏洞评估及密钥强度分析等。将轻量化模型嵌入通信网网元或终端，实现本地化实时分析，基于分析结果，优化密钥管理效率、密钥协商开销等。

（二）敏捷感知及处理

在技术需求方面，实时感知不安全的密码应用和风险信号，动态调整处理策略并触发快速响应，实现多源信息融合分析、动态策略匹配和自动化处置。

技术原理为构建分布式采集代理汇聚资产信息，建立图数据库存储密码资产关系。对密码行为基线建模，实时计算偏离度，通过关联规则引擎识别复合攻击模式。将安全策略表述为声明式规则，策略决策点接收态势感知输出的风险向量和业务上下文，通过强化学习模型选择最优算法组合和执行参数。策略执行点在数据平面无中断加载新配置，建立安全编排自动化工作流引擎，支持密钥停用、证书撤销、访问控制更新等原子动作的并行执行和条件分支。

（三）敏捷成熟度度量

在技术需求方面，量化评估密码敏捷能力，识别短板并指导迭代升级，建立从框架、指标体系到分级评分的完整度量技术。

技术原理为构建五维度量模型——度量对象、度量指标、敏捷目标、成熟度等级、度量方法。建立指标树：包括动态替换能力（切换成功率、中断时间）、验证恢复机制（回滚有效性、自愈时间）、成本开销（资源消耗）、安全合规（策略匹配度）等。通过自动化测试

用例采集各度量项数值，加权聚合得到综合得分。采用模糊综合评价法处理定性指标，结合层次分析法确定权重，将评分映射至五级成熟度（初始→可重复→已定义→量化管理→优化），并生成雷达图展示各维度短板。

（四）密码互操作

在技术需求方面，消除异构密码系统间的兼容性障碍，支持多算法混合部署、跨域信任传递和密码原子能力解耦。

技术原理为建立密码操作元模型，抽象定义密钥生成、加密/解密、签名等操作的通用语义，使用属性标签描述算法特定参数。多协议转换引擎采用适配器模式，将各厂商私有协议请求转换为标准描述，再生成目标协议报文，自动完成密钥格式转换和签名体制转译。混合密码网关由服务入口层、适配器注册中心、路由引擎组成，实现统一接口、热插拔适配和智能路由。跨域认证时可使用可验证凭证技术，通过零知识证明验证证书有效性，保护隐私。

（五）敏捷调度

在技术需求方面，根据风险评估结果和业务需求，动态编排调度异构密码资源，实现多算法共存、弹性容灾和快速资源迁移。

技术原理为采用控制面与数据面分离架构。控制平面运行编排引擎，将策略转换为资源调度任务；数据平面部署轻量级代理，执行资源绑定和服务热加载。控制器维护全局资源视图，使用有状态工作流编排跨节点算法切换任务。构建密码能力抽象层，定义统一能力描述语言，适配层实现描述到各厂商驱动的映射。采用集群管理方式，故障检测使用自适应故障检测器；节点失效时冻结会话，将密码上下文序列化后在健康节点重建实例，通过两阶段提交保证状态一致性，实现无缝切换。

（六）软件定义密码

在技术需求方面，摆脱密码服务对特定硬件的依赖，实现算法热替换、服务灵活扩展和多域资源动态分配。

技术原理为将物理密码设备虚拟化为多个实例，每个实例运行独立容器，封装算法库和密钥存储。容器编排平台将虚拟密码资源作为

扩展资源调度，支持自动伸缩和故障迁移。定义统一密码服务 API，服务端实现动态适配器链：请求经协议识别、策略匹配后选择适配器，完成参数校验和负载均衡。新增算法时注册适配器即可纳入服务发现。构建中心-边缘两级调度架构：中心调度器负责全局容量规划和跨域任务分配，边缘调度器实时响应本地请求。跨域任务通过任务拆分，将端到端密码服务拆解为子任务分配到最优节点执行。

（七）敏捷协商

在技术需求方面，在异构密码系统间实现动态协商，解决算法多样性引发的协商复杂性、降级攻击威胁、跨代协议兼容和资源受限效率问题。

技术原理为扩展传统安全协议字段，构建可兼容经典密码与 PQC 的混合协商架构，依托动态算法标识、双协议并行握手、量子安全签名校验等机制，分析协议交互流程、算法选择逻辑与密钥派生行为，实现异构密码算法的自动适配、跨域策略对齐与降级攻击防护。有效识别恶意算法降级、非法协议篡改、协商策略不匹配等安全风险，保障多代密码体系平稳过渡。通过轻量化协议裁剪与预协商模板机制，降低物联网终端协商时延与算力开销，同时依托策略智能匹配模型，实现不同网络切片、不同安全场景的自适应协商，全面提升跨域通信的安全性、适配性与协商效率。

（八）芯片算法重构

在技术需求方面，芯片层面实现密码算法的动态重构，支持“一芯多算法”，同时满足高性能和硬件安全性。

技术原理为采用可重构架构，将密码算法计算分解为多个可配置运算单元阵列，芯片硬件层固化密码运算单元，包括算法引擎，以及 NTT 变换器、多项式环乘法模块等核心数学原语和通用模数运算资源；智能调度中间件集成资源感知算法与安全策略引擎，按业务需求分配计算资源，支持多算法实例的时空隔离与优先级抢占，提升硬件利用率并降低任务响应时延。构建可信执行环境硬件扩展，通过内存加密引擎保护安全区域，同时重构映像经过哈希验证后写入。

（九）算法自适应

在技术需求方面，根据环境变化（威胁等级、业务负载、终端能力）自动优化密码算法参数或策略，实现安全性与性能的动态平衡。

技术原理为集成密码系统态势数据，主要包括网络环境数据、安全威胁等级、业务负载、终端类型、终端算力、密码系统运行情况等，并利用大数据分析、人工智能和分布式信任等技术构建风险评估算法，实时评估风险等级，为密码算法的优化策略提供准确依据。根据风险评估结果，基于规则引擎与人工智能模型，生成适配当前环境的密码算法策略，自动或手动切换算法相关参数及可选项，并管理加密策略的相关执行范围。针对物联网终端等资源受限场景，开发轻量级密码算法及协议、算法低功耗模式等技术，并根据环境及性能情况提供不同的算法可选项，在安全与能耗间实现平衡。与密钥管理、密码协议、6G 业务系统密码功能组件联动，实现算法相关性因素的统一切换，提高系统鲁棒性。

4. 展望

为应对通信网络与密码技术演进的持续加速，建议充分考量密码应用需求，通过构建对应的密码敏捷技术体系，规划密码敏捷关键技术，赋予 6G 网络密码敏捷特性，以应对未来日益严峻的安全挑战。面向未来，建议加快国产 PQC 算法标准研制，形成自主可控储备；推动敏捷关键技术产品化，构建密码敏捷中间件与芯片方案；同时，跨行业评估认证体系；依托试验网开展大规模验证，积累迁移工程经验，通过体系化布局、分阶段推进，保障 6G 网络在量子时代的安全韧性。

来源：中移智库