公钥密码算法评估准则

商用密码标准研究院

2025 年 10 月

目　录

本文档给出商用密码标准研究院举办的新一代商用密码算法征集活动公钥密码算法评估遴选的有关考虑。

1 算法安全性

（1）理论安全性：数字签名方案应满足 EUF-CMA 或 SUF-CMA 安全性，密钥封装机制应满足 IND-CCA2 安全性，密钥交换协议应满足在合适的安全模型（例如 CK、CK+、eCK、eCK-PFS 模型）下的安全性。

（2）具体安全性：算法实例应达到对应等级的经典（量子）安全强度，并具有一定的安全冗余。评估算法具体安全性时，可以假设敌手进行签名询问、解封装询问等的次数不超过 2^{80}。

（3）其他安全特性：算法抗侧信道攻击安全性、（完美）前向安全性、抗多密钥攻击安全性、（临时）密钥重用情况下的安全性等将在评估中考虑。

2 算法性能

（1）运算效率：数字签名方案的密钥生成速度、签名速度、验证速度；密钥封装机制的密钥生成速度、封装速度、解封装速度；密钥交换协议的共享秘密密钥建立速度。

（2）传输与存储开销：数字签名方案的公钥长度、私钥长度、签名长度；密钥封装机制的公钥长度、私钥长度、密文长度；密钥交换协议的轮数、长期公钥长度（如有）、长期私钥长度（如有）、密钥交换消息长度。

（3）资源消耗：软件实现内存资源占用；硬件实现面积、时延、

吞吐量、吞面比、功耗、能耗。

3 算法特点

（1）创新性：体现新设计理念、代表新发展趋势。

（2）简洁性：便于理解和实现，利于充分评估算法安全性。

（3）灵活性：支持在多种平台上安全高效实现，支持在运算效率与资源消耗之间平衡折中。

（4）兼容性：支持基于相同的数学困难问题和参数选择方案，实现安全强度相匹配的数字签名、密钥封装、密钥交换等不同密码功能；支持与已有协议和应用兼容，易于算法迁移。

（5）可扩展性：对算法进行修改后能够提供超出数字签名、密钥封装、密钥交换的其他密码功能。

（6）在不同平台上的实现性能优势：支持并行处理、指令集加速、资源受限环境下的安全高效实现。

4 算法遴选的综合考量

遴选过程将综合考量算法安全性、性能和其他特点。考虑到新型量子算法和密码分析技术发展的不确定性，遴选过程还将关注底层数学困难问题的多样性。

此外，算法提交者和相关专利权人的知识产权声明也是重要因素，不存在影响标准化或推广因素（例如知识产权问题）的算法将被优先考虑。