密码杂凑算法评估准则

（征求意见稿）

商用密码标准研究院

2025 年 2 月

目　录

本文档给出新一代商用密码算法征集活动密码杂凑算法评估遴选的有关考虑。

1 算法安全性

（1）理论安全性：在合理的假设条件下，算法应具有整体结构和组件安全性证明或分析。

（2）具体安全性：算法抗碰撞攻击的经典安全强度应不低于 $h/2$ 比特、抗原像攻击的经典安全强度应不低于 h 比特、抗第二原像攻击经典安全强度应不低于 h 比特，其中 h 是杂凑值长度。针对算法的量子计算攻击复杂度应不低于通用量子算法攻击复杂度。

（3）其他安全特性：算法应具有良好的统计随机性。算法针对近似碰撞攻击、半自由起始碰撞攻击、自由起始碰撞攻击、多碰撞攻击、长度扩展攻击等的安全性，以及输出的任意固定子集针对碰撞攻击、原像攻击、第二原像攻击等的安全性将在评估中考虑。

2 算法性能

（1）运算效率：生成杂凑值的运算效率。

（2）资源消耗：软件实现内存资源占用；硬件实现面积、时延、功耗、能耗、吞吐量、吞面比。

3 算法特点

（1）创新性：具备理论创新、结构创新或其他创新特点，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：支持构造消息鉴别码（MAC）等相关密码功能，

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）在多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。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，不存在阻碍标准化或推广因素（例如知识产权问题）的算法将被优先考虑。