对于密码杂凑算法提交要求与评估准则相关意见的反馈

商用密码标准研究院

2025 年 10 月

商用密码标准研究院（ICCS）感谢各位专家学者对新一代商用密码算法征集活动（NGCC）的关注。密码杂凑算法提交要求和评估准则是NGCC的重要工作依据。自公开征求意见以来，ICCS收到了全球多名专家学者提出的宝贵意见，ICCS 组织对意见进行了认真研究评估。意见处理及文件修订情况如下。

一、关于算法输出长度和安全强度要求

有专家学者询问征集输出长度为512比特和1024比特的密码杂凑算法的相关考虑，建议放宽对于密码杂凑算法抗原像攻击、抗第二原像攻击的安全性要求。

中国现有SM系列算法研制应用至今已逾20年，为了抵抗量子计算风险，同时满足大数据、物联网、云计算、人工智能等新技术新应用的发展需求，亟需研制新一代商用密码算法。NGCC计划征集公钥密码算法、密码杂凑算法和分组密码算法等3类密码算法，以期形成相互适配的新一代商用密码算法体系，推动新一代商用密码算法标准制定。

ICCS认为256比特经典安全强度的密码算法将逐渐成为密码应用中的主流算法，因此NGCC征集输出长度为512比特的密码杂凑算法。同时，ICCS也十分关注未来发展趋势，提出512比特经典安全强度且输出长度为1024比特的算法需求意在引领密码领域的技术创新，推动密码算法设计的代际发展，并为未来的高安全需求应用预留发展空间。

ICCS 注意到，近年来学术界正在积极推动大状态密码杂凑算法的设计与分析研究。在此发展趋势下，NGCC认为要求密码杂凑算法抗原像攻击、抗第二原像攻击的经典安全强度应不低于输出长度是合

理的。ICCS 期待具有理论创新、结构创新或其他创新特点的算法提案。

二、关于算法功能需求

有专家学者咨询 NGCC 是否仅接受面向二进制域的密码杂凑算法提案。也有专家学者提出密钥派生函数（KDF）、可扩展输出函数（XOF）是密码杂凑算法的重要应用，建议征集和遴选考虑密码杂凑算法易于支持相关函数构造的灵活性。

NGCC 的征集对象是通用型密码杂凑算法，满足《密码杂凑算法提交要求》的算法提案都是可接受的。ICCS 将根据《密码杂凑算法评估准则》对算法提案的安全性、性能、特点等进行综合评估。

关于密码杂凑算法的其他扩展功能，ICCS 采纳了该意见，在《密码杂凑算法评估准则》的“算法特点”章节中增加了易于构造安全的密钥派生函数（KDF）、可扩展输出函数（XOF）的相关考虑。

三、关于实现性能评估

有专家学者建议公开测试环境，并在统一的环境中进行算法实现性能测试。

ICCS 将在统一条件下对优化实现代码进行性能测试，并对算法的实现性能进行综合评估。ICCS 将适时公布统一的性能测试环境。

算法提交者提供的性能测试结果主要用于说明算法提案的性能优势，并不作为算法性能评估的正式依据。考虑到算法提案的性能测试结果不具备统一对比的参考价值，ICCS 删除了《密码杂凑算法提交要求》中“与已有标准算法的对比分析结果”的要求。

需要注意的是，软件和硬件实现性能是算法遴选的重要因素。首次提交算法时，应提交算法软件实现代码及自评估结果，鼓励提交算

法硬件实现代码及测试结果；后续评估轮次中将要求提供软件和硬件实现代码及测试结果。

四、关于知识产权

有专家学者关注 NGCC 知识产权的相关工作原则。

ICCS 尊重密码科研成果，高度重视合法知识产权权益保护。为了促进标准算法的广泛采用，NGCC 遵循公平合理无歧视的知识产权许可原则。因此，算法提交者和相关权利人的知识产权声明和许可承诺是算法遴选的重要因素，NGCC 要求算法提交者对知识产权事项进行充分披露并作出使用授权承诺。同等条件下，具有公平合理无歧视且免费的知识产权授权承诺的算法将被优先考虑。

五、关于辅助程序

有专家学者提出，ICCS 提供的辅助程序应具有良好的适用性，能够兼容各类编译器。

为了便于开展算法正确性验证，ICCS 开发了一套辅助程序，用于算法提交者基于算法实现生成已知答案测试（KAT）向量。ICCS 始终关注辅助程序的适用性。辅助程序支持 ISO/IEC 9899:1999（C99）标准，可在当前主流编译器环境下使用。

再次感谢所有反馈意见、参与讨论的专家学者！你们的专业建议和技术贡献为本次征集活动提供了有益参考和指导。ICCS 将继续秉持开放合作的态度，与全球密码学术界、产业界一道共同推动新一代商用密码技术的发展。