对于公钥密码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。公钥密码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、关于算法征集活动的目标和意义

有专家学者询问，在相关国家已陆续完成抗量子密码算法征集并推动相关算法标准化的背景下，商用密码标准研究院开展本次算法征集活动的目标和意义。

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类算法，是在前期国际密码研究工作取得的成果基础上做出的新探索，希望进一步促进密码算法设计与分析技术发展创新，进一步丰富密码算法特别是抗量子计算公钥密码算法的新颖性、多样性，进一步推动国际密码学术交流、繁荣密码学科发展，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。

二、关于算法提案的限制要求

有专家学者咨询，之前参与过其他国际标准化活动但未被选中进行标准化的算法是否可以参与NGCC。

按照《公钥密码算法提交要求》，NGCC 不排斥之前参与国际标准化活动但未被选中的算法提案，同时期待收到有进一步创新的算法提案。

三、关于算法安全强度等级要求

有专家学者关注公钥密码算法安全强度等级要求，建议增加 192 比特安全强度作为可选项，询问要求 512 比特安全强度的考虑。

考虑到未来技术的发展，256 比特会逐渐成为新一代商用密码应用的主流经典安全强度等级。为给未来的高安全需求应用预留发展空间，因此提出 512 比特安全强度等级需求。另一方面，ICCS 统筹考虑了公钥、杂凑、分组等 3 类算法的安全强度体系设置，以保障未来的配合应用。因此，NGCC 重点考虑 256 比特和 512 比特两个级别，不考虑 192 比特安全级别。同时考虑到算法迁移过渡期间，新一代公钥密码算法与现用商用密码算法匹配使用需求，对公钥密码算法单独提出了 128 比特安全强度的设计要求。

四、关于算法量子与经典安全强度级别的关系

有专家学者关注公钥密码算法量子与经典安全强度级别的关系，建议以量子安全强度作为算法安全等级度量依据，建议将 128 比特经典安全强度对应 80 比特量子安全强度改为对应 128 比特量子安全强度。

目前，公钥密码算法抗量子计算攻击的安全强度评估存在很大的不确定性。相比而言，经典安全强度的研究时间更长、更为充分，因此更为稳定。NGCC 采用经典安全强度刻画算法的安全强度级别要求，同时给出相应量子安全强度要求。基于不同技术路线设计的算法安全强度差异较大，因此 NGCC 设置了一组普适的安全强度下限要求，并将对算法的安全冗余进行评估。

另外，NGCC 仅对公钥密码算法有 128 比特经典安全强度等级的征集需求，相关算法主要用于迁移过渡中与现用 128 比特经典安全强

度的分组密码算法、密码杂凑算法配套使用，80 比特量子安全强度已能满足与相关对称算法的配用需求。

五、关于时间复杂度和空间复杂度

有专家学者建议定义算法安全强度时，应同时考虑已知攻击的时间复杂度和空间复杂度。

ICCS 采纳了该意见，将《公钥密码算法提交要求》中已知攻击的“时间复杂度”改为“复杂度”，以涵盖时间复杂度和空间复杂度。

六、关于解封装错误率

有专家学者建议明确解封装错误率要求。

《公钥密码算法提交要求》已关注到解封装错误率。NGCC 将结合具体技术路线及相关数学问题对算法的错误率进行评估，并分析错误率对算法安全性的影响。

七、关于密钥交换协议的提交要求

有专家学者指出《公钥密码算法提交要求》关于密钥交换协议的要求“密钥交换协议应包含通信双方的初始化算法、生成和交换消息算法”，描述不够准确，建议修改。

ICCS 采纳了该意见，将其修订为“密钥交换协议应包含通信双方的初始化算法、消息生成算法和共享秘密密钥派生算法”，并调整了编程接口。

八、关于密钥交换协议的设计方法和安全模型

有专家学者询问是否考虑静态-静态密钥交换协议，以及是否可以使用 IND-AA 等其他安全模型。

为丰富算法体系多样性，NGCC 未对密钥交换协议的设计方法进行限制，可基于小尺寸密钥封装机制构造，也可直接设计。NGCC 也

未对密钥交换协议的安全模型进行限制，但将对安全模型的合理性、证明的正确性进行评估。ICCS 期待静态-静态密钥交换协议提案，以及具有创新性和适用于各类应用场景的密钥交换协议提案。

九、关于算法中使用的分组密码算法

有专家学者询问 MPC-in-the-Head 数字签名算法设计是否可以自主选用分组密码算法。

NGCC 允许自主选择或设计分组密码算法作为公钥密码算法的组件，但须给出对其安全性的假设和分析。NGCC 将对算法提案进行综合评估。

十、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《公钥密码算法提交要求》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。

十一、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。

十二、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，建议可扩展输出函数（XOF）应支持输出“任意”长度。

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。ICCS 采纳了建议，修改了辅助程序中的可扩展输出函数，使其可以生成“任意”指定长度的输出值。

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。