《密码理论与技术丛书》第二批选题申请指南

为建设世界一流密码强国，汇聚密码学方向优秀人才力量，系统总结国内外前沿密码理论与应用技术，持续推动我国密码学科发展，培养更多优秀密码科研和技术人才，密码科学技术国家重点实验室正在牵头组织出版《密码理论与技术丛书》(以下简称《丛书》),该丛书由科学出版社出版,并被国家新闻出版总署列为“十四五”国家重点图书出版规划项目。此前,《丛书》已完成第一批图书选题,包括公钥加密、同态密码、属性密码、云计算安全、格公钥密码、安全多方计算、侧信道分析与防御、非线性序列、抗泄漏密码、区块链密码、密码算法工作模式等16个方向。现面向全国高等学校、科研院所和其它相关单位科研人员征集《丛书》第二批图书选题,经评审通过后纳入《丛书》,并资助图书出版经费。本批次重点资助方向包括但不限于以下方向:

1. 现代密码学数学基础。包括有限域、数论、格理论等，给出其在密码学中的应用示例。

2. 现代信息论。包括熵及其度量、信道容量与数据压缩、网络信息论、量子信息理论等。

3. 密码学中的计算复杂性理论。包括与密码学相关的经典计算复杂性理论、量子计算复杂性理论等。

4. 密码学中的可证明安全理论。包括密码算法、密码协议的可证明安全概念、模型、构造技术等。

5. 密码协议形式化分析方法。包括密码协议的形式逻辑方法、模型检测方法、定理证明方法等，介绍较为成熟的形式化分析工具及其最新进展。

6. 密码算法自动化分析技术。包括常用的组合优化数学模型及其求解器，基于 MILP/SAT/SMT/CP 模型的自动分析技术，分析技术涵盖但不限于差分、线性、积分、中间相遇、猜测确定攻击等。

7. 纠错码理论及其在密码学中的应用。包括纠错码基本理论、一般线性码主流译码算法及其复杂度分析、基于纠错码的抗量子公钥密码等。

8. 基于量子机理的密码技术。包括量子密钥分发、量子随机数的生成机理、关键技术、检测方法等，应包含目前主流 QKD 和 QRNG。

9. 数字认证技术。包括数字证书认证体系、各种数字认证方法、数字认证服务等。

10. 密码工程。包括密码算法、密码协议、密码资源管理的实现、优化，以及在各类通信、网络及信息系统中的应用等。

11. 密码高效安全实现技术。包括对主流及新型密码算法和安全协议的实现技术，针对其在高性能、资源集约、实现安全等方面的应用需求，包括但不限于椭圆曲线密码实现技术、格公钥密码

实现技术等。

12. 密码芯片设计与防护技术。包括主流和新型密码算法、密码协议、密码运算模块的芯片设计与防护技术。

13. 密码测评与认证技术。包括对主流的密钥管理、密码算法、密码协议、密码芯片、密码设备、密码软件、密码系统等的功能、性能、安全性分析测评方法、测评技术、相关标准要求等，密码产品认证相关理论及其进展。

14. 密码算法的量子安全性。包括公钥密码、对称密码、Hash 函数等密码算法的量子可证明安全技术、量子分析算法和量子安全强度评估模型等。

15. 认证加密体制。包括认证加密结构与模式的可证明安全理论，认证加密算法设计理论和专用分析技术，以及 CAESAR 和 LWC 等竞赛中涌现的新设计方法、分析方法和实现评估的总结归纳等。

本次图书选题恪守宁缺毋滥原则，不支持重复出版的项目，征集截止时间为 2022 年 7 月 31 日，每项选题支持经费不超过 6 万元，申请人须按规定格式撰写《密码理论与技术丛书》选题申请表，并于截止日期之前提交至邮箱 sklc@sklc.org。

联系人：徐老师

联系电话：(010)-82789199