《密码理论与技术丛书》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拟牵头组织出版《密码理论与技术丛书》。现面向全国高等院校、科研机构和其它相关单位密码科研人员征集《密码理论与技术丛书》图书选题，经评审通过后，我室将该图书纳入《密码理论与技术丛书》，并进行出版经费资助。本次将重点资助但不限于以下十四个方向：

1. 属性密码学。包括属性基密码的研究背景、相关概念和模型、近年来的突破性进展；属性基密码的构建技术、以及各类扩展和衍生技术。
2. 同态密码学。包括典型的同态加密、同态签名方案和构造方法；单同态加密、类同态加密和全同态加密介绍；线性同态签名、类同态签名和全同态签名介绍；其他同态密码学术界关注的热点研究问题等。
3. 可搜索密码学。包括密文检索需求、对称可搜索加密和非对称可搜索加密技术；密文数据库检索技术、范围查询技术、高维数据检索技术等。
4. 标识密码学。包括标识密码学的起源、发展以及基本方法；基于双线性对等的加密、签名及密钥协商、高效的双线性对实现；格基标识密码、标识密码的标准和应用等前沿技术。
5. 格公钥密码学。包括格基础知识；典型格加密（密钥封装）、签名和密钥交换体制介绍；格公钥密码设计实用化轻量化技术；格公钥密码分析及安全性评估等。
6. 密钥管理技术。包括密钥管理基础知识；基于对称密码、非对称密码以及物理安全的密钥建立；数字证书技术；动态群组、移动网络、多方计算环境下的密钥管理等。
7. 安全外包计算。包括安全外包计算中的安全威胁和安全需求；安全外包计算中的一般安全技术和基本计算模块；具体应用中的安全外包计算解决方案等。
8. 非线性序列。包括整数剩余类环上导出序列的经典结论以及近十年来的主要研究进展；带进位反馈移位寄存器序列、非线性反馈移位寄存器序列等的密码学性质及近十年的主要研究进展。
9. 侧信道分析与防御。包括现有主流侧信道分析方法的分析原理、实验环境、典型案例分析等；现有主流侧信道防御方法的原理和特点，比较总结不同防御方法面对的应用需求、资源性能影响、对应分析方法、安全性级别等。
10. 密码学与区块链。包括密码学与区块链原理、区块链技术架构与发展；哈希函数、数字签名、密码协议在区块链中的应用；区块链中高级密码学原语与协议等。
11. 安全多方计算。包括安全多方计算的各类模型及其可证明安全理论，所涉及的主要密码学工具；典型的安全多方计算协议，包括混淆电路方法和秘密分享方法；安全多方计算的实用化技术和具体应用。
12. 抗泄漏密码学。包括抗泄漏密码的基本概念及基础理论、密码侧信道泄漏理论模型；抗泄漏流密码各类构造、安全证明方法、实现方案；保密电路、抗泄漏公钥密码等。
13. 椭圆曲线离散对数（ECDLP）问题。包括椭圆曲线基础知识；ECDLP及相关变形问题；ECDLP经典通用求解算法；特殊曲线上离散对数问题求解算法；ECDLP问题量子求解算法等。
14. 密码函数。主要包括密码函数基础知识、单输出密码函数、多输出密码函数以及密码函数在序列设计中的应用等。

本次图书选题不支持重复出版的项目，征集截止时间为2021年2月8日，每项选题支持经费不超过4万元，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:xuxx@sklc.org。

联系人：徐老师

联系电话：(010)-82789199