密码科学技术国家重点实验室开放课题
2022 年度申请指南

本着“开放、流动、联合、竞争”的建设方针，密码科学技术国家重点实验室面向全国高等院校、科研机构和其它相关单位设立开放课题基金，支持密码及相关交叉领域的基础性和前沿性研究，欢迎并鼓励多个团队就某一方向联合申请。申请方向及研究内容如下（申请人可以对申请方向的部分研究内容开展研究）：

1. 抗量子公钥密码理论与技术

探索抗量子密码设计理论，提出新型的抗量子密码算法；针对格、多变量、编码等主流抗量子密码困难问题，研究量子安全强度评估模型；研究基于格、基于编码、基于多变量、基于杂凑函数、基于同源等现有抗量子密码算法的分析、测评和快速软硬件实现技术；研究高效抗量子零知识证明协议、身份认证协议；研究抗量子密码在密钥重用和随机数重用等环境下的安全性；研究抗量子密码的侧信道分析与防护技术；研究设计新型公钥密码认证体系，支持与传统密码技术的无缝融合和抗量子公钥密码迁移。

2. 新型对称密码理论与技术

2.1 研究设计面向 5G、全同态加密、零知识证明、安全多方计算等新应用环境的序列密码、可调分组、认证加密和杂凑函数等实用化密码算法；研究面向硬件指令集的新型对

称密码设计技术；研究针对 SM3、SM4 的新型工作模式，实现安全增强或高效随机数扩展等功能；研究具有较好密码学指标的新型对称密码组件。

2.2 研究和评估 SM3、SM4 和 ZUC 等国产对称密码算法的量子电路实现和量子攻击复杂度，给出具体的量子电路深度和门数等关键指标；研究提出对称密码分析相关的 MILP、SAT、CP 等模型的高效求解算法；研究提出适用于基于大规模 S 盒（8 比特及以上）的对称密码算法的自动化搜索方法，探索对称密码自动化设计与分析新技术。

3. 量子密码和量子通信技术

研究 QKD 协议现实安全模型和测试评估技术；研究高成码率 QKD 共纤技术，实现与经典密码通信的共纤应用；研究量子网络中继节点动态可信认证技术；研究量子随机数理论安全分析模型和安全评估准则；研究器件无关、半器件无关等量子随机数生成方案、提升效率和稳定性的方法及技术；结合特定应用场景，研究抗量子密码算法与 QKD/QRNG 应用融合技术。

4. 新型密码协议设计理论与技术

研究针对密钥泄露、设备篡改、内部状态泄露等场景下的密码协议安全设计与安全证明技术；研究信息论安全 MPC 协议的通信复杂性；设计预处理模型下具有低通信复杂度、恶意安全的 MPC 协议；研究适用于隐私保护机器学习的高

效 MPC 协议；研究 OT 协议及其他 MPC 协议基础组件改进和快速软硬件实现技术。

5. 人工智能与密码技术的融合

研究基于人工智能的密码设计与分析技术；研究基于人工智能技术的随机性检测与评估方法；研究人工智能与侧信道分析融合技术，提出系列先进的侧信道分析新方法；针对人工智能应用中的数据/模型的保密性、隐私性、完整性等，提出基于密码技术的高效解决方案。

6. 新应用环境下密码应用技术

针对大数据、区块链、边缘计算、物联网等新应用环境，研究提出或实现与 SEAL、Helib、HEAAN 等开源库具有可比较性能的全同态加密算法；研究支持同态密码计算的高效可验证计算技术；研究多密钥同态加密算法，探索多用户数据密码协同计算和验证技术；研究基于属性密码的访问控制技术，探讨如何将属性密码应用于大数据环境的数据机密性保护、细粒度访问控制和密钥管理等方面，提出在数据库安全防护、云存储等场景下的属性密码应用方案；研究支持匿名和高效证书撤销的车联网 V2X 数字证书服务技术体系。

7. 密码芯片及侧信道防护技术

研究针对国密算法的密码芯片快速实现技术；研究格密码中矩阵乘法、NTT 等基础运算的芯片实现技术；研究针对资源受限环境下的芯片随机数生成技术；研究密码芯片侧信道主动对抗技术，以及侧信道安全建模和形式化验证技术。

8. 密码学困难问题求解算法研究

提出对大整数分解、离散对数、格问题、多变量问题等现有主流密码学困难问题的更优求解算法；探索提出新的困难问题并给出密码学应用；提出针对特定密码学困难问题的新型量子算法。

9. 其他探索性密码研究问题

鼓励申请人探索新型密码基础理论和应用技术，选择该方向需申请人阐明研究问题的新颖性、原创性和可行性。

本次开放课题起始时间为 2022 年 7 月，面上课题研究周期一般不超过 2 年，支持经费不超过 10 万元；重点课题研究周期可根据研究内容确定，一般为 2~4 年，支持经费根据研究内容和预期成果的不同，一般为 20~40 万元。

开放课题申请受理于 2022 年 5 月 4 日截止，申请人须按规定格式撰写《密码科学技术国家重点实验室开放课题申请书》，并于截止日期之前在开放课题申请系统内在线提交。

联系人：徐老师

联系电话：(010) 82789199

邮箱：fund@sklc.org