密码科学技术国家重点实验室开放课题
2021 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. 实用密码算法设计、分析与安全性评估

1.1 竞赛分组密码算法分析与改进。对全国密码算法设计竞赛优胜分组算法进行安全性分析评估，给出相关密钥类攻击、不变子空间类攻击、交换攻击、基于可分性质的立方攻击等分析方法的安全性分析评估，研究密钥扩展算法、弱密钥特性；研究竞赛算法的改进方案或快速软硬件实现技术，给出多种平台的软硬件实现。

1.2 竞赛公钥密码算法分析与改进。对全国密码算法设计竞赛优胜公钥算法进行安全性分析评估，研究算法的经典和量子可证明特性，给出紧致的安全证明；研究提出底层困难问题的经典和量子计算复杂度评估模型，给出具体参数下的安全评估结果；研究竞赛算法的改进方案或快速软硬件实现技术，给出多种平台的快速软硬件实现。

1.3 新型序列密码算法设计、分析与实现。研究新型序列密码算法设计，深入研究有限扩域上可并行、长周期、伪随机、易扩展的 LFSR 和 NFSR 源构造，研究实现速率、安全性可与 AES 轮函数匹敌的新型底层模块，给出新算法组件选取的优势证明；研究适用 128/256 比特大输出的安全、高效认证方案；给出相关攻击、猜测确定攻击、选择 IV 攻击等常用方法或新方法的安全性分析评估，分析新算法结构特性并给出安全性证明，研究快速软硬件实现技术，给出多种平台的软硬件实现，并根据相关结果优化算法设计。

2. 大数据密文检索、计算、访问控制等关键技术

2.1 大数据密文检索技术。研究安全、实用的密文检索技术，包括可搜索加密、数据库加密检索等，使之能够适应密文全文检索、关键词 Top-K 检索、密文模糊检索、复杂查询模式等需求，并从安全性、查询效率和适用范围等角度进行分析评价。

2.2 全同态加密技术与应用。研究提出或实现与 SEAL、Helib、HEAAN 等开源库具有可比较性能或针对特定应用具有明显优势的全同态加密方案；开展基于全同态加密的密文计算应用研究，提出针对特定应用和场景的可实用解决方案；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。

2.3 属性基加密技术与应用。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，设计高效实用、可证明安全的抗量子属性密码算法，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。

3. 基于人工智能的密码技术

3.1 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密码算法/协议设计分析方法；研究基于人工智能技术的随机性检测与评估方法。

3.2 基于人工智能的侧信道分析与防护技术。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，突破经典侧信道分析难以高效实现的伪操作识别、信噪转换等问题，给出密码芯片全方位、立体化的侧信道攻击与测评方案。

3.3 人工智能与密码系统融合技术。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，研究针对人工智能应用中的安全需求，研究基于GPU/TPU/FPGA 等计算器件的密码算法及工程实现。

4. 抗量子密码的基础理论和实用化技术

提出新型密码学友好的抗量子困难问题，并研究其与标准数学困难问题的关系，提出密码困难问题的量子安全强度评估模型；探索抗量子密码设计理论，提出新型的抗量子密码算法；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、改进和快速实现技术；研究基于格的抗量子密码算法快速实现技术。

5. 新型对称密码理论与自动化设计与分析技术

5.1 新型对称密码设计理论与实用算法。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；研究提出更加安全高效的创新对称密码设计理论或框架；研究追踪NIST LWC 标准化征集中的新设计理念和新分析方法。

5.2 对称密码自动化分析技术前沿与应用。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；探索扩展对称密码自动化设计与分析技术，研究对称密码线性层及 S 盒的生成与优化实现，研究各类自动化分析方法适用性倾向和求解能力差异，研究提出适用于大规模基于 S 盒（8 比特及以上）的对称密码算法的自动化搜索方法；研究对称密码分析技术在量子计算模型下的应用；研究追踪对称密码统计检测分析的最新方法。

6. 安全多方计算理论与应用

研究信息论安全 MPC 协议的通信复杂性，证明其通信下界；设计预处理模型下具有更低通信复杂度、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 MPC 协议及其基础组件改进和快速软硬件实现技术。

7. QKD 和 QRNG 测评及应用融合技术

研究 QKD 协议现实安全模型和测试评估技术；研究 QKD 共纤技术，实现与经典密码通信的共纤应用；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。

8. 轻量级密码设计与应用技术

针对智能车联网，研究车内通信、车路通信、车云通信、车人通信等环节的轻量级密码协议关键技术；研究密码芯片硬件安全轻量化实现关键技术，探索密码芯片硬件安全测评技术。

9. 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，研究其“加速”特性并给出时间和资源复杂度。

10. 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 2021 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。

开放课题申请受理的截止日期为 2021 年 5 月 5 日，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基金申请书》，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