密码科学技术国家重点实验室开放课题

2018 年度申请指南

本着“开放、流动、联合、竞争”的建设方针，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. 密钥同态伪随机函数及其应用

构造基于LWE（Learning with Error）、LPN（Learning Parity with Noise）的可证明安全的密钥同态伪随机函数，并设计基于该伪随机函数的一些应用，如对称密钥代理重加密、分布式伪随机函数、可更新加密并用于不经意传输扩展等。

2. 抗量子攻击的伪随机数发生器及伪随机函数研究

构造可以抵抗量子计算攻击、低电路复杂度的伪随机函数、伪随机数发生器和随机性提取器；研究包括LWR（Learning with Rounding）等数学问题在内的几个常用问题在经典计算和量子计算下的安全强度；完善量子随机预言机模型的理论，并研究以上随机性构件和底层数学困难问题在该模型下的安全强度。

3. 密码学困难问题研究

对密码学中的一些基础理论问题：如大整数分解问题、离散对数问题、格困难问题、椭圆曲线同源计算、多变元代数方程组求解、纠错码译码等的困难性进行研究，给出更优求解算法；探

索提出新的困难问题并给出密码学应用。

4. **非交互零知识证明研究**

研究非交互零知识证明在各种安全模型下基于不同假设的高效构造；针对一些经典的非交互零知识证明，建立它们与可抽取单向函数之间的联系，探索利用非交互零知识证明构造可抽取单向函数；研究简洁非交互零知识证明（snark）的构造，探索snark在金融科技等方面的应用。

5. **安全多方计算的轮复杂性理论研究**

研究安全多方计算（MPC）协议的准确轮复杂性（交互的最优轮数）；突破自适应安全MPC协议的设计理论；针对在Plain模型下安全的MPC协议开展研究；研究达到最优轮数、且基于标准假设可证明安全的MPC协议。

6. **高效安全多方计算协议的设计**

研究在恶意敌手条件下高效安全多方计算协议的设计理论与方法，提出高效可证明安全的MPC协议并进行实验评估，在支持参与方的数量方面形成突破；针对常数轮的MPC协议开展设计与可证明安全分析，在MPC协议的通信与计算效率方面达到国际领先。

7. **低差分函数的性质与构造**

以“大APN（Almost Perfect Nonlinear）问题”为牵引，研究APN函数、PN函数和4-差分函数等低差分函数的映射性质，包括像集的代数和组合性质；给出APN置换性质新的刻画，争取推进“大APN问题”的研究及解决。在此基础上，分析蝴蝶结构及其推

广；研究低差分函数新的构造，尤其是构造代数次数大于2 的多项式APN函数和PN函数，构造同时具有高非线性度、高代数次数等良好密码学性质的低差分函数。

8. **抗侧信道攻击的掩码函数设计**

针对电磁泄漏攻击等侧信道攻击手段，研究可用于侧信道安全防护的高效掩码函数的设计；研究提出低重量高阶相关免疫的布尔函数的新型构造方法，并基于此设计能够有效抵抗d阶侧信道攻击的旋转S盒掩码函数。

9. **分组密码基础设计理论研究**

提出新型分组密码部件构造方法，给出一般环境下和资源受限环境下安全高效S盒、扩散层的具体构造；给出新型轮函数、密钥扩展算法等基础模块的设计准则；探索分组密码新型整体结构，设计高效简洁的分组密码算法。

10. **对称密码分析新理论新方法研究**

研究差分攻击、线性攻击等统计类分析方法的理论基础，验证其随机等价等假设条件的合理性、统计模型及复杂度分析的精确性，给出更加合理的密码分析模型；研究提出中间相遇攻击的可证明安全模型，提取密码算法抵抗中间相遇攻击的数值指标，进一步分析全轮AES算法；加强对典型序列密码的分析，关注Estream计划、Caesar竞赛最终入选算法、国际标准化序列密码算法、小状态序列密码算法等，给出新的分析结果；给出新的分组密码、序列密码、Hash函数、MAC设计等的安全性分析及评估方法。

11. 基于 NFSR 的序列密码设计与分析新理论、新方法研究

研究 NFSR 序列的密码学性质，提出 NFSR 组件设计方案；提出安全高效的以 NFSR 为基础组件的整体算法设计框架，对该框架下的组件参数选取提出具体要求；研究提出基于 NFSR 设计的序列密码的分析新理论、新方法，对具体 NFSR 序列密码算法进行分析；研究提出 NFSR 系统的输出函数序列的代数次数估计新方法。

12. 基于 MILP 的自动化分析技术研究

优化混合整数线性规划问题（MILP）模型的建模方法，挖掘 MILP 求解器的求解能力，提升 MILP 自动化分析技术的效率和精度，对某些对称密码算法的安全性进行分析。特别地：优化 ARX 型对称密码算法的差分传播模型、积分攻击和立方攻击的 MILP 建模方法，改进现有的攻击结果。

13. 密码方案量子安全模型及可证明安全技术研究

结合量子计算机的新型计算方式，研究不同密码方案针对量子计算机敌手的量子安全模型；研究量子安全模型和传统安全模型之间的关系；研究适合量子安全模型的新型安全证明技术；研究传统随机预言机模型下的抗量子密码方案在量子随机预言机模型下的安全性。

14. 量子算法及其应用研究

研究对 Shor、Grover、 Simon 等量子算法的优化和改进，探索其在更多经典密码上的应用；研究特定对称密码算法结构在量子计算模型下的安全强度及经典对称密码攻击方法在量子模型下的使用，给出复杂度低于理论安全界的攻击结果；研究评估

格、编码、多变量等主流抗量子困难问题的量子攻击加速及复杂度；设计新型量子算法，并将其应用到密码算法和数学问题的安全性分析；完善量子算法所需资源的评估模型。

15. **格公钥密码设计与分析**

研究格中各种困难问题，探索给出新型实用格及其困难问题设计；提出新型格公钥密码实用化关键技术，设计实用化格公钥密码方案，降低算法参数大小，提升安全强度；研究格密码方案的快速安全实现方法；研究格密码方案、格困难问题安全性分析评估方法；对已有的格公钥密码进行分析，给出攻击结果。

16. **测量设备无关类量子协议设计与分析**

研究并设计测量设备无关类量子协议，给出其安全性证明；研究针对测量设备无关类协议新的攻击方案，对特定测量无关类协议给出具体的攻击结果。

17. **结构化密钥协商协议及其应用研究**

利用结构化的思想，借助组合数学、代数几何、代数学与有限域等数学理论方法和技术，研究密钥协商的普适系统模型、高效构建方法以及（基于模型的)形式化安全证明等；研究提出新型密钥协商协议及其安全证明技术；设计安全高效的多用户会话密钥协商协议用于支持各种高安全性需求的交互应用环境。

18. **面向体域网的生物密码机制及认证与密钥分发协议研究**

研究适用于无线体域网的生物密码机制，设计基于生物密码的认证与密钥分发协议，使得其在安全性、模板长度和能量消耗

等指标方面能满足体域网需求，解决无线体域网采集的数据在传输过程中的隐私泄露问题。

19. 嵌入式设备中新型椭圆曲线算法安全与快速实现研究

以目前主流嵌入式芯片为对象，研究多精度乘法和模乘算法在其上的快速实现和优化；对不同类椭圆曲线（包括蒙哥马利曲线，扭曲爱德华兹曲线，GLV 曲线与 GLS 曲线）上的点操作进行详细的评估，提出优化的点加和倍点计算方法；研究标量乘算法的安全实现，能够防御主流的侧信道攻击；研究提出特殊类椭圆曲线的安全参数安全高效生成算法。

20. 可搜索加密若干关键技术研究

提出高效可验证密文检索系统框架和可验证密文索引结构方法，解决恶意服务器模型下检索结果的完备性验证问题；研究可支持非关系型数据库的可搜索加密技术，数据库文件的动态更新技术；研究针对可搜索加密的攻击技术等。

21. 外包数据存储与可验证更新关键技术研究

研究数据外包存储前的数据编码，防止外包服务器对数据进行破坏；研究数据外包存储后的完整性验证新方法，尤其是针对多用户共享数据外包情况下的新方案设计，解决其中的用户撤销问题；研究大规模数据库可验证更新技术，提出同时支持用户对数据记录的快速插入、删除、修改等全更新操作以及更新完整性校验操作的外包理论框架及更新方案；研究数据完整性遭到破坏后的赔偿机制。

22. 区块链中的新型密码理论和技术及其应用

研究适合区块链的新型密码理论和技术：如零知识证明、安全多方计算、环签名、群签名、混淆池等，保障基于区块链的各类复杂数字资产交易安全；研究基于区块链技术的异构物联网跨域认证技术，建立异构物联网密钥管理架构和具体操作模式。

23. 可证明安全的密码芯片防护方法

从可证明安全的角度提出芯片防护方法，从而有效解决传统防护方法存在的问题。研究可以抵抗差分故障、有偏故障攻击的可证明安全防护方法；研究可以同时抵抗能量分析与故障注入攻击的可证明安全综合防护方法与电路实现技术等。

24. 密钥泄漏容忍和防篡改保护机制研究

针对非可信环境下的密钥泄漏和被篡改等问题，设计连续密钥泄漏环境下的高泄露容忍和篡改检测发现的密钥保护机制；研究随机数提取器、不可延展编码(non-malleable codes)等工具在其中的应用。

25. 新型侧信道攻击方法及技术

研究对现有侧信道攻击技术的组合攻击技术；研究提出新型侧信道攻击方法及分析结果；研究 Flush+Reload 等软件侧信道攻击技术并给出具体密码算法攻击；设计具有鲁棒性的建模方法，提出新型的模板攻击技术，扩大模板攻击范围。

26. 基于人工智能技术的密码设计及分析

研究人工智能技术在侧信道分析中的应用，重点研究基于大数据的功耗、射频等侧信息样本归集、特征工程、自动化分析模

型训练等；研究利用人工智能方法对因特网中密码算法及密码协议进行嗅探分析的技术，提取更多有效信息；研究人工智能技术在格基约化算法中的优化应用，探索人工智能技术在密码分析中更多应用；探索利用人工智能技术对密码组件进行设计的方法和技术。

本次开放课题起始时间为 2018 年 5 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确定，一般为 20-40 万元。

申请受理的截止日期为 2018 年 3 月 26 日，申请人须按规定格式填写《密码科学技术国家重点实验室开放课题基金申请书》，并加盖单位公章，纸质版一式 2 份，于截止日期之前（以邮戳或发件日期为准），邮寄到下面的通讯地址，电子版及附属材料发送至以下邮箱。

联系人：谢老师

联系电话：(010)-82789199　　邮箱：xuxx@sklc.org

通讯地址：北京市 5159 信箱，密码科学技术国家重点实验室，100878