

先进密码技术与系统安全四川省重点实验室

2021 年度开放课题申请指南

先进密码技术与系统安全四川省重点实验室（以下简称“本实验室”）坚持“开放、流动、联合、竞争”的运行机制，为吸引和聚集国内高水平研究人员来本实验室开展合作研究与学术交流，共同提高本实验室研究水平，根据《四川省重点实验室建设与运行管理办法》和依托单位的相关管理规定，设立本实验室开放课题。现将《先进密码技术与系统安全四川省重点实验室 2021 年度开放课题申请指南》发布如下。

一、资助对象

本实验室开放课题面向国内开展先进密码技术与系统安全技术研究的高等学校、科研机构、产业部门等单位开放，凡以上单位中具有博士学位或中级以上专业技术职称的科技工作者，均可提出资助申请。同时，本实验室接收国内研究人员自带课题或经费，利用本实验室设备开展科学研究。

二、开放课题重点资助研究方向

根据本实验室的研究任务，本年度主要资助以下方向的研究：

1. 实用量子密码协议的研究与安全性分析

（1）噪音环境下的量子密码协议研究；

- (2) 设备无关的量子密码协议研究；
- (3) 资源受限情况下的量子密码协议研究；
- (4) 量子密码协议的安全性分析模型研究与应用。

2. 量子计算与人工智能研究

- (1) 量子人工智能算法及模拟电路研究；
- (2) 量子人工智能隐私保护研究；
- (3) 量子安全计算及量子人工智能安全。

3. 经典密码算法的量子分析方法研究

- (1) 对称密码算法的量子分析方法研究；
- (2) 非对称密码算法的量子分析方法研究；
- (3) 密码分析的量子算法实现线路及优化。

4. 侧信道分析与终端安全

- (1) 密码安全芯片侧信道攻击技术研究；
- (2) 人工智能在侧信道攻击中应用研究；
- (3) 密码安全芯片防御技术研究；

5. 工业控制系统模型与应用安全

- (1) 工业控制系统的漏洞识别和威胁建模研究；
- (2) 基于深度学习的工业控制系统防御模型研究；
- (3) 工业控制系统安全态势评估模型研究；
- (4) 工业控制系统安全能力验证研究。

6. 智能制造与工业互联网安全

- (1) 工业数据隐私保护及工业互联网安全研究；
- (2) 安全生产及智慧工厂安全研究；

(3) 智能主动控制与安全研究。

7. 人工智能系统安全

(1) 人工智能框架脆弱性分析与研究；

(2) 人工智能样本安全性研究；

(3) 人工智能算法安全性增强技术研究。

三、申请办法

申请人根据本实验室申请指南中的研究内容，自行选择前沿课题，在申请截止时间（2021 年 10 月 15 日）之前填写并提交《申请书》（一式肆份）及电子版。

申请人提出的项目申请，由本实验室学术委员会进行评审，评审结果于 2021 年 11 月 15 日前公布并通知申请人。获得资助的申请人自动成为本实验室访问学者。为了鼓励申请人与本实验室研究人员开展合作，本实验室在同等条件下优先资助有合作基础的申请人员。

申请人要遵守科学道德，以严谨的科学作风和实事求是的科学精神填写开放课题申请书，保证申请书的真实性，避免出现夸大和不准确的内容。

四、开放课题管理

1. 开放课题执行期限一般为 2 年，资助额度平均每项 10 万元人民币。项目经费根据研究进度，分三次划拨，分别为：立项后（30%）、中期检查（30%）、验收后（40%）；

2. 课题类型分为重点、一般、自筹三类；除自筹课题外，重点课题和一般课题的资助金额分别为 10 万元和 5 万元每

项；

3. 课题管理由本实验室负责实施。更详细的课题管理办法，请参阅《先进密码技术与系统安全四川省重点实验室开放课题管理办法》。

4. 课题预期成果至少同时包含：

（1）发表 SCI 期刊三区及以上论文 1 篇；

（2）申请发明专利 1 项（须进入实审）。

5. 本实验室组织专家按照研究计划对项目实施阶段检查。项目负责人需向本实验室提交年度研究总结报告和中期总结报告，并在本实验室学术年会上进行汇报。项目结题时，由学术委员会对项目完成质量和学术水平进行评价。

6. 课题如无法按期完成或要求更改计划，须提前提出书面申请，由本实验室学术委员会做出处理决定。对于进展不良或不按本实验室有关规定执行的课题，经本实验室主任批准，可以中断该课题资助或收回原批准的课题经费，并将情况进行公开通报。

7. 由本实验室开放课题资助课题所获取的研究成果（包括论文、报告、著作、专利等）归本实验室与申请者所在单位共享，并共同署名。中文单位署名“先进密码技术与系统安全四川省重点实验室”；英文单位署名“Advanced Cryptography and System Security Key Laboratory of Sichuan Province”。发表论文时，均需注明“先进密码技术与系统安全四川省重点实验室开放课题资助项目 XXX 号”或“This work

was supported by the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province (Grant No. xxx)”。专利的权利人需包含本实验室。

五、联系方式

联系人：吴老师

地 址：四川省成都市西南航空港经济开发区学府路一段 24
号（先进密码技术与系统安全四川省重点实验室）

邮 编：610025

电 话：028-85966648

E-mail: acsskl @cuit.edu.cn

先进密码技术与系统安全四川省重点实验室

二〇二一年九月