**浙江大学区块链与数据安全全国重点实验室**

**2024年开放课题申请指南**

浙江大学区块链与数据安全全国重点实验室面向“加快构建数据基础制度”和“区块链自主创新”的国家战略，聚焦技术自主可控、数据隐私安全、可信数字赋能的关键目标，突破安全完备、监管充分的数据安全与区块链原生理论，构建隐私安全、自主可控的技术体系，研制系统及科学装置。实验室坚持“求是、创新、交流、开放”，诚挚邀请国内外相关领域的研究人员申请开放课题资助。

开放课题分为重点课题和一般课题两类，重点课题的资助额度为10万元，一般课题的资助额度为4万元，研究周期一般为1到2年。实验室将根据申请情况均衡各方向资助项目数量。

国内外高等院校、研究院等具有博士学位或中级及以上专业技术职称的研究人员均可提出申请，无在研的实验室开放课题。欢迎并鼓励多个团队就某一方向联合申请。

校外人员申请的开放课题采用双负责人制，在提交申请书之前，请联系一名实验室固定成员作为课题校内负责人，且申请人在资助期内须来实验室、与课题校内负责人共同开展一定时间的合作访问研究（差旅费用由开放课题经费承担）。受实验室开放课题资助的发表成果（包括论文、申请专利或报奖等），作者单位必须署上“浙江大学区块链与数据安全全国重点实验室”单位名称（英文为“The State Key Laboratory of Blockchain and Data Security，Zhejiang University”），并在致谢里写“This work was supported by the Open Research Fund of The State Key Laboratory of Blockchain and Data Security，Zhejiang University”。开放课题的管理及验收要求，可查阅《区块链与数据安全全国重点实验室开放课题管理办法》。

2024年实验室开放课题拟资助的研究方向（但不限于）：

* 高效、安全的联邦问答关键技术
* 面向大规模数据的可验证索引优化技术研究
* 去中心化在线优化的最优算法研究
* 融合智能设备的数据可信通信技术研究
* 链上链下协同的可信查询与溯源确权关键技术
* 大模型安全防范护栏研究及合理化评估
* 多元化敏感图像生成技术
* 高逼真对象-场景融合视频伪造技术
* 高阶自动驾驶系统预期功能安全评测技术研究
* 智能车V2X网联功能的安全评测技术研究
* 面向智能车数据安全的攻击技术研究
* 抗量子安全的门限签名
* 后量子安全的隐私信息检索协议
* 面向大模型微调的差分隐私数据保护技术研究
* 区块链TEE安全性的形式化验证方法研究
* 复杂环境下低轮数零知识证明协议研究
* 基于开源鸿蒙的函数级软件供应链漏洞检测技术研究
* 基于开源鸿蒙的网络黑灰产数据检测与治理技术研究
* 面向数据泄漏的诱导式黑灰产情报获取技术研究
* 基于人工智能的标准漏洞数据集构建及智能化漏洞检测技术研究
* 区块链智能合约漏洞挖掘技术研究
* 基于大语言模型的智能合约修复技术研究
* RWA隐私保护技术研究
* 公有链区块高性能执行技术研究
* 数字资产交易监管辅助技术研究
* 全同态加密技术研究

所申请的开放课题将本着“公平竞争、科学评审、择优支持”的原则，经专家评审、学术委员会审批通过后确定立项课题。请申请者认真填写《浙江大学区块链与数据安全全国重点实验室开放课题申请书》，于**2024年5月1日**前将申请书与相关证明材料电子版发送给联系人邮箱，并抄送给已沟通好的课题校内负责人。批准立项的课题会另行通知邮寄加盖公章的纸质版。

联系电话：13777887910 Email: sklbds@zju.edu.cn

[**附件：浙江大学全国重点实验室开放课题申请书**](http://www.cad.zju.edu.cn/uploads/soft/190916/5_1556007831.doc)