



附表 1

完成人合作关系说明

本项目完成单位为西安交通大学、支付宝(杭州)数字服务技术有限公司、武汉大学。三方共同组建了金融人工智能算法安全测评与防护平台研究团队,展开了长期紧密合作,取得了一系列研究成果。

本项目完成单位西安交通大学组建了以项目完成人沈超教授为带头人的研究团队。项目完成人沈超、蔺琛皓、李前、管晓宏均属于西安交通大学,以上完成人发挥学科与平台优势,共同承担关键技术的理论研究和技術发明,并配合合作单位实现核心技术对接、系统集成、测试与推广应用。在项目研究过程中,上述完成人联合承担项目、合作发表论文与联合申请专利。

本项目完成单位支付宝(杭州)数字服务技术有限公司,是领先的数字支付平台和金融科技企业,始终与西安交通大学、武汉大学保持紧密合作关系。双方自项目启动即开展深入合作,支付宝公司组建了由周俊技术负责人组成的研发与应用团队,共同开展了技术攻关、平台研制、产业应用与规模化推广,实现了多项创新技术的落地应用。

本项目完成单位武汉大学组建了以王骞教授为负责人的研究团队,重点参与物理世界对抗攻击漏洞检测技术的研发与系统实现工作。在项目合作过程中,西安交通大学、支付宝(杭州)数字服务技术有限公司与武汉大学三方共同开展关键技术研究、系统集成、应用示范与成果转化,建立了稳定的产学研合作机制,取得了显著的经济与社会效益。

第一完成人签名: 沈超



完成人合作关系情况汇总表

序号	合作方式	合作者/项目排名	合作起始时间	合作完成时间	合作成果	证明材料
1	共同知识产权	沈超（1）， 蔺琛皓（2）， 王骞（4）	2020年12月	2022年4月	发明专利-深度神经网络模型公平性测试方法、系统、设备及介质	A-4
2	共同知识产权	沈超（1）， 蔺琛皓（2）， 管晓宏（6）	2022年9月	2023年4月	发明专利-机器学习框架漏洞检测方法、系统、设备及可读存储介质	A-2
3	共同知识产权	蔺琛皓（2）， 沈超（1）， 管晓宏（6）	2021年1月	2023年5月	发明专利-深度学习模型对抗样本生成方法、系统、设备及存储介质	A-6
4	共同知识产权	沈超（1）， 蔺琛皓（2）， 管晓宏（6）	2022年9月	2023年3月	发明专利-机器学习框架漏洞API参数定位方法、系统、设备及介质	A-3
5	共同立项	沈超（1）， 蔺琛皓（2）， 李前（5）， 周俊（3）	2024年1月	2025年12月	国家重点研发计划战略性新兴产业科技创新合作项目-面向金融场景的人工智能算法安全测评与隐私增强技术	B-1
6	共同立项	沈超（1）， 蔺琛皓（2）， 李前（5）， 周俊（3）， 王骞（4）	2022年1月	2023年12月	工业和信息化部人工智能产业创新任务揭榜挂帅项目-面向金融场景的人工智能算法安全测评与防护平台	B-2

承诺：本人作为项目第一完成人，对本项目完成人合作关系及上述内容的真实性负责，特此声明。

第一完成人签名：/sk 8