软件学院导师团队与招生意向信息表

团队名称	智能计算与安全			团队负责人	刘哲
联系人	刘哲	邮箱	zhe.liu@zju.edu.cn	电话	18014814499
主要团队成员					
姓名	职称	研究方向		个人主页	
刘哲	教授	抗量子密码、大模型与智能体、人工智能安全、空天地海一体化计算		https://person.zju.edu.cn/0822187	
潘家雨	百人计划研究员	边缘计算及智能、量子计算、空天地海计算		https://jiayupan26.github.io/	
李振源	特聘研究员	系统安全、AI 驱动自动化攻防对抗、安全态势感知		https://li-zhenyuan.github.io/	
杜天宇	特聘研究员	大语言模型、人工智能安全		https://tydusky.github.io/	
团队介绍	团队现有教授/研究员 4 人，均有丰富的海外学习工作经历。团队负责人刘哲教授为国家高层次人才青年项目入选者、浙江省顶尖人才计划入选者、博士生导师。潘家雨研究员毕业于美国俄亥俄州立大学电子与计算机工程系，入选国家级青年人才计划。李振源研究员毕业于浙江大学计算机学院，期间在新加坡国立大学访问交流，曾在华为 2012 可信实验室任职，入选宁波市人才计划；杜天宇研究员毕业于浙江大学计算机学院，曾在美国宾夕法尼亚州立大学从事博士后研究工作。团队在 Nature Machine Intelligence、ACM Computing Surveys、IEEE Trans. TDSC、TIFS、TC、IoT、USENIX Security 和 AAAI、NIPS、ACL、ICCV、ICLR 等顶级期刊和会议上发表论文 200 余篇，刘哲教授获得了包括 “浙江省青年科学企业家”、“教育部计算机专业优秀教师奖励计划”、《麻省理工科技评论》中国区 “35 岁以下科技创新 35 人”、中国密码学会密码创新奖一等奖”和“阿里巴巴达摩院青橙奖”等多项奖励项。				
在宁波开展的研究方向	1. 量子软件与安全 - 抗量子密码高效实现 - 抗量子密码算法软硬件协同优化 - QKD 与 PQC 的敏捷迁移 2. 大模型与智能体技术 - 多模态大模型 - 多智能体技术 - 模型与智能体安全 - 垂域模型和智能体应用 3. 人工智能安全技术 - 对抗攻击与防御机制 - 大模型驱动的安全漏洞挖掘与防御 - 数据隐私保护与联邦学习 4. 复杂网络攻击建模与智能检测技术				

	- 基于主机的复杂网络攻击建模理论与方法 - 高级持续性威胁与入侵检测系统设计 - 实战化网络威胁分析与自动化溯源技术 5. 面向新一代通信与智能架构的网络科学优化技术 - 复杂信道下的信息新鲜度理论与智能采样优化 - 适应生成式 AI 大规模部署的边缘计算与网络协同调度 - 面向太赫兹通信等复杂场景的前沿量子网络传输架构
项目情况	团队负责人近年来主持浙江省顶尖人才团队计划以及国自然重点基金等 10 余项国家级/省级重点项目。团队与阿里、字节、华为、商汤、钉钉等企业有长期项目合作，此外与亚洲最大的火力发电厂-宁波北仑电厂在重要信息基础设施的“人工智能+”和量子安全达成项目合作；与物产中大、恒生电子、万事利、激智科技、中扬立库、七一五所、浙大邵逸夫医院等领域头部企业在垂域大模型和 AI 智能体方面开展项目合作。
团队与企业合作情况	团队与企业有长期项目合作，相关研究成果已经在阿里、华为、商汤、钉钉、恒生电子、激智科技、北仑电厂等头部企业落地应用，取得了良好的应用效果，建立了紧密的合作关系。
对学生的要求	1、志存高远、追求卓越，并能够持之以恒、攻难克艰；2、要求科研背景与团队的研究方向匹配；3、对科研和工程有浓厚的兴趣，有较强的动手能力；4、有 AI 实习经验或者论文发表经验者优先
团队可以在宁波开设专业课程情况	《后量子密码学》、《量子计算导论》、《智能计算导论》、《边缘计算》、《计算机视觉》、《可信人工智能技术》等