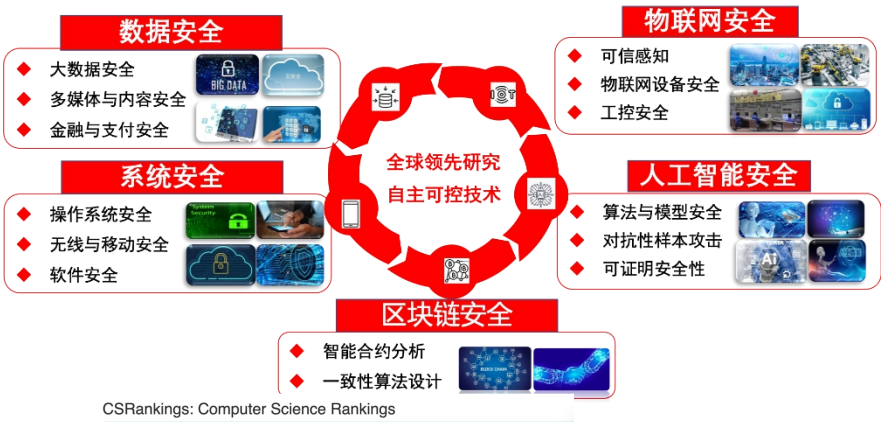
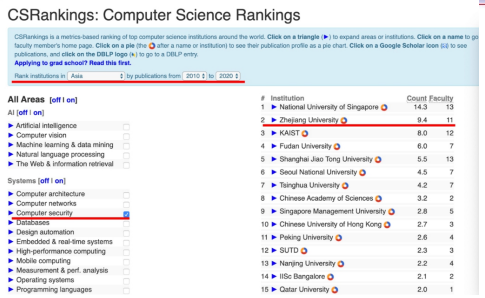
软件学院论文导师团队与招生意向信息表

团队名称	浙江大学网络空间安全研究中心			团队负责人	任奎
联系人	常瑞	邮箱	crix1021@zju.edu.cn	电话	18538038615
主要团队成员（论文指导教师要求是电子信息专业学位博导/硕导）					
姓名	职称	简介	研究方向		个人主页
任奎	教授	IEEE Fellow、ACM Fellow、博导	人工智能安全、数据安全、物联网安全与隐私保护		https://person.zju.edu.cn/kuiren
秦湛	百人计划研究员	博导	用户隐私保护、人工智能驱动的安全信息处理、人工智能安全、云安全计算、物联网安全		https://person.zju.edu.cn/qinzhan
周亚金	百人计划研究员	博导	软件安全、漏洞挖掘、操作系统安全、程序分析(基于源代码或者二进制)、体系结构安全		https://person.zju.edu.cn/yajin
韩劲松	教授	博导	物联网安全、智能手机安全、人工智能安全、网络安全、可信认证、隐私保护		https://person.zju.edu.cn/hanjinsong
林峰	百人计划研究员	博导	物联网安全，无线感知安全，移动传感，数字身份安全认证		https://person.zju.edu.cn/flin
张帆	教授	博导	硬件安全、系统安全、物联网安全、体系结构、密码学、人工智能安全		https://person.zju.edu.cn/fanzhang
张秉晟	百人计划研究员	博导	密码学、区块链、数据安全、安全多方计算、零知识证明		https://person.zju.edu.cn/bingsheng
申文博	百人计划研究员	博导	软件攻防，操作系统安全，容器安全，固件安全系统，安全，程序分析		https://person.zju.edu.cn/shenwenbo
卜凯	副教授	硕导	计算机网络与信息安全		https://person.zju.edu.cn/kaibu
吴磊	讲师		移动安全，系统安全，区块链安全		https://person.zju.edu.cn/lei_wu
常瑞	副教授	博导	嵌入式系统安全，设备固件安全，形式化分析与验证，边缘计算安全		https://person.zju.edu.cn/changru

				i
刘健	百人计划研究员	博导	应用密码学、分布式系统、区块链、人工智能	https://person.zju.edu.cn/jianliu
巴钟杰	百人计划研究员	博导	物联网安全、移动安全	https://person.zju.edu.cn/zhongjieba
赵永望	教授	博导	形式化方法、操作系统安全、安全关键系统	https://person.zju.edu.cn/zhaoyw
杨子祺	百人计划研究员	博导	人工智能安全，数据隐私，系统安全，移动安全	https://person.zju.edu.cn/yangziqi
王志波	教授	博导	人工智能安全、物联网、数据安全与隐私保护	https://person.zju.edu.cn/zhibowang
许海涛	百人计划研究员	博导	Web 安全、网络安全、在线欺诈检测、恶意软件检测	https://person.zju.edu.cn/haitaoxu
刘金飞	百人计划研究员	博导	数据市场、数据安全与隐私、数据查询	https://person.zju.edu.cn/jinfeiliu
卢立	研究员	博导	物联网安全、移动安全、普适计算、人机交互	https://person.zju.edu.cn/lynnlului
团队介绍	**主要情况介绍：** 浙江大学网络空间安全研究中心成立于 2017 年 9 月，依托计算机学院与控制学院、信电学院等共同建设网安一级学科。2019 年 4 月，批准成立浙江大学网络空间安全学院。目标定位是建设国内领先，国际一流的学科研究高地，高级人才培养基地，和产学研转化的典型示范。			

<table>
<tr>
<td></td>
<td>




中心研究方向分为数据安全、物联网安全、系统安全、网络安全、人工智能安全以及区块链安全六大方向。中心已初步形成了一支一流的科研与教学队伍，主要包括：图灵奖得主 Whitfield Diffie 教授（中心荣誉主任），IEEE Fellow 2 人，国防科技卓越青年人才基金获得者 1 人，“”青年项目入选者 1 人，浙江大学求是特聘学者 1 人、青年学者 1 人，浙江大学“百人计划”10 人在内的十余位优秀人才。中心教师大部分拥有海外博士学位，具有开阔的国际视野，广泛的海外科研合作以及坚实的科研基础。在 csrankings 计算机安全 computer security 排名中，浙江大学网络空间安全位居国内第一、亚洲第二。

中心高度重视科研人才培养，全程导师培养，稳步推进人才培养建设和网安一级学科的发展。从 2017 级开始以网络空间安全一级学科招收硕士和博士生，目前共招收硕士生超百人，博士生近 50 人。中心同时积极营造良好的软硬件环境，包括国际学术交流和良好的实验设备，每年邀请海内外知名网络空间安全学者/教授到校讲座 40 余场，同时成功举办连续三届网络空间安全西湖国际论坛等多场学术活动，极大扩大了浙江大学网络空间安全学科的国际影响力。当前中心科研经费充足，科研氛围浓厚，硕博士生有大量机会参与众多研究项目，展现个人能力，实现学术追求。
</td>
</tr>
<tr>
<td>实习项目情况</td>
<td>
基于可信软件硬件的安全多方计算（张秉晟）
小物体目标非侵入式探测与发现（韩劲松）
区块链安全（周亚金，张秉晟）
软件漏洞挖掘，修复，二进制代码分析（周亚金、常瑞）
新型软硬件一体化加密数据库（周亚金，任奎）
缓存旁路分析评估和 SGX 密码库安全实现（张帆，任奎）
合理攻击假设下的差分隐私保护机制研究（秦湛，任奎）
人工智能模型与算法攻击与防御技术（秦湛，杨子祺，任奎）
</td>
</tr>
</table>

	机器学习模型机密性与数据隐私（杨子祺，张秉晟，秦湛） 机器学习模型数字水印与后门植入（杨子祺，秦湛） 基于可信硬件的不经意随机访问及研究（张秉晟，任奎） 隐私集合求交分析研究与实现项目（张帆，张秉晟） 基于源代码的物理泄露自动化搜索（张帆） 基于软件仿真的人工智能网络实现抗故障攻击评估（张帆） 软件可触发的硬件漏洞利用技术研究（张帆） 软件定义网络中高效及安全的流量管控（卜凯） 新型多因子多模态生物认证技术（林峰，任奎） 物联网设备认证安全与攻击技术（巴钟杰，林峰，任奎） 基于毫米波的显示与语言攻击（林峰） 私有云安全形式化分析与证明技术（赵永望，常瑞） 操作系统的形式化验证技术（赵永望，常瑞） 新型编程语言与编译器设计（赵永望） 系统代码自动分析与验证（赵永望，常瑞） 基于机器学习的模型生成（赵永望） 操作系统新型防护机制，包含控制流和数据流（申文博） 基于 RISC-V 硬件的新型安全机制（申文博，周亚金，吴磊） 新型容器安全机制研究，包含 Docker 和 gVisor（申文博） WebAssembly 安全性分析和防护（申文博，周亚金） 基于微内核的新型操作系统安全架构，如鸿蒙（周亚金，申文博，常瑞，吴磊） 人脸图像数据隐私保护（王志波） 面向深度学习模型的可解释性和脆弱性研究（王志波，任奎）
对学生的要求	欢迎对安全感兴趣的同学