**网络空间安全研究中心团队情况介绍表**

|  |  |  |  |
| --- | --- | --- | --- |
| 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 瑞叶梦楠 | Email | crix1021@zju.edu.cn;yemengnan@zju.edu.cn | 电话 | 18538038615;15057168240 |
| **主要情况介绍：**浙江大学于2017年成立网络空间安全研究中心，2019年成立网络空间安全学院，负责网络空间安全一级学科建设，由校长吴朝晖院士亲自担任建设领导小组组长，由国际知名学者任奎担任院长，是国家首批网安一级学科博士学位授权点之一。浙江大学信安专业为教育部一流本科专业，在软科2021年排名中位列全国第一，在国际著名CSRankings安全领域最新排名与清华并列亚洲第一、全球第七。学院拥有一支活跃在国际学术前沿的年轻教师队伍，包括ACM/IEEE会士、国家创新人才入选者、高校计算机优秀教师和全军优秀教师等，院长任奎是安全领域亚洲唯一国际计算机学会会士当选者。学院现有院士（双聘）1人、教授5人、百人计划研究员15人、副教授3人、特聘研究员3人、博士后3人。其中1人获聘教育部科学技术委员会委员、教育部高等学校教学指导委员会委员，入选国家“千人计划”创新项目1人、“千人计划”青年项目2人、国家自然科学基金优青项目1人、海外优青项目1人、浙江省千人计划3人。学生培养成绩显著，在多个国内外著名安全比赛中获得冠军，包括首届“逐梦杯”中国青年芯片科技创新大赛一等奖，“龙芯杯”一等奖，打破CMU十余年的垄断获得Defcon CTF冠军，iDash国际比赛第一，强网杯冠军等。学院坚持以国家网络空间安全重大战略需求为导向，确立了数据安全与隐私、软硬件系统安全、人工智能安全、网络与通信安全四个研究方向。已建立中央网信办/教育部网络空间国际治理研究基地、浙江省区块链与网络空间治理重点实验室、移动终端安全技术浙江省工程研究中心等多个创新平台，并与华为、阿里巴巴、蚂蚁金服、浙数文化等企业成立多个联合实验室，以及浙江大学-华为系统和数据安全联合实验室、浙江大学杭州国际科创中心-浙报数字文化集团-浙江大学网络空间安全学院数字安全联合实验室、浙江大学-阿里巴巴网络空间安全联合实验室、浙江大学-蚂蚁集团金融科技研究中心-数据安全与隐私保护实验室、浙江大学-光通天下网络空间安全联合实验室等多个产学研协同的研究中心和创新基地，正在积极筹建区块链与数字安全全国重点实验室。近3年来，学院科研成果卓著，承担科技部“科技创新2030”重大项目、国家重点研发计划项目、工信部高质量发展专项等国家/省部级重大项目30余项，主导多项ISO、IEEE国际标准制定，参与多项安全相关国家标准立项，提升我国网安领域国际影响力与话语权；申请国际/国内专利70余个，获得授权21个；在国际顶级安全学术会议/期刊上发表论文200余篇，其中CCF-A类110余篇，获得19项杰出论文奖。承担了科技部首个人工智能安全重大研究计划项目；研发了零权限手机窃听技术受到有关部门、华为、谷歌等重视，提升了数十亿智能终端安全水平；研发了数字货币交易监控系统，构建了自主溯源和反洗钱研究体系，填补我国在这一领域空白；验证了一批国产操作系统和航空航天关键系统，获得首个国内最高等级的软件EAL5+级别证书，并在我国载人航天工程、国产高速列车系统中应用；提出的生物认证防伪技术，在华为鸿蒙操作系统中广泛应用。**导师简介：**1）任奎，教授/博导，中心主任。任奎是浙江大学求是讲席教授、ACM和IEEE会士，目前担任浙江大学网络空间安全学院院长、浙江省区块链与网络空间治理重点实验室主任，并曾担任纽约州立大学布法罗分校冠名教授及普适安全与隐私实验室主任。任奎教授是数据安全与隐私保护、物联网安全与认证、人工智能安全等领域的国际知名专家。他先后主持和参与了多项科技部、国家自然科学基金委员会、浙江省领军型创新团队、美国国家科学基金会、美国能源部、香港研究资助局、韩国国家研究基金会、华为、阿里巴巴、亚马逊等机构和公司的科研项目，研究成果在工业界有广泛应用。任奎教授获得了包括浙江大学首届国华杰出学者奖、IEEE通信分会安全技术委员会技术成就奖、纽约州立大学校长杰出研究奖、美国国家自然科学基金青年职业奖在内的一系列奖项。任奎教授发表了300余篇同行评议的期刊与会议文章，获得了多篇ACM/IEEE顶级会议最佳论文和时间考验论文奖。他的H-Index为84，文章总引用次数超过40,000次，并多次入选科睿唯安高被引科学家。任奎教授担任了多个国际权威期刊编委，国际一流会议主席。同时任奎教授担任了第八届教育部科学技术委员会委员、教育部高等学校教学指导委员会委员、IEEE计算机学会和通信学会会士遴选委员会委员、ACM亚洲计算机与通信安全会议指导委员会委员、ACM中国安全分会主席等学术职务。2）韩劲松，网络空间安全研究中心教授，博导，现任信息安全系系主任。2007年在香港科技大学计算机科学与工程学系获博士学位。研究工作主要集中在物联网安全、可信认证、智能感知和移动计算等方面。近年来在国际一流期刊与重要国际会议上发表论文70余篇；主持重点研发项目课题一项，国家自然科学基金区域联合基金重点项目课题一项、面上项目三项；担任中国计算机学会物联网、普适计算、教育专委会委员，学术期刊Computer Networks（COMNET）、网络与信息安全学报编委，以及多个国际一流会议的程序委员会委员，如MOBICOM、INFOCOM、SenSys、ICNP、IWQoS等；获2019 IEEE 信息通信年会（INFOCOM，CCF A类会议）最佳论文奖、2019年全球通信会议（GLOBECOM）最佳论文奖、2021年INFOCOM最佳论文提名奖、2021年ACM 嵌入式网络传感器系统(SenSys，CCF B类会议)最佳论文提名奖、2011年香港信息及通讯科技奖最佳研究与创新奖，获选“高校计算机专业优秀教师奖励计划”，2018年ACM 西安优博指导教师。3）赵永望，教授/博士生导师。担任移动终端安全浙江省工程实验室主任，工信部重大专项首席科学家，中国计算机学会(CCF)杰出会员，CCF系统软件专委、形式化方法专委和抗恶劣计算专委委员，国际ARINC653操作系统标准委员会成员等。主要研究方向包括操作系统安全、形式逻辑与验证、编程语言原理等。主持和参与国家自然基金重点项目、工信部重大专项、载人航天工程重点项目等二十余项，获省部级科技进步一等奖2项。主持/参与国家自然基金重点项目、工信部重大专项项目、核高基重大专项、载人航天工程、工信部物联网集成创新等国家纵向项目十余项，同时承担华为虚拟私有云形式化验证、蚂蚁金服分布式金融系统通用安全框架、华为云计算安全策略形式化验证、中兴通讯高速网络交换机嵌入式操作系统验证等企业合作项目十余项。提出了操作系统形式验证的系统性理论和方法，已应用到十多个国产操作系统和国外工业/开源操作系统中，显著提升国产系统的安全可靠性。设计并实现了面向多核并发系统的形式化编程语言CSimpl、多核系统形式化验证工具PiCore、面向信息安全评估的形式化建模与验证工具CCCert等。相关成果发表在ACM TOPLAS、IEEE TDSC等期刊和CAV、FM、TACAS等会议上。部分成果被美国波音、法国空客等认可纳入ARINC653国际标准，并受美国波音公司邀请加入ARINC653委员会，成为国内唯一的委员。研制的工具已应用到我国航空航天领域、多个操作系统厂商、华为、蚂蚁金服等，取得了显著的应用成效。任国际标准化组织 ISO/IEC JTC1 SOA 研究组组长、 国家信标委分委会委员，起草 4 项 ISO 国际标准、12 项国家标准。曾任新加 坡南洋理工大学高级研究员。4）张帆，教授/博导。2012年博士毕业于美国康涅狄格大学。2014年加入浙江大学信息与电子工程学院。2019 年加入浙江大学计算机科学与技术学院网络空间安全研究中心。近5年在网络安全、密码学、硬件安全、芯片设计、人工智能领域发表高水平论文100余篇，其中CCF-A/B会议期刊论文约50余篇。其中，2012年获国际会议COSADE最佳论文奖。2018 年获中国密码学会 ChinaCrypt 最佳论文奖。2019年获亚洲硬件安全年会 AsianHOST 最佳海报奖。2021年中国密码测评会最佳论文奖。2018 年以浙 江大学为第一单位在密码硬件安全领域顶级会议 CHES 上发表了高水平学术论文1篇，系浙江大学在该会议上被接收的第一篇论文。出版了《密码故障分析与防护》和《下一代电信网与服务的安全管理》两本著作。作为中国密码学会 专家组成员参与编写了《2014－2015密码学学科发展报告》。2020年担任嵌 入式系统安全证明国际会议PROOFS的程序委员会主席，并担任DAC、AsiaCCS、ICICS、SCC、SPACE、FDTC、AsianHOST、MASS、ICPADS 等重要国际会议的TPC成员。担任CyberSecurity等国际期刊的副编辑，并担任IEEE TIFS、TCAD、JoC 等顶级期刊的长期审稿人。目前承担8项科研项目，并担任其中6个项目的负责人，其中包含国家自然科学基金面上项目2项、武器装备预研项目1项、省部级武器装备预研基金项目（保密通信重点实 验室基金）、密码科学技术国家重点实验室重点基金项目、浙江省重点研发计 划等。主持完成研发了旁路攻击采集和分析平台；获军工科技进步奖二等奖1项。指导硕士生获得研究生国家奖学金2人次。指导硕士研究生参加2018和2019年“全国研究生创芯大赛”获全国一等奖1项，全国二等奖1项，专项一等奖2项，荣获优秀指导教师称号。指导本科生参加“全国大学生信息安全竞赛”获全国二等奖4项。5）王志波，教授，博士生导师，国家优秀青年科学基金获得者。2007 年毕业于浙江大学信息学院自动化专业，获学士学位；2014 年获美国田纳西大学诺克斯维尔分校计算机工程博士学位。曾任武汉大学计算机学院副教授和武汉大学国家网络安全学院教授，入选湖北省楚天学者和武汉大学武汉大学珞珈青年学者。现为IEEE/CCF/电子学会高级会员，CCF物联网专委会常委，电子学会物联网青年专技组常委，人工智能学会智能信息网络专委会常委，CCF大数据专家委员会委员，CCF网络与数据通信专委会委员，中国通信学会云计算与大数据应用委员会首届委员。主要研究方向包括人工智能安全、数据安全与隐私保护、物联网、边缘智能与安全。在网络与安全领域国际著名期刊和会议上发表论文100余篇，其中CCF 推荐的A类顶级期刊和会议论文40余篇、ESI高被引论文七篇。授权发明专利16项，公开发明专利10余项。主持与参与了多项国家自然科学基金、科技创新2030-新一代人工智能重大项目、973计划等国家级项目，并与华为、蚂蚁金服、阿里达摩院等公司有深度合作。担任INFOCOM、ICDCS、KDD、AAAI等多个国际著名会议的大会程序委员。荣获FUSION 2019国际会议最佳学生论文奖，IEEE HPCC 2019国际会议杰出论文奖，电子学会优秀科技工作者与先进工作者。6）周亚金，研究员/博导。研究兴趣是区块链智能合约安全、新型网络犯罪、软件安全、漏洞挖掘、操作系统安全等。2015 在美国北卡州立大学获得博士学位，随后担任奇虎 360 高级安全研究员。2018 年加入浙江大学担任百人计划研究员（博导）。他在安全顶级会议上发表多篇文章，其中包括安全 四大会议(CCS, S&P, USENIX Security, NDSS)文章 20 篇，他的文章引用数超过 8000 次，多次担任一流会议 (CCF-A 或者安全顶级会议)程序委员会委员并单位多个 CCF-A 类期刊审稿人。更多信息参加个人网站 http://yajin.org 。欢迎对软件安全、漏洞挖掘、区块链安全感兴趣同学报考，要求考生具有（以下一点）：熟练的程序编写能力，掌握常见漏洞挖掘和攻击方法，有过程序分析、区块链安全相关安全经验；对未知事物有好奇心（必须）。7）秦湛，研究员/博导。秦湛研究员从事数据安全与隐私保护、人工智能安全等领域的研究工作。在数据隐私保护领域，他参与了多个当今的研究热点方向，包括差分隐私下的数据共享、本地差分隐私保护的数据收集、社交网络中的差分隐私保护等，是国际上本地差分隐私研究的先行者之一；在云计算安全领域，他在包括图像特征提取、图像搜索与匹配等研究方向上提出并实现了一系列的创新理论方法与系统。主持/参与科技部重点研发项目课题、基金委区域联合重点项目、面上项目等纵向项目，华为、蚂蚁金服、阿里巴巴等多个企业横向项目。目前他已经发表40余篇论文，其中大多数发表在 IEEE/ACM 汇刊等顶级期刊和 ACM 计算机与通信安全国际会议（CCS）、ACM 多媒体大会（MM）、ACM 嵌入式网络传感器系统国际会议（SenSys）和 IEEE 计算机通信国际会议（INFOCOM） 等重要国际学术会议上。根据谷歌学者（Google Scholar）的统计，他的文章总引用次数则超过2000次。他获得过包括 ASIACCS’18, IEEE/ACM 全球网络服务质量会议（IWQoS’17）最佳论文奖等多个奖项。8）常瑞，副教授/博士生导师。CCF高级会员、CCF体系结构专委委员、CCF系统软件专委委员，从事系统安全方向的科研与教学十余年，曾获评全军优秀教师，于中国人民解放军信息工程大学获得计算机科学与技术博士学位，并获 ACM 中国优秀博士学位论文分会奖。研究方向包括处理器安全架构、可信执行环境安全、软件供应链安全、固件安全分析、形式化验证等，主持完成国家、省部级科研项目十余项，发表学术论文四十余篇，多项研究成果获得省部级奖励（军队教学成果一等奖 1 项、军队科技进步二等奖 2 项等），担任AAA战队指导教师、“龙芯杯”系统能力大赛优秀指导教师（2021年国赛一等奖）、“强网杯”网络安全挑战赛优秀指导教师（2021年总决赛特等奖、高校第一名）。更多信息欢迎参见个人主页 https://person.zju.edu.cn/changrui.9）卜凯，副教授/硕导。浙江大学计算机科学与技术学院副教授，浙江大学网络 空间安全研究中心成员。于 2013 年获香港理工大学电子计算学系博士学位， 并分别于 2006、2009 年获南京邮电大学计算机学院学士、硕士学位。主要研 究方向为网络安全。曾在 HPCA、NDSS、INFOCOM、ToN、TIFS、TPDS 等网络与 安全领域知名国际会议和期刊发表多篇论文，并获得 IEEE/IFIP EUC 2011 Best Paper Award (第二作者)。更多信息欢迎参见 http://list.zju.edu.cn/kaibu。10）吴磊，副教授。2015年毕业于美国北卡州立大学获得计算机科学博士学位，博士期间研究方向为移动安全。2015年加入奇虎360无线安全研究院担任高级研究员，继续从事移动安全方向的研究和产品研发。2017年作为联合创始人加入区块链安全初创公司派盾信安(PeckShield Inc.)，担任工程副总裁，主要负责智能合约安全研究和相关业务。2019年加入浙江大学，主要研究方向为区块链安全和系统安全。个人主页：https://leiwu.org。11）林峰，研究员/博导。林峰研究员研究方向为物联网安全，无线感知，设备攻防，身份认证及人工智能应用。在以上领域共发表近 90 篇高水平论文，引用超过 3000 次，包括安全顶会ACM CCS(CCF A 类) ，NDSS(清华A类,安全顶级会议)，移动计算顶会ACM MobiCom (CCF A 类), , ACM UbiComp(CCF A 类)，ACM SenSys (清华A类，移动系统顶级会议)，ACM MobiSys(清华A类,移动系统顶级会议)，Infocom（CCF A类），IEEE TMC (CCF A类)，IEEE TCAD (CCF A 类)，IEEE TNET（CCF A类），IEEE TII( SCI 1 区顶级刊物)，IEEE IoT-J ( SCI 1 区顶级刊物)，等。参与英文编著一部，标准制定一项。主持 1 项国家自然科学基金面上项目，1项JW科技委项目，1项美国职业安全与健康保障部 (NIOSH)项目和多项华为公司、光通天下等企业的合作项目，参与7 项美国自然科学基金委(NSF), 美国海军研究办公室(ONR)，浙江省领军型创新创业团队等资助的研究。担任IEEE Network Magazine, IEEE Access等多个知名SCI 期刊编委和 IoTDI,WiSec 等国际会议的宣传主席与出版主席，担任 MobiCom, SenSys, MobiHoc, ICDCS等多个国际会议 TPC 成员。是IEEE/CCF高级会员，浙江省特聘专家，杭州市特聘专家。获得过ACM SIGSAC China Rising Star Award（ACM中国安全分会新星奖），ACM MobiSys'20, IEEE Globecom'19 , IEEE BHI'17 会议最佳论文奖、ACM HotMobile'18 会议最佳演示奖、ACM SenSys'21, IEEE Infocom'21最佳论文奖提名。获中国研究生创“芯”大赛 全国一等奖及优秀指导教师奖、中国高校计算机大赛网络技术挑战赛总决赛一等奖，IEEE/J-BHI 期刊封面文章、NYNJERC 前沿研究 奖，沃达丰全球无线创新项目提名奖等。主持与参与的科研项目产生巨大的影响力，被美国NSF 新闻，ACM通讯新闻，华尔街日报等国际媒体广泛报道。12）张秉晟，研究员/博导。浙江大学百人计划研究员，博士生导师。科技部重大科研项目首席科学家（网络空间安全治理专项），以密码学研究为核心，主要从事安全多方计算、零知识证明和区块链安全。回国前曾任英国兰卡斯特大学助理教授(终身教职 tenured)、信息安全学科带头人、网络安全系主任。在学术方面，张秉晟近年来在国际高水平期刊会议上发表学术论文 50 余篇，其中通信作者或者第一作者 29 篇:包括三大 IACR 国际密码学顶级会议(例如 Eurocrypt、Asiacrypt)、四大国际安全顶级会议(例如 ACM CCS、NDSS) 和其他网络安全相关 CCF A 类国际顶级会议及 SCI 1 区期刊(如 INFOCOM、TIFS、TMC)。在国内，他主持了自然科学基金面上项目和科技部重点研发项目。在国外，他主持和参与了英国工程和自然科学研究委员会(EPSRC)、美国国家自然科学基金委(NSF)、欧洲研究院(ERC)、欧盟地平线 2020 (Horizon2020)、希腊研究与技术委员会(GSRT)等资助的多个大型研究项目。他的科研成果在科学界与工业界产生了巨大的影响力，被华尔街日报(Wall Street Journal)、台湾科技新报(TechNews)等多家国际媒体报道。最近，张秉晟致力于推进隐私计算相关国际标准，任IEEE CES/SC P2859 多模态融合标准化工作组副主席、IEEE CES/SC P2842安全多方计算工作组秘书、ISO SC27国际标准化中国专家组成员，主导推进ISO SC27 基于零知识证明的隐私保护指南国际标准。13）申文博，申文博：研究员/博导，主要研究方向为软件供应链安全、操作系统安全、容器安全、软件及系统攻防和程序分析。2015年获得美国北卡罗莱纳州立大学计算机博士学位。2015-2019担任三星美国研究院（Samsung Research America）操作系统内核安全的技术负责人。2019年加入浙江大学网络空间安全研究中心和计算机科学与技术学院。申文博研究方向为软件与系统安全，着眼于设计新型、实用的系统及软件安全方案，发表论文及专利30余篇，包含10余篇安全领域四大顶级会议论文及CCF-A类论文(包含IEEE S&P, ACM CCS, USENIX Security, NDSS, TDSC, ACM MobiCom, TMC)，覆盖全部计算机安全四大国际会议，获得2项杰出论文奖，包含四大顶级会议之一的NDSS的杰出论文奖。申文博研究员常年活跃于移动系统安全攻防的第一线，通过分析实际攻击，设计相应的操作系统保护方案，具有学术界和工业界的双重研究经历和视野；多年来设计、实现并主导部署了多种操作系统内核安全机制，保护超过亿部设备系统安全。个人主页https://wenboshen.org/。14）刘健，研究员/博导。浙江大学百人计划研究员，博士生导师。2019 年 11 月加 入浙江大学网络空间安全学院。2018 年 7 月获得芬兰阿尔托大学博士学位， 并于同年加入加州大学伯克利分校担任博士后研究员。其研究领域涵盖应用密 码学、分布式系统、区块链、人工智能。致力于构建可证明安全的、易用的、 可部署的系统应用。在学术方面，刘健近年来在国际高水平期刊会议上发表学 术论文 10 余篇，其中通信作者或者第一作者 6 篇，包括两篇网络安全相关 CCF A 类国际顶级会议论文。根据谷歌学 者(Google Scholar)的统计，他的论 文引用 400 余次。更多信息欢迎参见 <https://person.zju.edu.cn/jianliu>15）沈浩頲，浙江大学百人计划研究员，博士生导师。2014 年 1 月博士毕业于宾夕法尼亚州立大学，随后于美国标准与技术研究所、佛罗里达大学从事博后、副研究员工作，2019 年 至 2021 年于内华达大学担任 tenure-track 助理教授，作为主要参与者参加了美国自然科学基金、国防部和能源部的若干重大项目。研究工作主要结合了计算机、集成电路、半导体工艺、材料科学等交叉学科的技术，探索新兴技术为安全研究带来的新挑战和新机遇。发表40余篇论文，被引700余次（谷歌学术），包括以主要作者发表在CCF-A DAC、硬件安全顶会CHES、芯片设计顶刊TVLSI等；授权发明7项美国专利，参编书籍2部，担任国际会议专题/出版主席，及多个国际期刊的审稿人。16）杨坤，浙江大学百人计划研究员，博士生导师。本科毕业于中国科学技术大学，硕士先后毕业于中国科学院微电子研究所和美国康涅狄格大学，博士毕业于美国佛罗里达大学。曾先后在康涅狄格大学和佛罗里达大学担任助理研究员。曾在美国康卡斯特公司总部担任硬件安全工程实习生。曾于2018年5月至2022年1月在美国英伟达公司总部担任高级安全架构师。深度参与了包括NVIDIA Drive AGX Orin及NVIDIA Grace CPU在内的多款芯片的研发工作。主持研发的对称加密加速器及参与研发的非对称加密加速器已被集成到英伟达最新的包括Orin与Grace在内的多款芯片中。主持开发的多种硅前及硅后安全特征评估流程及方法学已被应用于英伟达的芯片安全验证流程。于2022年3月加入浙江大学。研究方向包括硬件安全，芯片安全架构，及软硬件融合安全架构。作为主要发明人已获授权2项美国专利，另已提交3项国际专利申请，以第一作者发表5篇SCI期刊论文(其中4篇为ACM汇刊)及6篇EI会议论文(包括1篇EDA领域顶级会议ICCAD，及1篇硬件安全领域顶级会议HOST)，以合作作者发表3篇EI会议论文(包括1篇EDA领域顶级会议DAC)，另有多次会议报告及硬件演示。曾获2016年硬件安全领域顶级会议IEEE HOST最佳论文奖提名，2020年英伟达NTECH会议最佳论文奖唯一一等奖，及2021年英伟达专利奖。17）许海涛，浙江大学百人计划研究员，博士生导师。2015 年 12 月博士毕业于威 廉与玛丽学院，2016 年 1 月至 2018 年 5 月于美国西北大学先后担任博士后、研究助理教授职位，2018 年 7 月至 2020 年 12 月于亚利桑那州立大学担任 tenure-track 助理教授。许博士主要从事Web安全、深度学习、智能车安全、互联网反欺诈、以及黑灰产研究等领域的研究。许博士曾作为团队主要负责人参与美国国防部高级研究计划局（DARPA）透明计算项目，负责开发针对高级可持续性攻击（APT）的检测及追溯机制。许博士的研究成果先后发表在NDSS, WWW, INFOCOM, TMC等国际顶级会议以及期刊，部分成果被华尔街日报、中国日报等主流媒体报道。18）刘金飞，“百人计划”研究员，博士生导师。2017年博士毕业于美国埃默里大学，毕业后在佐治亚理工学院和埃默里大学任博士后研究员。2020年加入浙江大学计算机科学与技术学院/网络空间安全学院。刘金飞博士主要从事数据要素市场，数据安全与合规、数据查询等方向的研究工作，带领浙江大学DIVER（Data prIVacy, sEcurity, and maRket）研究小组。 2015-2021年间以第一作者身份发表CCF数据库领域A类顶级论文10余篇（全美最多），是所有数据库领域旗舰会议（e.g., VLDB, SIGMOD, ICDE）的程序委员会委员，并参与所有数据库领域旗舰期刊（e.g., VLDBJ, TKDE, TODS）的审稿工作。主持国家自然科学基金和国家重点研发计划课题。19）巴钟杰，“百人计划”研究员，博导。2019年毕业于美国纽约州立大学布法罗分校并获得计算机科学与工程博士学位。曾任加拿大麦吉尔大学计算机科学学院博士后研究员。2020年加入浙江大学网络空间安全学院。研究工作主要围绕物联网安全、深度伪造、隐私保护、智能感知等方向展开，尤其致力于研究音、视、图等多媒体数据的安全与隐私问题。在CCS，NDSS，INFOCOM，ICDCS，TIFS等多个国际著名安全会议及期刊中均有文章发表；主持国家自然科学基金委面上项目，与华为等厂商开展深入合作，担任IEEE ICC, IEEE ICDCS等多个国际著名会议的TPC成员以及IEEE Internet of Things Journal的编委；多项研究成果在工业界具有广泛应用，并受到包括CCTV，新华网，中国科学报，NSF News在内的超过80家海内外媒体的广泛报道。其中，团队在加速计窃听方向的工作促使了谷歌公司对安卓操作系统权限管理机制进行优化，加强了对零权限传感器的使用限制。20）杨子祺，研究员/博导。博士毕业于新加坡国立大学。主要从事人工智能安全、智能化信息安全、数据安全与隐私保护等领域的研究工作。他是国际上人工智能安全与隐私研究的前沿技术研究者之一，在机器学习对抗攻防、后门攻防、版权保护、隐私保护等研究方向上做出一系列创新研究工作。此外，在人工智能与信息安全交叉研究领域，他研究了多个前沿热点方向，包括二进制恶意代码的作者信息溯源、跨设备的侧信道功耗分析、自适应的DDoS检测与防御等。近年来，他以第一和通讯作者发表的高水平学术论文包含信息安全领域四大顶会之一ACM计算机与通信安全国际会议（ACM CCS）、ACM设计自动化国际会议（DAC）等国际顶级会议论文（CCF A类）。现担任网络与信息安全领域顶级期刊IEEE TDSC评审，信息安全领域四大顶会之一网络与分布式系统安全会议（NDSS）审稿人，并担任网络和系统安全国际会议NSS和嵌入式系统安全证明国际会议PROOFS的程序委员会委员。21）卢立，研究员/博导。2020 年于上海交通大学计算机科学与工程系获博士学位，2015 年于西安交通大学计算机科学与技术系（现计算机科学与技术学院）获学士学位。曾获国家留学基金委资助赴美国罗格斯大学无线信息与网络实验室（WINLAB）交流访问。研究工作主要集中在物联网安全、移动感知、普适计算等方面。在国际一流期刊与重要国际会议上发表近30篇论文，包括IEEE INFOCOM、ACM UbiComp、ACM SenSys、IEEE/ACM ToN、IEEE TMC、IEEE TPDS等；获授权专利11项;部分成果被IEEE Spectrum、凤凰网、搜狐网等主流媒体报道。工作受到国家自然科学基金委、国家重点研发计划、浙江省重点研发计划、浙大-华为联合实验室等项目资助。获ACM MobiCom'19 First Runner-up Poster Award, ACM中国SIGAPP分会优秀博士学位论文奖，上海市计算机学会优秀博士学位论文提名奖等荣誉。担任中国计算机学会普适计算专委会执行委员，浙江省网络空间安全协会专家技术委员会副秘书长。担任IEEE INFOCOM, IEEE ICDCS, IEEE/ACM IWQoS, IEEE ICPADS等国际会议的TPC、及多个国际期刊的审稿人。 |
| **团队主要成员** |
| **姓名** | **职称** | **研究方向** | **联系方式** |
| 任奎 | 教授 | 数据安全与隐私保护、人工智能安全、物联网安全 | kuiren@zju.edu.cn |
| 韩劲松 | 教授 | 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 | hanjinsong@zju.edu.cn |
| 赵永望 | 教授 | 形式化方法、操作系统安全、安全关键系统 | zhaoyw@zju.edu.cn |
| 张帆 | 教授 | 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 | fanzhang@zju.edu.cn |
| 王志波 | 教授 | 人工智能安全、物联网、数据安全与隐私保护，边缘智能与安全 | zhibowang@zju.edu.cn |
| 周亚金 | 研究员 | 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 | yajin\_zhou@zju.edu.cn |
| 秦湛 | 研究员 | 数据安全、人工智能安全、隐私保护 | qinzhan@zju.edu.cn |
| 常瑞 | 副教授 | 处理器安全架构、可信执行环境安全、固件安全分析、形式化验证、软件供应链安全 | crix1021@zju.edu.cn |
| 卜凯 | 副教授 | 无线网络，网络安全 | kaibu@zju.edu.cn |
| 吴磊 | 副教授 | 区块链安全、移动安全、系统安全 | lei\_wu@zju.edu.cn |
| 林峰 | 研究员 | 物联网安全、可信感知、安全认证、移动安全 | flin@zju.edu.cn |
| 张秉晟 | 研究员 | 密码学、区块链、数据安全、安全多方计算、零知识证明 | bingsheng@zju.edu.cn |
| 申文博 | 研究员 | 系统安全、容器安全、移动安全、操作系统安全、软件攻防 | shenwenbo@zju.edu.cn |
| 刘健 | 研究员 | 应用密码学、区块链、分布式系统、机器学习 | liujian2411@zju.edu.cn |
| 沈浩颋 | 研究员 | 硬件安全、物联网安全、区块链、智能制造 | htshen@zju.edu.cn |
| 杨坤 | 研究员 | 硬件安全、芯片安全架构、软硬件融合安全架构 | kuny@zju.edu.cn |
| 许海涛 | 研究员 | Web 安全、网络安全、在线欺诈检测、恶意软件检测 | haitaoxu@zju.edu.cn |
| 刘金飞 | 研究员 | 数据要素市场、数据安全与合规 | jinfeiliu@zju.edu.cn |
| 巴钟杰 | 研究员 | 物联网安全、移动安全 | zhongjieba@zju.edu.cn |
| 杨子祺 | 研究员 | 人工智能安全，智能化信息安全、数据安全与隐私保护 | yangziqi@zju.edu.cn |
| 卢立 | 研究员 | 物联网安全、移动感知、普适计算、人机交互 | li.lu@zju.edu.cn  |