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	周亚金	Email	yajin_zhou@zju.edu.cn	电话	18911375133

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。

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，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”7 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。中心目前已建立了中央网信办/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-浙江省工程实验室、浙江大学-阿里巴巴网络空间安全联合实验室、浙江大学-蚂蚁金服金融科技研究中心-数据安全与隐私保护实验室、浙江大学-华为安全技术创新实验室、浙江大学-光通天下网络空间安全联合实验室、浙江大学-华为系统与数据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，持续不断地产出高水平科研成果，成为支撑科研、教学和实践的重要平台。

中心近三年在物联网安全、系统安全、网络安全、数据安全、区块链安全、人工智能安全等方向先后承担科技部科技创新 2030 重大项目、国家自然科学基金重点项目、中国科协重大调研课题、浙江省重点研发计划等重大重点课题七项和十余项国家自然科学基金项目，发表相关学术论文近百篇，其中 CCF-A 类 50 余篇，获得 11 项杰出论文奖。国际安全顶会论文数 CS Rankings 全国第一、亚洲第二。成果被国内外多家媒体报道，包括中央电视台、新华社、光明日报、科技日报、华尔街日报、美国国家公共电台、科学美国人以及搜狐、腾讯、新浪、今日头条等。

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。中心积极营造良好的软硬件环境，积极邀请国内外知名专家学者到校学术交流，每年举办海外/高峰讲座 40 余场，同时也多次与国际机构 IEEE,ACM 等联合举办国际会议，极大提高了浙江大学网络空间安全学科的国际影响力。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。

导师简介：

1） **任奎：教授/博导，中心主任。**任奎教授本硕毕业于浙江大学，2007 年于美国伍斯特理工学院获博士学位，2017 年成为纽约州立大学冠名教授。任奎是浙江大学求是讲席教授，ACM 和 IEEE 会士。**任奎教授是数据安全、人工智能安全、物联网安全与认证与隐私保护等领域的国际知名专家。**他先后主持和参与了科技部、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、阿里巴巴、蚂蚁金服、华为、亚马逊等机构和公司的多项科研项目，多项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，获得了包括 IEEE ICDCS’20、ACM MobiSys’20、IEEE INFOCOM’20、IEEE Globecom’19、中国密码学会’18、ACM/IEEE IWQoS’17，IEEE ICNP’11 等在内的多篇最佳论文和时间考验论文奖。他的 H-Index 为 76，

文章总引用次数超过 35,000 次，并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，国际一流会议主席或共同主席，包括现/曾任《中国科学： 信息科学》、《ACM 互联网技术汇刊》、《ACM 信息物理系统汇刊》、《ACM 物联网汇刊》、《IEEE 网络汇刊》、《IEEE 可信任安全计算汇刊》、《IEEE 服务计算汇刊》、《IEEE 移动计算汇刊》、《IEEE 网络科学与工程汇刊》、《IEEE 信息取证与安全汇刊》、《IEEE 无线通信杂志》、《IEEE 物联网期刊》、《IEEE 智能电网汇刊》、《Elsevier 计算机网络期刊》、《ZTE Communications》、Springer 安全系统与网络书系 、中国计算机学会网络汇刊 、电子学报 (英文版)和网络及信息安全学报等的编委和副主编。任奎教授同时担任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、ACM 亚洲计算机与通信安全会议指导委员会委员、ACM 中国安全分会会长，浙江省网信咨询委员会委员以及浙江省海高会青年分会首任会长。

2） **周亚金：研究员/博导。研究兴趣是软件安全、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。**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 10 篇，获得 ICPADS 18 最佳论文和 IEEE EURO S&P 2019 最佳论文奖。他的文章引用数超过 5000 次，两篇论文入选自 1981 年以后引用最多的安全论文列表，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、操作系统、程序分析、体系结构、数据攻击数源等感兴趣的同学报考，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，了解计算机操作系统运作方法，有过程序分析（基于 LLVM)或者逆向经验，有体系结构安全经验，有基于大数据的异常攻击检测经验等。

3） **秦湛：研究员/博导。秦湛研究员从事用户隐私保护、云计算安全、物联网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。目前他已经发表 21 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，他的文章五年内总引用次数则超过 800 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。最近 5 年共 10 篇发表同行评议的会议论文（5 篇 CCF A 类

会议），15 篇期刊论文。

4） **林峰：研究员/博导。林峰研究员研究方向为物联网安全，可信感知，移动安全，安全认证及移动传感物联网应用。**在以上领域共发表近 60 篇高水平论文，引用超过 1000 次，包括 ACM MobiCom (CCF A 类), ACM CCS(CCF A 类), ACM UbiComp(CCF A 类)，ACM MobiSys(CCF B 类,移动系统顶级会议)，NDSS(CCF B 类,安全顶级会议)，IEEE TMC (SCI CCF A)，IEEE TCAD (SCI CCF A 类)，IEEE TII (SCI 1 区顶级刊物)，IEEE IoT-J (SCI 1 区顶级刊物)，IEEE TBioCAS (SCI 2 区刊物)，IEEE TVT (SCI 2 区刊物)，IEEE J-BHI (SCI 2 区刊物，分别选为当期唯一封面文章)等。参与英文编著一部。主持 2 项美国职业安全与健康保障部(NIOSH)和 Comcast 网络公司资助的研究项目，主持 1 项国家自然科学基金面上项目，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 ICDCS,MASS 等多个国际会议 TPC 成员。获得过 IEEE Globecom'19 最佳论文奖，IEEE/BHI'17 会议最佳论文一等奖、ACM/HotMobile'18 会议最佳演示奖、中国研究生创“芯”大赛全国一等奖及优秀指导教师奖、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在科学界产生巨大的影响力，被美国（NSF 新闻，ACM 通讯新闻，华尔街日报，CNN 等）和国际媒体（包含国内新浪，搜狐等）广泛报道。

5） **申文博：研究员/博导。浙江大学百人计划研究员，博士生导师。主要研究方向为操作系统安全、容器安全、系统安全、软件及系统攻防和程序分析。**本科于 2010 年毕业于哈尔滨工业大学，曾带队获得全国大学生信息安全竞赛一等奖；2015 年获得美国北卡罗来纳州立大学计算机博士学位，研究方向为系统及无线安全，并于同年加入位于美国硅谷的三星美国研究院（Samsung Research America），担任操作系统内核安全的技术负责人。于 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。研究成果包含论文及专利 20 余篇，其中 8 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)，是国际少有的论文覆盖全部计算机安全四大顶级国际会议的青年学者，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内核安全。个人主页：https://wenboshen.org/。

6） **韩劲松：教授/博导。**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。**近年来已出版英文专著两部；在国际一流期刊与重要国际会议如 IEEE/ACM

TON、IEEE TMC，ACM MobiCom、CCS、UbiComp、SenSys、IEEE INFOCOM、ICN 等上发表 40 余篇高水平文章，获得美国专利 2 项，中国专利 10 余项；主持国家自然科学基金面上项目三项，并担任多个重要项目的主要负责人，如国家自然科学基金重点项目子课题、973 计划子课题、香港创新及科技基金重点项目等。担任多个国际一流会议的程序委员会委员，如 INFOCOM, ICNP, ICCCN, DCOSS, ICPADS 等；获 2019 IEEE 信息通信年会（INFOCOM）最佳论文奖、2019 IEEE 全球通信会议（GLOBECOM）最佳论文奖、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。

7） **张秉晟：研究员/博导。**浙江大学百人计划研究员，博士生导师。研究工作以应用密码学为核心，主要从事数据安全、安全多方计算、零知识证明和区块链安全。 自 2011 年海外博士毕业至今，已积累了连续 8 年的海外教研经验，加入浙江大学前，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。兰卡斯特大学在英国三大排名系统中均为前十(Times/Sunday Times 2019 第 6 名、Guardian University Guide 2020 第 7 名、Complete University Guide 2020 第 7 名)，是英国国家网络安全中心(NCSC)认证的第一批 8 所网络安全优秀 科研机构(Academic Center of Excellence in Cyber Security Research)之一。同时主持的网络安全硕士专业是首批 4 个得到英国政府通信总部(GCHQ)完全认证的专业。在学术方面，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)。根据谷歌学者(Google Scholar)的统计，他的论文引用 900 余次，H-index 为 16。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。现任中国工信部信通院下的中国通信标准化协会大数据技术标准推进委员会的评审专家、中国 ISO SC27 标准化 38 位专家之一。

8） **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。主要研究方向为无线网络及网络安全。曾在 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。

9） **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

10） **张帆，副教授/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 年在硬件安全、芯片设计、体系结构、密码学领域发表高水平论文 60 余篇，其中 CCF-A/B 会议期刊论文约 20 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。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 IEEE Access, 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。

11） **常瑞，副教授，博导。全军优秀教师，**从事系统安全方向的科研与教学十余年，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。研究兴趣围绕**嵌入式系统安全，研究方向包括可信执行环境安全防护、系统安全加固、形式化分析与验证、边缘计算安全**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)，指导学生多次获得全国信息安全竞赛、大学生蓝桥杯竞赛、物联网大赛、体系

结构创新竞赛等国家级奖励，个人获全国微课竞赛二等奖、省部级讲课竞赛一等奖等。更多信息欢迎参见个人主页 https://person.zju.edu.cn/changrui.

12） **吴磊，讲师。**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 年加入浙江大学网安学院。主要从事移动安全以及区块链安全领域的研究工作，尤其致力于程序分析技术在漏洞挖掘、检测等相关的安全性分析中的应用等方向的研究；在国际著名安全会议 CCS、FC、ASIACCS 等均有论文发表，并参与多个国际一流会议的审稿工作。

13） **赵永望，教授，博士生导师。**担任 ARINC653 国际操作系统标准委员会委员（国内唯一委员）、国际信息技术安全评估标准(Common Criteria,CC)操作系统内核技术委员会委员、中国计算机学会(CCF)高级会员、CCF 系统软件专委会和形式化方法专委会委员。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。主要研究方向包括操作系统安全、形式化验证、编程语言原理等。主持和参与国家自然基金、核高基重大专项、重点研发计划、载人航天工程重点项目、工信部物联网创新项目等 10 余项，2011 和 2017 年分别获得中国电子学会和山东省科技进步一等奖。相关研究成果得到美国波音、法国空客和国际知名实时操作系统厂商的认可，被纳入国际标准，并在开源实时操作系统社区产生影响力。

14） **杨子祺，“百人计划”研究员，博导。**博士毕业于新加坡国立大学计算机学院。主要从事人工智能安全与隐私、人工智能在信息安全领域中的应用、数据安全等领域的研究工作。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，在机器学习模型逆向攻击与防御、成员推断攻击与防御、神经网络后门植入技术、对抗样本攻击等研究方向上做出一系列创新研究工作。他首次提出黑盒神经网络的模型逆向攻击方法，并实现世界上第一个对商用人脸识别服务的逆向攻击。在人工智能在安全问题中的应用领域，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。博士期间以第一作者和通讯作者发表高水平学术论文 8 篇，包含 ACM 计算机与通信安全国际会议（CCS）、ACM 设计自动化国际会议（DAC）等国际顶级会议论文（CCF A 类）。除此之外，还有多篇论文在投国际顶级会议和期刊。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。在业界也建立了广泛合作关系，与华为、蚂蚁金服、卡巴斯基实验室、新加坡人工智能院（AI Singapore）、新加坡国家网络安全研究

室等单位广泛合作并取得诸多学术成果。

15） **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。毕业后加入加拿大麦吉尔大学计算机科学学院任博士后研究员。2020 年加入浙江大学网络空间安全学院。巴钟杰博士主要从事物联网安全，隐私保护，智能感知等方向的研究工作，尤其致力于研究移动智能设备的物理层攻防体系，包括基于物理指纹的移动安全增强机制和基于零/低权限传感器的侧信道攻击技术。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，并参与多个国际著名会议和期刊的审稿工作。其中，在侧信道攻防方面的工作已被超过 80 家海内外媒体广泛报道，包括 CCTV，新华网，中国科学报，NSF News 等多个高影响力的媒体。

16） **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、网络安全、在线欺诈检测、黑灰产研究、网络测量、以及用户隐私保护等领域的研究。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，曾获阿里巴巴总部的邀请专程回国做专题报告。

17） **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安全与隐私保护，数据市场，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。 是最近五年全美大学以第一作者身份发表 CCF 数据库领域 A 类顶级论文数量最多(9 篇)的学者，并参与多个国际著名会议和期刊的审稿工作。

18） **卢立特聘研究员、博士生导师，浙江省区块链与网络空间治理重点实验室骨干成员。**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）和电子与计算机工程系作为访问研究学生从事研究。研究工作主要集中在物联网安全、移动安全、普适计算、人机交互等方面。在国际一流期刊与重要国际会议上发表 20 余篇高水平文章，包括 IEEE INFOCOM、ACM UbiComp、IEEE/ACM ToN、IEEE TMC、IEEE TPDS 等；获授权专利 8 项。担任过 IEEE/ACM IWQoS, IEEE ICPADS 等国际会议的 TPC，并为多个国际期刊与会议进行审稿工

作。曾获上海市计算机学会优秀博士学位论文提名奖，ACM MobiCom'19 First Runner-up Poster Award。

19） **王志波，教授，博士生导师。**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 高级会员、CCF 高级会员和电子学会高级会员，CCF 物联网专委会常委，中国电子学会物联网青年专技组常委，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。主要研究方向包括物联网、人工智能安全、数据安全与隐私保护、边缘计算与边缘智能。先后发表了 100 余篇论文在国际权威期刊和学术会议上，其中 CCF 推荐的 A 类顶级期刊和会议论文 30 篇、ESI 高被引论文七篇。授权发明专利 11 项，公开发明专利 10 余项。主持与参与了国家自然科学基金、科技创新 2030-新一代人工智能重大项目、973 计划、教育部装备青年人才基金等国家级项目，并与华为、蚂蚁金服等公司开展多项合作研发项目。担任 INFOCOM、IPCCC、Globecom 与 ICC 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。

团队主要成员

姓名	职称	研究方向	联系方式
任奎	教授、博导	人工智能安全、数据安全、物联网安全与隐私保护	kuiren@zju.edu.cn
周亚金	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	yajin_zhou@zju.edu.cn
秦湛	研究员、博导	数据安全、人工智能安全、隐私保护	qinzhan@zju.edu.cn
林峰	研究员、博导	物联网安全、可信感知、安全认证、移动安全	flin@zju.edu.cn
申文博	研究员、博导	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
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	hanjinsong@zju.edu.cn
张秉晟	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	bingsheng@zju.edu.cn
卜凯	副教授、硕	无线网络，网络安全	kaibu@zju.edu.cn

	导		
刘健	研究员、博导	应用密码学、区块链、分布式系统、机器学习	liujian2411@zju.edu.cn
张帆	副教授、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	fanzhang@zju.edu.cn
常瑞	副教授、博导	嵌入式系统安全、设备安全、系统安全分析、形式化方法	crix1021@zju.edu.cn
吴磊	讲师	区块链安全、移动安全、系统安全	lei_wu@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
杨子祺	百人计划研究员	人工智能安全，数据隐私，系统安全，移动安全	yangziqi@zju.edu.cn
巴钟杰	百人计划研究员	物联网安全、移动安全	zhongjieba@zju.edu.cn
许海涛	百人计划研究员	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	百人计划研究员	数据市场、数据安全与隐私、数据查询	jinfeiliu@zju.edu.cn
卢立	研究员	物联网安全、移动安全、普适计算、人机交互	li.lu@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	zhibowang@zju.edu.cn