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	秦湛 陈思思	Email	qinzhan@zju.edu.cn; 0922b48@zju.edu.cn;	电话	13521791022 18767120330

主要情况介绍：

浙江大学于2012年设立信息安全专业方向，2016年获批首批网络空间安全一级学科博士、硕士学位授权点之一。2017年网络空间安全研究中心成立，凝聚本校多个A+、A类学科的优势力量共同开展网络空间安全一流学科建设。2019年网络空间安全学院成立，同年网络空间安全学科获批成为浙江大学7个优势特色学科之一。2020年浙江大学信息安全专业获评教育部一流本科专业，网络空间安全学科学位授权点专项评估合格。2021年本科信息安全专业在**软科专业排名中评分A+**，位列全国第一。2025年浙江大学在全球计算机科学领域权威学术排名CSRankings计算机安全与移动计算方向近三年论文排名**全球第二**，网络空间安全学科在软科中国最好学科排名位列全国第四。

学院形成了一支由国家高层次人才、AAAS/ACM/CCF/IEEE会士、万人领军人才、新世纪百千万人才、青年人才、海外高校教职人员等优秀人才组成的高水平国际化学术队伍，平均年龄37岁，具有海外博士学位者超过80%。学院坚持以树人为核心，以立德为根本，主持教育部教改项目4项，获教育部产学协同育人优秀案例一等奖，培养的学生赴国家战略急需的重点单位就业人数占比超过70%，学生在国内外著名比赛中屡创佳绩，包括**Defcon CTF全球总冠军（打破国外高校CMU连续十余年冠军垄断）**、BlackHat MEA CTF全球总冠军、iDash国际比赛第一名、HACK@DAC硬件CTF竞赛全球第一、NeurIPS国际人工智能安全竞赛冠军、“挑战杯”揭榜挂帅专项赛特等奖、强网杯冠军、信安赛一等奖、全国大学生人工智能安全竞赛一等奖等。

学院依托**区块链与数据安全全国重点实验室**、中央网信办/教育部网络空间国际治理研究基地、新一代信息安全与隐私保护标准化技术工业和信息化部重点实验室、教育部重点实验室（B类）、移动终端安全技术浙江省工程研究中心等多个国家级、省部级科研平台，同时与中国信通院、人民网、中国联通、华为、阿里巴巴、蚂蚁等企事业单位共建十余个产学研用协同创新平台，持续不断产出高水平科研成果。

学院围绕**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**等四大重点科研方向，近年来持续不断地产出高水平科研成果，主持科技部“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级、省部级项目/课题**90余项**，荣获中国电子学会自然科学一等奖、浙江省自然科学一等奖、浙江省科学技术进步一等奖、中国电子学会自然科学二等奖等多个省部级奖项，发表**CCF-A类论文470余篇**，获得30余项最佳/杰出论文奖，获国际/国家专利授权160余项，主导/参与制定国内外标准50项，报批CVE漏洞200余项，发布开源项目与工具20余项。形成了科学研究、人才培养、技术创新、产业发展的良性生态链。

导师简介：

1）任奎，浙江大学求是讲席教授，美国科学促进会（AAAS）会士、国际计算机学会（ACM）会士、中国计算机学会（CCF）会士和国际电气与电子工程师学会（IEEE）会士，目前担任浙江大学计算机科学与技术学院院长、网络空间安全学院院长、上海浙江大学高等研究院院长，区块链与数据安全全国重点实验室常务副主任，校学术委员会委员，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。任奎教授主要从事数据要素安全、人工智能安全等领域的研究。发表了500余篇同行评议的期刊与会议文章，获得多篇最佳论文奖和时间考验论文奖。H-Index为109，文章总引用次数超过60,000次，授权发明专利90余项，连续入选科睿唯安全球高被引科学家。国家重点研发计划项目首席科学家，获三项省部级一等奖、IEEE安全技术委员会技术成就奖、纽约州立大学杰出学者奖、美国国家科学基金会青年职业奖、浙大国华杰出学者奖等多项荣誉。在数据要素安全领域，研发自编译高扩展可证明安全隐私保护计算平台，主导制定ISO国际标准2项、起草全国数据标准化技术委员会（SAC/TC609）《可信数据空间 技术架构》“安全要求”章节。获IEEE INFOCOM时间考验论文奖等10余项国内外学术荣誉，应用于阿里、蚂蚁及华为等相关产品，保护上亿用户的数据安全。在人工智能安全领域，人工智能可证明安全理论、AI模型安全攻防技术、生成内容检测与水印、AI自动化入侵检测与漏洞挖掘等领域取得一系列重要技术创新，领导研发DeepSeek-R1-Safe基础大模型、国产软硬件自主可控大模型安全训练平台、AI全周期安全评测平台、深度合成与认知安全平台、AI自动化渗透测试平台等重要成果与科学装置。成果获ACM MobiSys’20最佳论文奖、NeurIPS’24 模型安全大赛冠军、第三届中国人工智能竞赛一等奖等奖项，应用于公安、华为、中国联通、国网、中车、阿

里等政府单位与企业关键部门，有效提升AI系统体系化安全能力与产业安全水平。任奎教授现任IEEE计算机学会会士遴选委员会副主席、IEEE通信学会会士评选委员会委员、IEEE ISI Award 奖励委员会主席、Kyoto Prize京都奖提名人、ACM ASIACCS指导委员会委员、ACM China副主席及多个国际权威期刊编委和学术会议主席。同时担任国家数据专委会委员、全国数标委委员、中国电子学会理事、中国网络空间安全学会常务理事、中国密码学会理事、浙江省政协委员、浙江省知联会副会长等职务。

2) 秦湛，浙江大学长聘副教授/博导、网络空间安全学院副院长、国家创新人才计划青年项目获得者、国家网信创新人才。在2018年加入浙江大学计算机科学与技术学院前，于2017年美国纽约州立大学布法罗分校获得计算机科学与工程博士学位，同年加入德克萨斯大学圣安东尼奥分校任助理教授（终身轨）。他的主要研究领域包括人工智能安全、数据安全与隐私保护技术等。累计发表论文90余篇，其中在IEEE TIFS、IEEE TDSC、Proc. IEEE等期刊和IEEE S&P、ACM CCS，NDSS、SIGMOD、VLDB、WWW、SIGKDD等CCF A顶级国际学术会议上发表论文40余篇，根据谷歌学术统计论文总引用次数超过9000次，曾获得2024年浙江省科技进步一等奖、2023年浙江省自然科学一等奖、2023年电子学会自然科学一等奖、2024年电子学会自然科学二等奖、以及2017年IEEE IWQoS最佳论文奖和2018年ASIACCS最佳论文奖，近5年来主持国家自然科学基金专项基金重点项目1项、联合基金重点项目1项、科技部科技创新2030重大项目课题1项，以及华为、阿里巴巴、蚂蚁集团、浙数集团等头部企业科研项目10余项，相关成果应用于南方电网、中车株洲、阿里巴巴数据安全中台Datatrust系统、华为数据通信网络安全检测平台和杭州城市大脑人工智能安全检测平台等产品中，保护亿级用户隐私与数据安全。

3) 王志波，浙江大学教授，计算机科学与技术学院院长助理，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。现为CCF杰出会员、ACM/IEEE/电子学会高级会员、电子学会网络空间安全专家委员会副秘书长、CCF网络与系统安全专委会常委、CCF物联网专委会常委、人工智能学会智能信息网络专委会常委。研究方向包括智能物联网、人工智能安全、数据安全与隐私保护，发表CCF A类论文90余篇，多篇论文荣获最佳论文奖和最佳学生论文奖，入选全球前2%顶尖科学家榜单和爱思唯尔(Elsevier)中

国高被引学者榜单。主持国家优青、联合基金重点项目、科技创新2030-新一代人工智能重大项目课题等多项国家级项目，研究成果服务于华为、阿里、蚂蚁、新华三、海康威视、杭州城市大脑等企业。荣获电子学会自然科学一等奖，浙江省自然科学一等奖、浙江省科技进步一等奖和IEEE 可扩展技术专委会职业中期研究成就奖等多个奖项。

4）杜文亮，浙江大学求是讲席教授/博导、ACM Fellow、IEEE Fellow。在2025年加入浙江大学计算机科学与技术学院前，于2001年美国普渡大学获得计算机科学与工程博士学位，同年加入美国雪城大学（Syracuse University）任助理教授（终身轨）。2012 晋升为正教授，2019 年评为 Meredith 讲席教授。他的主要研究领域包括计算机网络和系统安全、网络仿真技术、网安实际教育等。累计发表论文100余篇，根据谷歌学术统计论文总引用次数超过18200次，并获得2013 安全顶级学术会议ACM-CCS和2021年ACSAC会议颁发的时间考验奖（Test-of-Time Award）。主持美国科学基金会项目 11 项、谷歌研究项目 1 项、蚂蚁集团企业科研项目 1 项。他2002 年创立的SEED实验开源项目开发了近 40 多个网络空间安全动手实验，被全球80多个国家1100所学校采用。2010年，美国国家科学基金会（NSF）在递交给国会的报告中把 SEED项目作为一个模范项目。2024年，NSF的SaTC（Secure and Trustworthy Cyberspace）部门将SEED实验列为该部门资助的最有影响的项目之一，并邀请杜教授在PI大会上做主题演讲。杜教授著写的教科书《Computer & Internet Security: A Hands-on Approach》被全球290所高校采用。因为对网安科研和教育的重大影响，他在2023年被IEEE和ACM同年评选为 Fellow。

5）吴强，浙江大学，计算机科学与技术学院，求是特聘教授，博导。国家级高层次人才，中国通信学会会士；获国家技术发明二等奖，国家科技进步二等奖，及其它省部级奖励8项。他的主要研究领域包括新一代信息网络理论与关键技术、移动互联网理论与关键技术、算力/智算网络、云网基础设施智能与优化、确定性网络、工业互联网、空天地一体化网络、网络空间安全等。作为项目负责人或课题负责人承担国家重点研发计划（项目负责人）、国家重大科技专项（项目负责人） 、国家高技术研究发展计划、973计划、863计划、国家科技支撑计划等10余项国家级重大项目，研究成果在欧美亚太市场广泛应用。获得百余项国家发明专利授权，其中欧美日韩国际授权40+，第一发明人50+，与国内、国际标准组织IETF、ITU-T、ETSI、CCSA有对应关系的基本专利20+。发表CCF A&中

科院一区高水平论文30余篇。

6）杜跃进，浙江大学求是特聘教授/博导，区块链与数据安全全国重点实验室首席研究员，获国家科技进步一等奖两项，并获得新世界百千万人才工程国家级人才，国务院特殊津贴、全国青年岗位能手、信息产业十大杰出青年、CCF杰出会员、亚太信息安全领袖成就奖等荣誉。他的主要研究领域包括网络安全、数据安全、人工智能安全、智能汽车与具身智能安全、工业互联网安全、智慧应急与安全管理等。作为项目骨干或者总体技术负责人完成国家多项国家重大工程任务；作为项目或技术负责人完成国家级网络安全实验平台、国家网络安全应急关键技术、人工智能安全国家开放创新平台等重大研究项目近十项；作为核心负责人推动建立了国家网络安全应急响应体系与大量国际合作。在多个国家级智库担任专家，参与大量网络空间安全战略研究。此外他拥有丰富的产业经验，曾任阿里巴巴集团技术副总裁和首席安全专家，从产业视角建立安全能力体系，主导提出并推动数据安全能力成熟度DSMM成为业界广泛使用的国家标准。曾任360集团副总裁、首席安全官和安全技术委员会主席，推动面向未来的数字安全能力体系研究。目前在重点推动智能汽车安全技术与能力体系、智慧应急与智能安全以及相关技术和管理交叉学科融合、数据与智能安全国际合作等方面工作。

7）赵永望，教授/博导。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AI/LLM软件开发、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、ACM TOSEM、IEEE TDSC 等期刊和OOPSLA、ICML、CAV、FM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。

8) 王小航，教授/博导，国家级青年人才计划入选者，现任浙大计算机信息安全系系主任。毕业于浙江大学信电系，曾在华南理工大学软件学院任教。研究方向为大模型软硬件协同加速、智能车安全、领域专用众核芯片等。发表包括IEEE/ACM Trans顶级期刊和DAC顶级会议在内的论文70余篇，获得包括VLSI-SoC在内的两项芯片设计与硬件安全领域著名会议最佳论文奖，主持20项科研项目，包括5项国家级科研项目。担任CCFDAC 组织委员会副主席、CCF芯片大会论坛主席、JCR 1区期刊Mathematics等多个顶级期刊的客座主编。成果在某部、国家重点单位中国电子科技集团、多家公司应用。

9) 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、人工智能安全、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百余篇；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；获安全四大顶会之一2026年网络与分布式系统安全研讨会（NDSS）杰出论文奖、 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。

10)张帆，教授/博导，国家重点研发计划项目首席科学家，中央网信办重要人才，浙江省商用密码学会副理事长。2012年博士毕业于美国康涅狄格大学。2014 年加入浙江大学。近5

年在网络安全、人工智能、硬件安全等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。获COSADE2012、ChinaCrypt2018、AsianHOST 2019、CryptoTE 2021、SAFE2025会议等6项最佳论文奖。出版《密码故障分析与防护》、《侧信道分析与防御》和《集成电路硬件安全》等5本著作/教材。2020-2021年担任国际会议PROOFS的程序委员会主席，2022年中国密码测评会组织委员会主席，并担任 DAC、CHES、DATE等重要国际会议的TPC成员。主持（承担）科技部重点研发计划、国家自然科学基金联合基金重点、国防基础加强计划、国家密码科学基金、浙江省重点研发等国家级和省部级项目。获北京市科技进步奖二等奖、商业联合会一等奖等省部级科技进步奖5项。指导研究生获得国家奖学金5人次。指导研究生获网络安全“强网杯”恶意流量检测全国冠军2次，获“全国研究生创芯大赛”一等奖1项、二等奖5项、专项一等奖2项，获优秀指导教师称号。

11）林峰，长聘副教授/博导，入选教育部青年长江学者，浙江省千人计划专家，ACM中国安全分会新星奖获得者。曾任浙江大学信息技术中心副主任（双专）。研究方向为智能网联车安全、人工智能安全和物联网安全。在以上领域共发表140余篇高水平论文，引用5400余次，包括发表在安全四大顶会(Oakland、Security、CCS、NDSS)，移动计算顶会(MobiCom、MobiSys、SenSys)，人工智能顶会（CVPR、AAAI、MM）以及顶级期刊TDSC、TIFS、TNET、TMC等。参与英文编著一部，标准制定两项。主持国家自然科学基金联合基金重点项目，面上项目，JKW国防项目，浙江省基金重点项目，以及与华为、浙数集团、浙商银行等企业合作的横向项目，参与科技部重点研发课题、浙江省领军型创新创业团队等项目。研究工作入选SIGMOBILE Research Highlights (国内单位首次)，IEEE-JBHI 期刊封面文章。获6项最佳论文奖和提名奖，包括MobiSys'20、Globecom'19、CHASE'22、BHI'17 最佳论文奖，SenSys'21、INFOCOM'21最佳论文提名奖；获HotMobile'18最佳演示奖。担IEEE TIFS、IEEE Network Magazine、IET Information Security、Security and Communication Networks等多个知名SCI期刊编委，ACM Morse'22 会议TPC主席，MobiCom、SenSys、MobiHoc、IPSN、INFOCOM、MM等多个国际会议TPC成员。科研成果在华为、北京市公安、杭州城市大脑等单位落地应用。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，全国人工智能创新应用大赛总决赛二等奖、中国机器人及人工智能大赛总决赛城市道路自动驾驶赛道二等奖、沃达丰全球无线创新项目提名奖等。

12) 申文博，长聘副教授，博士生导师，CCF系统软件专委执行委员，体系结构专委执行委员。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，硅谷）操作系统内核安全的技术负责人，2019年回国加入浙江大学计算机科学与技术学院。研究方向为操作系统安全，AI系统安全，云原生系统安全，软件供应链安全。在IEEE S&P, ACM CCS, USENIX Security, ASPLOS等计算机安全、系统、网络国际顶级会议、期刊发表论文60余篇，获得ESORICS 24, ACSAC 22, AsiaCCS 17, NDSS 16 (CCF-A)等4项国际会议杰出论文奖，其中作为唯一通讯作者获得 ESORICS 24(CCF-B 类国际会议)唯一的杰出论文奖(1/535)和 ACSAC 22(CCF-B 类国际会议)杰出论文奖(3/303)，均是国内第一单位首次获得。主持科技部重点研发课题、国家自然科学基金-面上项目、青年科学项目等十余项科研项目。设计并流片浙大安全芯-求是一号（28纳米工艺），包含多种新型安全机制，与业界最新广泛部署ARM芯片安全方案相比具有显著优势。设计、实现并主导部署了体系化操作系统保护方案，部署超过亿部设备。研究成果获得蚂蚁学术合作优秀项目，系统与数据安全联合实验室优秀合作奖等奖项，并获得人民网、光明网专题报道。主导浙江大学操作系统课程和计算机系统贯通课程教学改革，主持省级教改项目《CPU-操作系统贯通人才培养课程建设》。被评为24年高校计算机专业优秀教师，22年教育部-华为“智能基座”优秀教师，浙江大学校级优秀班主任；获得第二届网络空间安全产学协同育人优秀案例一等奖等奖励。指导多名研究生获得国家奖学金、省奖学金和浙江大学奖学金；指导学生获得全国大学生计算机系统能力培养大赛（龙芯杯）一等奖，逐梦杯一等奖，全国大学生信息安全竞赛一等奖等奖项，本人获得 4次全国大赛优秀指导教师奖。 英文主页https://wenboshen.org/。

13) 张秉晟，浙江大学计算机科学与技术学院/网络空间安全学院长聘副教授、博士生导师，国家级青年人才项目获得者、科技部重大科研项目首席科学家、中国密码学会密码数学理论专业委员会委员、SIGSAC China委员、CCF高级会员；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70余篇：包括Eurocrypt、Asiacrypt、PKC、Usenix Security、S&P、CCS、NDSS等密码学和安全领域顶级会议，撰写专著《隐私保护机器学习》，以主编身份在第三届全球数字贸易博览会上发布《2024全球隐私计算报告》。回国前，张秉晟曾任英国兰卡斯特大学助理教授、信息安全学科带头人、网络安全系主任。近年来，

张秉晟主要致力于我国的国际标准推进工作，任ISO/IEC 27565《基于零知识证明的隐私保护指南》主编，ISO/IEC 26226《隐私增强技术在消费者隐私设计中的应用》主编，ISO/IEC 27574《脑机接口隐私》联合编辑等；获2024年度全国网络安全标准化技术委员会标准化工作先进个人奖。

14）刘健，长聘副教授/博导，国家级青年人才，浙江大学金融科技安全国际研究中心副主任。2018 年 7 月获芬兰阿尔托大学博士学位， 曾就职于加州大学伯克利分校。其研究领域涵盖应用密码学、隐私计算、分布式系统、区块链、人工智能。曾获CCF-A类期刊最佳论文奖、华为奥林帕斯先锋奖、中国电子学会最佳论文奖等多个重要奖项。根据谷歌学者(Google Scholar)的统计，他的论文引用近3000次，单篇引用达千余次。更多信息欢迎参见https://person.zju.edu.cn/jianliu。

15）刘金飞，百人计划研究员，博士生导师，国家高层次青年人才，浙江省杰青，小米青年学者。2017年博士毕业于美国埃默里大学，荣获埃默里大学毕业生最高荣誉“Chris Schoettle杰出研究奖”，毕业后在佐治亚理工学院和埃默里大学任博士后研究员。刘金飞博士主要从事数据要素交易、数据安全与合规等方向的研究工作。发表了60余篇同行评议的会议与期刊论文，其中CCF-A类论文50余篇，荣获包括CCF-A类顶会CCS杰出论文奖在内的多个奖项，设计了全球首个以机器学习模型为交易对象的数据要素交易架构。担任ACM TKDD和AILET副主编，是数据库领域所有旗舰会议（e.g., VLDB, SIGMOD, ICDE）和其他领域旗舰会议（e.g., CCS, NeuIPS, KDD, SIGIR, WWW）的程序委员会委员，参与国标《数据交易安全服务》和国际IEEE数字水印标准制定，主持国家自然科学基金、国家重点研发计划课题和浙江省杰出青年科学基金。

16）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。研究工作围绕深度合成与检测、AIGC安全、物联网安全、隐私保护等方向展开。在S&P，CCS，NDSS，Usenix Security，TDSC，TIFS等CCF-A类国际会议及期刊中发表多篇论文。主持国家自然科学基金面上项目并担任国家重点研发计划项目课题负责人。担任ACM CCS, IEEE ICDCS等多个国际著名会议的TPC成员以及IEEE

IoT-J的编委。多项研究成果在工业界具有广泛应用，受到包括CCTV，NSF News在内的80多家媒体报道。其在加速计窃听方面的工作促使谷歌优化安卓系统权限管理机制。AIGC安全方面的工作得到Midjourney与Stability AI的认可并用于产品提升。

17)杨子祺，浙江大学百人计划研究员，博士生导师。本科毕业于华中科技大学，博士毕业于新加坡国立大学。担任CCF网络与系统安全专委会执行委员，长期担任网络与信息安全领域四大顶会IEEE S&P、ACM CCS程序委员会委员，CCF-A类会议AAAI、MM、NeurIPS等程序委员会委员，担任TDSC、TIFS 等顶刊常驻评审。深度参与制定强制性国家标准GB 45438-2025《网络安全技术 人工智能生成合成内容标识方法》，研发强制性标准配套服务平台GCmark。曾获ACM AISec最佳审稿人、全国大学生信息安全竞赛优胜奖指导教师等奖项。主讲课程获评浙江省“名师名课”省级一流课程、入选教育部国家高等教育智慧教育平台人工智能通识课程。研究方向包括人工智能安全、大模型安全、智能体安全，发表安全四大论文及CCF-A类论文20余篇，主持和参与国家自然科学基金项目、科技部重点研发计划项目等多个国家级科研项目。

18) 许海涛，百人计划研究员/博导。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，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。曾作为团队核心成员参与美国国防部高级研究计划局（DARPA）透明计算（TC）项目，负责开发针对高级持续威胁（APT）的检测及追溯机制。截止目前，已承担科技部重点研发计划、国家自然科学基金委面上、以及JWKJW重大专项等多项国家级科研项目。研究成果先后发表在USENIX Security，NDSS，ICSE，WWW，IMWUT/UbiComp，INFOCOM，TIFS等国际顶级会议以及期刊，并获WWW最佳论文提名奖，相关成果被华尔街日报、中国日报等主流媒体报道。课题组毕业生就业去向涵盖高校教职、国家部委特招岗位，以及知名科技企业和大型金融机构。

19) 沈浩颋，百人计划研究员/博导。于2014年在美国宾夕法尼亚州立大学完成博士学位；先后在美国国家标准与技术研究院（NIST）和佛罗里达大学电子工程和计算机科学系、内华达大学计算机系担任博后、副研究员(research associate)和长聘序列助理教授，从事安全研究工作。申请人从芯片安全出发，结合物联网和去中心化的应用场景，在安全电路

设计、芯片身份认证等方面开展研究工作，取得了一系列科研成果。相关研究有 40 余篇论文和报告收录于安全相关的期刊会议，引用 1000 余次、H因子15，包括以一作、共同一作或通讯作者身份发表在TC（CCF-A）、DAC（CCF-A）、CHES（硬件安全顶会），和TVLSI（芯片设计顶刊）的论文等，取得10余项中美专利，参与编撰安全领域前沿技术介绍书籍2部。

20）杨坤，百人计划研究员（第一类），海外优青（A类），博导，杭州高新区（滨江）区块链与数据安全研究院副院长。主要研究方向包括芯片安全架构、大模型推理优化、智能网联车安全等。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。2018-2022年任美国英伟达公司总部高级架构师。主持国家重点研发计划课题、国家自然科学基金面上项目、国家自然科学基金优秀青年科学基金项目（海外）、浙江省“尖兵”研发攻关计划课题等国家级和省级项目，以及华为、蚂蚁、吉利、地平线等企业横向项目。发表国际高水平论文近30篇，获授权美国专利5项和中国专利9项，登记软件著作权2项。担任ACM SIGSAC China委员、CCF高级会员、CCF容错计算专委执行委员、CCF体系结构专委执行委员、Electronics期刊客座主编、第七届电路与系统国际会议程序委员会主席，长期担任DAC、USENIX VehicleSec等多个国际会议程序委员会委员和近20项刊顶会审稿人。获2023年海外优青（A类）、2022年杭州市西湖明珠工程海外高层次人才青年人才、2022年浙江大学启真优秀青年学者、ICML 2026 杰出审稿人银奖、《网络空间安全科学学报》2024-2025年度优秀学术论文、2021年英伟达专利奖、2020年英伟达NTECH会议最佳论文奖唯一一等奖，及2016年IEEE HOST最佳论文奖提名。指导学生获小米特等奖学金、浙江大学校级优秀毕业研究生、浙江大学毕业研究生奖学金、“铸网—2024”网络安全实网攻防演练最佳攻击队伍、2025“招商铸盾”智能网联汽车攻防赛优秀奖、NVDB-CAVD杯汽车信息安全总决赛二等奖1次和三等奖2次、第一届HISEC杯全国高校汽车信息安全挑战赛优秀奖、浙江省大学生网络与信息安全竞赛二等奖2项和三等奖2项。带领浙大“天下一”战队参与“铸网—2024”、NVDB-CAVD杯汽车信息安全竞赛，累计获得12项工信部漏洞编号和3项超高危原创漏洞证书。参编白皮书2项、国际标准4项、国家标准3项、行标2项。

21） 李松，浙江大学百人计划研究员，博导。国家重点研发计划项目首席科学家，入选

中国科协青年人才托举工程。博士毕业于美国约翰斯霍普金斯大学计算机科学学院。主要研究方向为漏洞挖掘、软件安全、AI辅助安全等。在安全领域四大顶会（CCS、USENIX Security、NDSS，IEEE S&P），软件领域顶会ESEC/FSE等会议发表均有论文发表。担任安全领域四大顶会IEEE S&P、USENIX Security、ACM CCS等国际顶尖学术会议的学术委员会委员。主持国家重点研发计划项目、基金委青年项目以及来自华为、蚂蚁、中国联通等公司的多项项目。主持开发洞锋、ODGen等漏洞挖掘平台，共挖掘零日漏洞1000余个，获得数百个CVE编号，获得IEEE S&P 2025年度、ACM CCS 2023年度杰出论文奖等奖项。

22） 张聪，百人计划研究员/博导，国家级青年人才。 2020年获得罗格斯大学博士学位并于同年加入马里兰大学任职博士后研究员，2022年9月加入浙江大学网络空间安全学院，任职百人计划研究员。入选2022年度国家自然科学基金优秀青年基金项目（海外）与科技部2023年度国家重点研发网络空间安全专项青年科学家项目。获得2023年度ACM China 新星提名奖与2023年度ACM SIGSAC China新星奖。研究方向为理论密码学和应用密码学，具体包括，安全计算模型分析，抗量子安全密码算法与分析；在CRYPTO，Asiacrypt与TCC等密码学顶级会议上发表论文8篇。

23）罗梦，百人计划研究员/博导/海外优青。研究方向：移动应用安全、智能体安全、漏洞挖掘、Web安全等，研究内容主要围绕利用大模型与智能体提升智能终端中软件与系统安全，以及利用漏洞挖掘与程序分析等提升大模型应用及智能体安全。博士毕业于美国纽约州立大学石溪分校，曾任美国东北大学博士后研究员，于2022年10月加入浙江大学计算机科学与技术学院。近三年，主持国家重点研发计划课题、国家自然科学基金面上等多个国家级项目，与中国联通、华为、蚂蚁等头部企业有项目合作。研究成果发表在ACM CCS、NDSS、TDSC、FSE、WWW、TKDE等网络安全四大国际顶会和CCE-A类国际顶级期刊和会议上。研究成果具有较强应用价值，荣获谷歌、阿里巴巴、华为等国际知名厂商的漏洞报告认可奖励。实验室也注重科研思维和综合实践能力培养。在社会服务方面，目前担任ACM TOPS（CCF-B）的副编辑，长期担任ACM CCS、Usenix Security、NDSS等安全四大顶会的程序委员会委员，以及ACM SIGSAC China委员、中国电子学会-网络空间安全专家委员会委员等。

24) 冯博，百人计划研究员/博导/国家优秀青年科学基金（海外）项目获得者。研究领域包括：软件与系统安全、机器人/无人机安全、AI驱动的程序分析与二进制逆向、基于智能体的漏洞挖掘。博士毕业于美国东北大学，师从卢龙教授（现任蔚来汽车副总裁、首席数字安全官），曾在美国佐治亚理工学院担任博士后研究员，合作导师：Prof. Wenke Lee (John P. Imlay Jr. Chair, ACM Fellow, IEEE Fellow)和Prof. Sukarno Mertoguno。主要成果发表在IEEE S&P、USENIX Security等安全领域四大国际顶会，IEEE TDSC等CCF-A类高水平期刊上。研究构建首个完全基于模拟器的自动化嵌入式固件漏洞挖掘平台，基于首创的处理器—外设接口建模机制，发现12个高危零日漏洞。11个国家、二十多所国际知名高校的领域专家使用该平台，10余篇CCF-A类高水平会议论文使用该测试集作为测试基准。主持国家重点研发计划课题、国自然面上基金、某重大专项项目等国家级项目5项，主持多项华为的校企合作项目，曾作为骨干成员参与美国国防部高级研究计划局（DARPA）、美国国家科学基金会（NSF）等资助的多个大型项目，总资助金额超过2000万美元。多次受邀担任网络安全四大国际顶会ACM CCS、NDSS、USENIX Security等国际高水平学术会议程序委员会委员，并担任ACM SIGSAC China委员。2023年荣获浙江大学“启真优秀青年学者”荣誉。

25) 李晓白，浙江大学百人计划研究员，博导，浙江省千人。本科毕业于北京大学，硕士毕业于中科院大学，博士毕业于芬兰奥卢大学。获得芬兰科学院博后奖金，2020年至2023年4月在芬兰奥卢大学担任tenure track助理教授，主持芬兰科学院、芬兰工作环境基金会等多个科研项目，并荣获奥卢大学2019最具科学领导力的青年学者奖。2023年底加入浙江大学网络空间安全学院，兼任奥卢大学客座教授。研究领域包括机器视觉、机器学习、情感计算、生物识别等。具体方向有微表情识别、基于视频的远程生理信号测量、生物特征识别、人脸活体检测、对抗攻击和伪造检测、多模态情感识别和内容生成等等。发表期刊和会议文章80余篇，包括高水平期刊和会议文章如IEEE PAMI、TAC、SPM、PIEEE、IJCV、ICCV、CVPR等20余篇，谷歌学术检索H指数43，总引用11500，入选2022至2025年全球2%高被引学者。IEEE高级会员，IEEE MLSP委员会委员，ELLIS会员，CSIG情感计算与理解专委会常委，担任IEEE-TMM、CVIU和IVC期刊副编辑。关于微表情的研究被麻省理工科技评论报道，远程心率测量文章获IEEE芬兰区2020年最佳学生论文奖。个人网页 https://xiaobaili-uhai.github.io/。

26) 刘振广，百人计划研究员/博导。新加坡国立大学博士后，中央网信办网信创新人才、浙江省高层次特殊人才支持计划青年拔尖人才、首批浙江省高校领军人才青年优秀人才，在人工智能安全和区块链安全方向发表CCF-A类、ACM/IEEE Transactions等高水平论文100余篇,以第一或通讯作者发表国际顶级CCF-A类论文40余篇，涵盖TPAMI、NDSS、TIFS、TDSC、TKDE、CVPR、NerIPS、ICCV、WWW、AAAI、ACM MM等顶会顶刊，谷歌引用7000余次，长期坚持论文代码开源。获IJCAI 2020(CCF-A类)最佳论文候选，软件学报高影响力论文、IEEE CCIS最佳论文提名奖，KSEM最佳论文提名奖、ChinaMM最佳学生论文奖等。主持工信部揭榜挂帅项目、国家重点研发计划课题、国家自然科学基金面上项目、浙江省重点研发计划项目等国家级省部级项目20余项。作为第一完成人获浙江省科技进步二等奖，作为第二完成人获中国电子学会科技进步二等奖。与蚂蚁，央行数字货币研究所，阿里云，国家电网，上期所等行业头部企业积累了长期科研与产业合作关系。

27) 姚培森，百人计划研究员、博导， CCF形式化方法专委、理论计算机科学专委执行委员，ACM SIGPLAN、SIGSAC会员，入选国家级高层次青年人才计划。主要研究方向为编程语言(程序分析与验证、程序合成与优化)、数理逻辑(自动定理证明)、软件安全(漏洞挖掘)。相关成果发表于编程语言(PLDI, OOPSLA)、形式化方法(CAV)、软件工程(ICSE, FSE, ISSTA, ASE, TOSEM)、安全(S&P, USENIX Security, TDSC)、系统(ASPLOS)等领域的CCF-A会议或期刊(包括浙大第一篇PLDI);获编程语言领域旗舰会议OOPSLA杰出论文奖、SIGSOFT杰出论文奖、Google Research Paper Rewards等奖项，发现Linux内核、MySQL数据库、Firefox浏览器等开源软件数百真实缺陷，在蚂蚁、腾讯、华为等公司的金融、嵌入式系统得到实际部署。担任相关领域顶级会议(POPL, PLDI, OOPSLA, FSE, ISSTA, ASE, CCS等)程序委员会委员(其中POPL, PLDI, OOPSLA均为浙大首次）。更多信息参见个人主页 https://rainoftime.github.io/

28) 褚志轩，百人计划研究员/博导。博士毕业于美国佐治亚大学。曾任职于阿里巴巴和蚂蚁集团，负责大模型预训练和应用，推动了大语言模型、多模态大模型在实际场景中的落地。主要研究方向为安全可信大模型，包括大模型可信性、安全性、可解释性和因果性，同时兼顾大模型与图神经网络、视觉智能、推荐系统等前沿技术的结合。在人工智能、数

据挖掘和数据库领域的顶级期刊和会议，如NeurIPS、ICLR、CCS、IJCAI、AAAI、ACL、KDD、ICDE、TKDD、TNNLS等发表40余篇论文，研究成果在业界和学界产生了广泛影响。同时，还多次应邀担任NeurIPS、ICLR、IJCAI、AAAI等国际顶级会议的程序委员会委员和领域主席，组织主持多次tutorials 和workshops。

29）倪王泽，浙江大学百人计划研究员，博士生导师，浙江大学-元杰瑞智机器人异构集群联合研发中心执行主任，国家级青年人才项目获得者，担任中国计算机学会区块链专业委员会执行委员和信息系统专业委员会执行委员。主要研究领域包括人工智能安全、大模型推理效率优化、时空数据库和区块链，相关智库报告获得部委领导批示，在CCS、NDSS、ICML、SIGMOD、VLDB、ICDE、WWW、TKDE和SIGKDD等CCF A类顶级国际学术会议和期刊上发表论文二十余篇。多年担任VLDB、ICDE等CCF A类顶级国际学术会议技术委员会委员，与TKDE、TPDS、TDSC、TMC等国际顶级期刊审稿人。

30）郑天航，百人计划研究员/博导/国家优秀青年科学基金（海外）项目获得者。郑天航研究员致力于人工智能多维度攻防的研究。在人工智能安全领域，他近五年发表20篇左右论文，以第一作者发表7篇CCF-A长文。这些论文分别发表于 TDSC、CCS、NDSS、ICML、TIFS、AAAI、ICCV、IJCAI、INFOCOM、UAI、EMNLP、MLSys 等会议期刊。根据谷歌学术搜索（Google Scholar），他的研究工作被引用超2000次。此外，他主持了国自然面上项目等多项国家级/省部级项目课题，他还担任了 IEEE TCSVT的编委与人工智能顶会 ICML 和NeurIPS 的领域主席。

31）卜凯，副教授/博导，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， 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，体系结构安全。曾在 MICRO、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。

32) 吴磊，副教授/博导，也是业内知名的区块链安全研究团队BlockSec Team的联合创始人。2015年毕业于美国北卡州立大学获得计算机科学博士学位，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，聚焦于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，在智能合约安全领域开展相关研究和探索。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。

33) 常瑞，副教授/博导，CCF杰出会员、CCF体系结构、系统软件、形式化方法专委委员，全军优秀教师，曾获ACM中国优秀博士学位论文分会奖。研究方向包括体系结构及系统安全、形式化方法等，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，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)、全国大学生信息安全大赛优秀指导教师（2022年国赛一等奖）、TCTF金牌指导教师（2023年全国总冠军）。更多信息欢迎参见个人主页 https://person.zju.edu.cn/changrui 。

34) 卢立，特聘研究员/博导。IEEE/ACM/CCF高级会员，CCF网络与系统安全专委、普适计算专委执委，IEEE VTS自动驾驶汽车专委委员，IEEE TIFS、ACM IMWUT编委。曾获国家留学基金委资助访问美国罗格斯大学。在CCF-A国际期刊/会议上发表40余篇论文，包括IEEE S&P、USENIX Security、IMWUT/UbiComp、TIFS、ToN等。主持国家重点研发课题、国自然基金面上、浙江省领雁项目、浙江省自科基金、华为/蚂蚁公司横向等项目。获IEEE ICC最佳论文奖，2项MobiCom最佳海报展示提名奖，ACM SIGAPP China新星奖，华为联合实验室优秀合作奖等奖项。指导学生获国自然青年学生基础研究项目（博士研究生）、中科协青托博士生专项、全国网安学院学生创新资助项目、全国大学生信安竞赛三等奖、浙江大学未来学术新星项目等。担任ACM BCB的AC，IEEE ICC奖励委员会委员，USENIX Security, INFOCOM, IWQoS, VehicleSec等国际会议的TPC。具体信息详见:https://person.zju.edu.cn/lynnluli。

35) 张明雪，特聘研究员、博士生导师。2022年博士毕业于香港中文大学，研究方向为Web安全和软件安全，包括(1)软件漏洞挖掘，(2)Web安全攻防，(3)软件隐私合规分析等。研究成果全部发表于CCF-A类顶级学术会议，包括USENIX Secuity，IEEES&P，CCS，ICSE，ESEC/FSE，WWW等论文十余篇，受邀担任 NDSS 2025，ICSE 2025，ISSTA 2024，TON 2023，ESEC/FSE 2023等国际顶级学术会议及期刊审稿人。获CCS 2024杰出论文奖、浙大启真优秀青年学者等荣誉，DataCon 2023漏洞挖掘赛道二等奖队伍指导老师，主持和参与多项横纵向项目。更多信息见个人主页：https://zhangmx1997.github.io/

团队主要成员

序号	姓名	职称	研究方向	联系方式
1	任奎	求是讲席教授	数据安全与隐私保护、人工智能安全、智能设备与车联网安全	kuiren@zju.edu.cn
2	秦湛	长聘副教授	人工智能安全、数据安全与隐私保护技术	qinzhan@zju.edu.cn
3	王志波	教授	智能物联网、人工智能安全、数据安全与隐私保护、边缘智能与安全	zhibowang@zju.edu.cn
4	杜文亮	求是讲席教授	计算机网络和系统安全、面向网安的网络仿真、网安实际教育	Wenliangdu@zju.edu.cn
5	吴强	求是特聘教授	新一代信息网络理论与关键技术、移动互联网理论与关键技术、算力/智算网络、确定性网络、云网基础设施智能与优化、网络空间安全	wu.qiang@zju.edu.cn
6	杜跃进	求是特聘教授	网络安全与应急管理、数据安全、人工智能安全、智能制造安全、数字城市安全	du_yuejin@zju.edu.cn

7	赵永望	教授	操作系统安全、形式逻辑与验证、	zhaoyw@zju.edu.cn
8	王小航	教授	AI智算芯片与系统建模与优化，AI算力底座安全	xiaohangwang@zju.edu.cn
9	韩劲松	教授	物联网安全、人工智能安全、可信认证、智能感知和移动计算	hanjinsong@zju.edu.cn
10	张帆	教授	网络安全、密码学、硬件安全、	fanzhang@zju.edu.cn
11	林峰	长聘副教授	智能网联车安全、人工智能安全、物联网安全	flin@zju.edu.cn
12	申文博	长聘副教授	操作系统安全，智能系统安全，xPU安全，自动化攻防	shenwenbo@zju.edu.cn
13	张秉晟	长聘副教授	密码学为核心的安全多方计算、零知识证明、联邦学习、可证明安全等隐私计算技术	bingsheng@zju.edu.cn
14	刘健	长聘副教授	应用密码学、隐私计算、分布式系统、	jian.Liu.work@zju.edu.cn
15	刘金飞	百人计划研究员	数据要素市场、数据安全与合规、	jinfeiliu@zju.edu.cn
16	巴钟杰	百人计划研究员	深度合成与检测、AIGC安全、物联网安全、隐私保护	zhongjieba@zju.edu.cn
17	杨子祺	百人计划研究员	人工智能安全、大模型安全、智能化攻防	yangziqi@zju.edu.cn
18	许海涛	百人计划研究员	网络黑灰产治理、大语言模型隐私与安全、攻击检测溯源、以及Web安全	haitaoxu@zju.edu.cn

19	沈浩颋	百人计划研究员	硬件安全，车安全，大模型硬件安全	htshen@zju.edu.cn
20	杨坤	百人计划研究员	芯片安全架构、大模型推理优化、智能网联车安全	kuny@zju.edu.cn
21	李松	百人计划研究员	漏洞挖掘，软件安全，AI辅助安全	songl@zju.edu.cn
22	张聪	百人计划研究员	理论密码学，抗量子安全密码算法与分析	congresearch@zju.edu.cn
23	罗梦	百人计划研究员	移动应用安全、智能体安全、漏洞挖掘、Web安全	meng.luo@zju.edu.cn
24	冯博	百人计划研究员	软件与系统安全、机器人/无人机安全、AI驱动的程序分析与二进制逆向、基于智能体的漏洞挖掘	bo.feng@zju.edu.cn
25	李晓白	百人计划研究员	机器视觉、人工智能、生物识别、合成与伪造检测、情感计算	xiaobai.li@zju.edu.cn
26	刘振广	百人计划研究员	人工智能安全、区块链安全	Liuzhenguang@zju.edu.cn
27	姚培森	百人计划研究员	程序分析与验证、程序合成与优化、逻辑与定理证明	pyaoaa@zju.edu.cn
28	褚志轩	百人计划研究员	大模型预训练与强化学习，智能体开发应用，大模型与智能体安全可信，大模型可解释	Zhixuanchu@zju.edu.cn
29	倪王泽	百人计划研究员	人工智能安全、大模型推理效率优化、时空数据库与区块链	Niwangze@zju.edu.cn
30	郑天航	百人计划研究员	人工智能安全，隐私保护	zthzheng@zju.edu.cn

31	卜凯	副教授	网络安全，体系结构安全	kaibu@zju.edu.cn
32	吴磊	副教授	区块链安全、系统安全	lei_wu@zju.edu.cn
33	常瑞	副教授	系统安全、形式化方法	crix1021@zju.edu.cn
34	卢立	特聘研究员	智能语音安全、自动驾驶安全、物联网安全、普适计算	li.lu@zju.edu.cn
35	张明雪	特聘研究员	软件安全、Web安全	mxzhang97@zju.edu.cn