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2017年成立网络空间安全研究中心，凝聚浙大多个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年浙江大学网络空间安全学院正式成立，由ACM/IEEE会士任奎担任院长，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。经过三年多的建设，中心在师资队伍、科学研究、人才培养、成果转化、国际影响等方面形成了明显的特色与优势，已成为国内外网络空间安全学术研究的重要力量。2020年浙大信息安全专业获评**教育部一流本科专业**，在2021年软科专业排名中评分A+，位列**全国第一**，在2022年著名CSRankings安全领域最新排名并列**亚洲第一、全球第七**。2022年软科中国最好学科排名，浙江大学网络空间安全学科位列**全国第三**。

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6人、百人计划研究员16人、副教授3人、特聘研究员4人、求是工程岗1人、求是科创学者5人、嘉兴研究院研究员8人及博士后多名。其中国家千人计划特聘教授1人、国家杰出青年基金获得者1人、国家千人计划青年项目入选者2人、浙江省千人计划入选者5人、浙江省万人计划文科领军人才1人、国家自然科学基金优青项目1人、优秀青年科学基金项目（海外）入选者4人。另有教师获得“高校计算机专业优秀教师奖励计划”、“全军优秀教师”等荣誉。科研实力受到国内外广泛认可。同时，组建了由多名外籍院士领衔的海外学术委员会，牵头主办及参加多场国际学术会议及讲座，并与海外著名高校的众多学者建立了长期广泛的科研合作，牵头主办了IWQoS2020（国际网络服务质量顶级会议）、DSC2019（国际网络空间数据科学大会）、APSys2019（综合网络规划亚太系统研讨会）等国际学术会议。

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2020年DEFCONCTF全球冠军、2021年DEFCONCTF全球冠军、第五届“强网杯”网络安全挑战赛最佳高校战队、中国高校计算机大赛网络技术挑战赛一等奖、第二届中国研究生创“芯”大赛决赛一等奖、第

五届计算机系统能力培养大赛“龙芯杯”一等奖、第五届“强网杯”人工智能挑战赛一等奖、第三届中国人工智能大赛A级、第十五届全国大学生信息安全竞赛一等奖等二十余项奖项。其中浙江大学网安学院AAA战队组成的A*O*E联合战队获**2020年DEFCONCTF这一世界顶级安全大赛冠军，打破国外院校CMU十余年的冠军垄断**。

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**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、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，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-数据安全与隐私保护实验室等多个产学研协同的研究中心和创新基地。

近三年来，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、GFXXX专项等**国家/省部级重大项目50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100余个，获得授权53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120余篇，获得20余项杰出论文奖。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世界广泛重视，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，浙江大学求是讲席教授，美国计算机协会（ACM）会士、美国电气电子工程师学会（IEEE）会士、中国计算机学会（CCF）会士，目前担任浙江大学网络空间安全学院院长，区块链与数据安全全国重点实验室副主任，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安全与隐私保护、人工智能安全、物联网安全等领域的研究。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，研究成果广泛应用在包括阿里、蚂蚁金服、华为等公司的产品和服务中。任奎教授获得了包括浙江大学首届国华杰出学者奖，IEEE通信学会CISTC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ACSAC'22、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。H-Index为89，文章总引用次数超过44,000次，授权发明专利30余项，连续入选科睿唯安高被引科学家。任奎教授现任教育部科学技术委员会委员、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中国安全分会主席以及浙江省海高会副会长，并担任了多个ACM和IEEE国际权威期刊编委，及国际一流会议主席或共同主席。

2) 韩劲松，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) 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。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。获国际会议COSADE2012、中国密码学会ChinaCrypt2018、亚洲硬件安全年会AsianHOST 2019、中国密码测评会CryptoTE 2021、

SAFE2021会议等5项最佳论文奖。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》。2020-2021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，2022年中国密码测评会组织委员会主席，并担任 DAC、CHES、DATE、AsiaCCS、ICICS、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。主持（承担）科技部重点研发计划、国家自然科学基金仪器仪表项目和面上项目、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。主持研发旁路采集和分析平台；获省部级科技进步奖二等奖2项。指导硕士生获得研究生国家奖学金4人次。指导硕士研究生获网络安全“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。

4) 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。

5) 王志波，教授/博导，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珞珈青年学者。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 50 余篇，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。。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省部级项目，并与华为、蚂蚁金服、阿里达摩院等公司有深度合作，受邀担任INFOCOM、WWW、KDD、ICDCS、AAAI等多个国际会议的大会程序委员。 现为IEEE/CCF/电子学会高级会员，CCF物联网专委会常委，电子学会网络空间安全专家委员会青年常委兼副秘书长，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。

6) 王小航，浙江大学网络空间安全学院教授，获广州市珠江科技新星。毕业于浙江大学信电系，曾在华南理工大学软件学院任教。研究方向隐私计算软硬件加速、芯片安全、智能汽车安全等。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，主持国家自然科学基金在内的16项科研项目。担任CCF芯片大会论坛主席、NoCS特别分会组织者、NoCArc会议指导委员会委员、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。

7) 周亚金，百人计划研究员/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）。

8) 秦湛，百人计划研究员/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，他参与推进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前沿研究者之一；在人工智能安全领域，他在包括人工智能对抗性安全、数据毒化与后门检测攻防、恶意软件检测可解释性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 CCS、MM、SenSys、ICLR、KDD、VLDB、INFOCOM 等顶级国际学术会议上。根据谷歌学者（Google Scholar）的统计，他的文章总引用次数则超过 4000 次，h-index 33。他获得过包括ASIACCS、IWQoS最佳论文奖在内的多个奖项。

9) 林峰，百人计划研究员/博导。IEEE/CCF高级会员，浙江省千人计划专家，ACM中国安全分会新星奖获得者。研究方向为智能网联车安全、物联网安全、人工智能应用、和无线感知。在以上领域共发表100 余篇高水平论文，引用近 4000次，包括发表在安全四大顶会（Oakland，CCS、NDSS），移动计算顶会（MobiCom、MobiSys、SenSys、UbiComp），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面上项目，JW 科技委国防项目，以及与华为、浙数集团、光通天下等企业合作的横向项目，参与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/J-BHI 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、IEEE 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，Mobicom'22最佳海报论文提名奖。担任 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、INFOCOM等多个国际会议TPC成员。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、沃达丰全球无线创新项目提名奖等。相关工作被央视财经频道、光明日报、美国 NSF 新闻、ACM 通讯新闻等中外媒体广泛报道。

10) 申文博，百人计划研究员/博导。浙江大学计算机科学与工程系副主任，移动终端安全-浙江省工程中心副主任，CCF系统软件专委委员。研究方向为操作系统安全，云原生系统安全，软件供应链安全。在IEEE S&P, ACM CCS, USENIX Security, NDSS, DAC, ASPLOS, ACM MobiCom, TDSC, TMC等计算机安全、系统、网络国际顶级会议、期刊发表论文30余篇，覆盖全部计算机安全四大国际会议，获得3项杰出论文奖（NDSS 16, AsiaCCS 17, ACSAC 22）。主持国家自然科学基金、科技部重点研发课题等多项科研项目。研究成果被应用于保护超过亿部设备系统安全，并获得人民日报网络版专题报道。申文博研究员于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。常年活跃于系统/软件安全攻防的第一线，通过分析实际攻击，设计相应的系统保护方案，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软件及操作系统安全机制，部署超过亿部设备。

11) 张秉晟，百人计划研究员/博导，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专委会委员。他的主要研究方向是以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。回国前，他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。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 60 余篇:包括Eurocrypt、Asiacrypt、CCS、NDSS、INFOCOM等密码学和安全领域顶级会议，并撰写专著《隐私保护机器学习》。在科研项目方面，主持和参与了多个国家自然基金、教育部和科技部重点项目，并与阿里、蚂蚁、华为等头部企业保持着长期密切的合作关系。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、主导ISO 27565 基于零知识证明的隐私保护指南国际标准。

12) 刘健，百人计划研究员/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，他的论文引用达 1500 余次、单篇引用达600余次。更多信息欢迎参见https://person.zju.edu.cn/jianliu。

13) 刘金飞，百人计划研究员/博导。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。

14) 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。

15）杨子祺，百人计划研究员/博导。博士毕业于新加坡国立大学。主要从事人工智能安全、智能化攻防、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，包括二进制代码分析、安卓恶意代码检测与防御等。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）、以及人工智能顶级会议(AAAI)等国际顶级会议论文。现担任网络与信息安全领域顶级期刊 IEEE TDSC、 ACM TOPS 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，并担任深度学习安全国际会议 DLS 和嵌入式系统安全证明国际会议 PROOFS 的程序委员会委员。更多信息参见 https://person.zju.edu.cn/yangziqi。

16）许海涛，百人计划研究员/博导。2015年12月博士毕业于美国威廉与玛丽学院，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。曾作为团队主要成员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的检测及追溯机制。2020年12月加入浙江大学计算机科学与技术学院和网络空间安全学院以来，已承担包括国家自然科学基金委面上项目在内的多项国家级项目。主要从事网络欺骗防御、攻击检测溯源、Web安全、互联网黑灰产等方向的研究。研究成果获得华尔街日报，中国日报等主流媒体的报道。

17）沈浩硕，百人计划研究员/博导。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。

18) 杨坤，百人计划研究员/博导。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。曾于2014年5月至2014年8月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，车安全，微架构漏洞攻防。作为主要发明人已获授权2项美国专利，有1项国际专利已发表，另已提交2项国际专利申请和2项中国专利申请，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，单篇被引用68次，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，单篇被引用102次)，另有多次重要学术会议报告及硬件演示(IEEE HOST 2019, IEEE HOST 2017, and IEEE HOST 2016)。曾获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， 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年硬件安全领域顶级会议IEEE HOST最佳论文奖提名。

19) 李松，百人计划研究员/博导。博士毕业于美国约翰斯霍普金斯大学计算机科学学院。主要研究方向为移动安全、程序分析、漏洞挖掘以及网络安全等。在安全领域四大顶会（CCS、USENIX Security、NDSS，IEEE S&P），度量领域顶会IMC和系统软件领域顶会ESEC/FSE等会议发表均有论文发表。担任安全领域四大顶会USENIX Security、USENIX Security AE、CCF-A类学术会议TheWebConf等国际顶尖学术会议的学术委员会委员，以及Empirical Software Engineering、Computing Surveys等顶级期刊的审稿人,并作为骨干参与了由美国国防部高级研究计划局和美国国家科学基金委等资助的多个漏洞挖掘相关的核心项目。更多信息参见https://songli.io/。

20）张聪，百人计划研究员/博导。2022年度海外优秀青年项目入选者；于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；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，保序加密算法，以及不可微分安全框架等；在密码学领域旗舰会议CRYPTO，Asiacrypt和TCC发表多篇论文。

21）罗梦，百人计划研究员/博导。浙江大学百人计划研究员，博士生导师。研究领域包括：Web安全、物联网安全、网络犯罪检测、漏洞挖掘、数据驱动安全。博士毕业于美国纽约州立大学石溪分校，毕业后曾任美国东北大学博士后研究员。其研究致力于提升移动设备（包括智能手机、物联网设备等）和Web生态系统应对网络安全威胁的攻防对抗能力。近年来，主持1项国家自然科学基金项目，参与5项美国国家科学基金委（NSF）资助项目、2项美国海军研究办公室（ONR）资助项目等纵向项目，华为等企业横向项目。在安全四大国际顶级会议和CCF-A类计算机领域国际著名期刊和会议发表多篇文章，包括 ACM CCS、NDSS、WWW、TDSC、TKDE等。多次受邀担任网络安全四大国际顶会（如ACM CCS、NDSS），CCF-A类国际顶会（如WWW）等国际一流学术会议的程序委员会委员（TPC），承担论文评审工作。研究成果具有较强应用价值，报告的多个移动浏览器安全漏洞得到谷歌、阿里巴巴等知名浏览器厂商的确认及漏洞报告奖金，辅助修复了多个知名网站安全漏洞（如美国和俄罗斯的银行网站，中国、美国、巴西和印度的政府网站等）。

22）李晓白，百人计划研究员/博导，本科毕业于北京大学，硕士毕业于中科院大学，2017年博士毕业于芬兰奥卢大学。2019年获得芬兰科学院博后奖金，2020年8月至2022年11月在芬兰奥卢大学担任tenure track助理教授，期间主持芬兰科学院、芬兰工作环境基金会、Eudaimonia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年回国加入浙江大学网络空间安全学院。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、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60余篇，包括高水平期刊和会议文章如IEEE TPAMI、TAC、SPM、PIEEE、IJCV、ICCV、CVPR等十余篇，谷歌学术检索H指数31，总引用5400

（https://scholar.google.com/citations?user=JTFfexYAAAAJ ）。关于微表情的研究被MIT Technology Review报道，远程心率测量文章获IEEE芬兰区2020年最佳学生论文奖。

23) 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。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。

24) 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。

25) 常瑞，副教授/博导，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。

26) 卢立，特聘研究员/博导。分别于上海交通大学、西安交通大学获工学博士学位、工

学/管理学双学士学位。曾获国家留学基金委资助访问美国罗格斯大学。研究工作主要集中在智能物联网安全、语音对抗攻防、语音合成与检测、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40余篇论文，包括UbiComp、SenSys、INFOCOM、ICASSP、ToN等；获授权专利11项。获MobiCom 2019与2022年最佳海报展示提名奖，ACM中国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奖励。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INFOCOM, ICDCS, IWQoS等国际会议的TPC、及TMC, ToN, TDSC, TSC, IMWUT (UbiComp), ACM MM等国际期刊会议的审稿人。具体信息详见：https://person.zju.edu.cn/lynnluli。

27) 姚培森，特聘研究员，CCF形式化专委委员、ACM SIGPLAN会员。主要研究方向包括编程语言(程序分析与验证、程序合成)，计算机理论(定理证明)和软件安全(模糊测试)。相关成果发表在编程语言(PLDI, OOPSLA, ECOOP)、软件工程(ICSE, ESEC/FSE, ISSTA, ASE, TOSEM)、信息安全(S&P, USENIX Security)等领域的顶级会议和期刊；获得编程语言领域旗舰会议OOPSLA杰出论文奖、Google Research Paper Rewards等奖项；发现Linux Kernel、MySQL等开源程序上千个真实缺陷，在蚂蚁、腾讯、华为等公司的金融、嵌入式等系统中得到实际部署。担任相关领域顶级会议(PLDI'23, ISSTA'24, RAID'23)程序委员会委员，以及ACM TOPLOS, IEEE TR, ATVA、ESEC/FSE、ISSTA、ASE、VMCAI等期刊和会议审稿人。更多信息欢迎参见个人主页 https://rainoftime.github.io/

28) 张明雪，特聘研究员。2022年博士毕业于香港中文大学，研究方向为软件安全和Web安全，包括：(1)软件漏洞挖掘，(2)基于浏览器引擎的web安全风险检测与防御。2018-2022年间在上述领域CCF-A类学术会议发表论文6篇，包括USENIX Security, IEEE S&P, ESEC/FSE, WWW等软件工程和信息安全领域顶级学术会议论文。受邀担任ESEC/FSE 2023程序委员会委员和Empirical Software Engineering期刊审稿人。更多信息欢迎参见个人主页：https://zhangmx1997.github.io/

29) 刘振广，特聘研究员。新加坡国立大学博士后，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，在计算机视觉、区块链和人工智能方向发表CCF A类、ACM/IEEE Transactions等高水平论文80余篇，以第一或通讯作者发表国

际顶级的CCF A类论文20余篇，涵盖PAMI、CVPR、TKDE、TIFS、TDSC、ICCV、WWW 、AAAI 、IJCAI、 ACM MM等视觉和人工智能领域各顶会顶刊，长期坚持论文代码开源。获IJCAI 2020最佳论文候选，获IEEE CCIS最佳论文提名奖，China MM最佳学生论文奖等。主持国家重点研发计划课题、国家自然科学基金、浙江省重点研发计划项目等国家级省部级项目10余项。作为项目负责人获浙江省科技进步二等奖。承担蚂蚁，华为，上期所，中国高铁等行业顶级企业横向项目。

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、物联网安全	Kuiren @zju.edu.cn
2	韩劲松	教授	物联网安全、可信认证、 智能感知、移动计算	Hanjinsong @zju.edu.cn
3	张帆	教授	网络安全、密码学、硬件安全、 芯片设计、人工智能	Fanzhang @zju.edu.cn
4	赵永望	教授	操作系统安全、形式逻辑与验证、 编程语言原理	Zhaoyw @zju.edu.cn
5	王志波	教授	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	Zhibowang @zju.edu.cn
6	王小航	教授	隐私计算软硬件加速、芯片安全、 智能汽车安全	Xiaohangwang @zju.edu.cn
7	周亚金	百人计划研究员	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	yajin_zhou @zju.edu.cn

8	秦湛	百人计划 研究员	数据安全与隐私保护、人工智能安全	Qinzhan @zju.edu.cn
9	林峰	百人计划 研究员	智能网联车安全、物联网安全、 人工智能应用、无线感知	Flin @zju.edu.cn
10	申文博	百人计划 研究员	操作系统安全，云原生系统安全， 软件供应链安全	Shenwenbo @zju.edu.cn
11	张秉晟	百人计划 研究员	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
12	刘健	百人计划 研究员	应用密码学、隐私计算、分布式系统、区块链、人工智能	Jian.Liu.work @outlook.com
13	刘金飞	百人计划 研究员	数据要素市场、数据安全与合规、 数据查询	Jinfeiliu @zju.edu.cn
14	巴钟杰	百人计划 研究员	物联网安全、深度伪造、 隐私保护、智能感知	Zhongjieba @zju.edu.cn
15	杨子祺	百人计划 研究员	人工智能安全、智能化攻防、 数据安全与隐私保护	Yangziqi @zju.edu.cn
16	许海涛	百人计划 研究员	网络欺骗防御、攻击检测溯源、 Web安全、互联网黑灰产	Haitaoxu @zju.edu.cn
17	沈浩頲	百人计划 研究员	硬件安全、物联网安全、区块链、 智能制造	Htshen @zju.edu.cn
18	杨坤	百人计划 研究员	硬件安全、芯片安全架构、车安全、 微架构漏洞攻防	Kuny @zju.edu.cn
19	李松	百人计划 研究员	移动安全、程序分析、漏洞挖掘、 系统安全	Songl @zju.edu.cn

20	张聪	百人计划 研究员	理论密码学和应用密码学（具体包括安全计算模型分析、保序加密算法以及不可微分安全框架等）	Congresearch @zju.edu.cn
21	罗梦	百人计划 研究员	Web安全、物联网安全、网络犯罪检测、漏洞挖掘、数据驱动安全	meng.luo @zju.edu.cn
22	李晓白	百人计划 研究员	机器视觉、机器学习、 生物识别身份认证、情感计算	Lixiaobai @gmail.com
23	卜凯	副教授	无线网络，网络安全	Kaibu @zju.edu.cn
24	吴磊	副教授	区块链安全、系统安全	lei_wu @zju.edu.cn
25	常瑞	副教授	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	crix1021 @zju.edu.cn
26	卢立	特聘 研究员	智能物联网安全、语音对抗攻防、 语音合成与检测、移动感知、 普适计算	li.lu @zju.edu.cn
27	姚培森	特聘 研究员	编程语言(程序分析与验证、程序合成)、计算机理论(定理证明)、 软件安全(模糊测试)	Pyaoaa @zju.edu.cn
28	张明雪	特聘 研究员	软件安全、Web安全	mxzhang97 @zju.edu.cn
29	刘振广	特聘 研究员	计算机视觉、区块链、人工智能	Zhenguangliu @zju.edu.cn