智能移动身份认证专题前言

身份认证是保障信息系统安全的第一道防线，在大多数系统中甚至是最主要的防线。自20世纪70年代以来，口令一直是最主要的身份认证方法，但始终面临着“可记忆 vs. 抗猜测”这一难以调和的矛盾。自2000年以来，大量替代口令的新型认证技术不断被提出(如图形口令、生物特征认证、隐式行为认证、多因素认证等)，但它们在安全性、可用性或可部署性方面都存在固有缺陷。近年来，无线通信技术(如LTE，LTE-A，WiMAX，5G，蓝牙，WiFi，ZigBee，Z-Wave，LoRa，NB-IoT)的快速发展，一方面促进了智能移动设备(如智能手机、可穿戴设备、智能汽车)的迅速普及，极大地丰富和改善了人们的生产生活方式；另一方面，如何确保移动环境下通信的安全性和敏感数据的隐私性，对实体(包括设备和用户)进行可靠的身份认证，在防止非法实体未授权访问的同时，不降低甚至提升用户体验，成为了必须解决的关键问题。

相较于传统计算环境下的身份认证，智能移动计算设备环境下的身份认证面临3个方面的挑战：一是智能移动设备的计算资源、存储资源和能源通常有限，不适合采用计算复杂度较高的密码算法和原语，这意味着一大批应用于传统计算设备(如个人电脑和笔记本)的现有身份认证方案不适合轻量的移动环境；二是智能移动设备通常具有显示屏幕小、输入键盘小、键位少的特点，现有传统计算设备下的身份认证方案往往对用户不够友好；三是智能移动设备通常需要处理非常敏感的应用和数据(如位置、健康信息、行为爱好等)，基于智能移动设备的认证方案对隐私保护的需求比传统认证方案更高。总之，在进入智能移动时代之际，重新思考面向智能移动设备的身份认证方法十分必要，研究既轻量强健又简单易用的新型身份认证方法迫在眉睫。

《计算机科学》“智能移动身份认证”专栏收录了近期智能移动身份认证研究中的创新性和基础性成果，旨在为国内身份认证领域的研究拓展视野并提供有益的启发。本专栏邀请了身份认证领域的知名专家参与审稿工作，每篇论文都经过至少2位专家的评审。本专栏包括10篇论文：

《车联网互信认证与安全通信综述》分析了现有车联网互信认证和安全通信存在的安全威胁，探讨了5G技术给车联网安全认证带来的影响。《面向边缘计算环境的密码技术研究综述》以身份认证技术为例，重点分析了应用于边缘计算环境的密码技术，对比了不同密码技术保障边缘计算安全的优劣，为面向边缘计算的身份认证提供了新的思路。《基于上采样单分类的智能手机手势密码隐式身份认证机制》融合使用了时间、二维及三维等多类手机内置传感器从不同维度采集用户的行为特征，提出了基于单分类的认证决策机制。《基于WiFi信号的轻量级步态识别模型LWID》将原始时序数据进行图片化重构，设计了一种仿生的Balloon机制，并联合使用不同尺寸的卷积核，实现了基于多层神经网络的轻量级步态识别模型LWID。《基于FPGA集群的Office口令恢复优化实现》在FPGA上以流水线结构优化了核心Hash算法，以多算子并行设计了FPGA整体架构，实现了Office口令快速恢复系统。《口令Zipf分布对相关安全协议的影响分析》以基于口令的签名协议和基于口令的秘密共享协议为例，说明了“口令服从Zipf分布”这一发现对口令密码协议的基础性影响。《基于攻击算法的海量真实用户口令数据分析》基于概率上下文无关文法和TarGuess-I定向口令猜测模型，利用海量真实的用户数据，发现了用户在选择生成口令时存在易被攻击者发现并利用的脆弱行为，为避免用户设置脆弱口令以及设计口令强度评估方法提供了依据。《车联网环境下基于区块链技术的条件隐私消息认证方案》针对目前车联网环境中基于区块链技术的消息认证方案还存在不可链接性的问题，基于物理不可克隆函数和区块链技术设计了一个适用于车联网环境的具有条件隐私的轻量级消息认证方案。《云环境下基于代理盲签名的高效异构跨域认证方案》针对现有不同体系公钥基础设施和无证书公钥密码体系的跨域身份认证方案不能满足身份盲化以及高效的异构跨域认证问题，提出了代理盲签名的高效异构跨域认证方案。《多重PKG环境中高效的身份基认证密钥协商协议》基于椭圆曲线密码体制提出了一种多重PKG环境中的身份基认证密钥协商协议，该协议中多个PKG之间不是相互独立的，而是具有层级隶属关系，更贴近实际应用。

南　开　大　学　汪　定
福建师范大学　黄欣沂
西安交通大学　沈　超
北京航空航天大学　李舟军

专栏特邀编审

汪　定　南开大学教授，博士生导师，百名青年学科带头人，天津市网络与数据安全技术重点实验室副主任，研究方向为身份认证。以第一作者（或通信作者）在 ACM CCS，USENIX Security，NDSS 和 IEEE TDSC，IEEE TIFS 等刊物发表论文 60 余篇，被引用 2700 余次，H-index 为 26。主持国家自然科学基金、装备预研等项目 8 项。担任 CCF《技术动态》编委，CCF 推荐期刊 WCMC，IJISP，《计算机科学》等国内外期刊的编委，SPNCE 2020 和 SocialSec 2020 的 PC Chair，ACSAC，ASIACCS，ISC，ACISP 等著名会议的 PC member。研究成果获教育部自然科学奖一等奖（排名第 2）、天津市科技进步二等奖（排名第 4）、CCF 优博、ACM 中国优博。

黄欣沂　福建师范大学数学与信息学院教授、博士生导师、副院长。长期从事数字签名、身份认证等方面的研究，研究成果获教育部自然科学奖一等奖（第 3 完成人）。担任中国密码学会理事、《密码学报》编委、《中国科学：信息科学》青年编委、AsiaCCS2016 等学术会议主席；入选教育部青年长江学者和福建省“百人计划”，获得国家自然科学基金优秀青年科学基金项目资助。

沈　超　西安交通大学自动化系教授，网络空间安全学院副院长，CCF 大数据专委会委员，国家优秀青年科学基金获得者，阿里巴巴达摩院青橙奖获得者，教育部霍英东青年教师奖一等奖获得者。目前主要从事数据驱动的网络与系统安全、可信人工智能、电力系统综合安全的研究。近年来主持了国家自然科学基金、重点研发计划课题、预研重点基金等部委与企业项目 30 余项。共发表论文 70 余篇，包括 USENIX Security，ACM CCS，ASE，IEEE TDSC，IEEE TIFS 等期刊和会议；获得教育部自然科学二等奖 1 项和国内外学术会议最佳/优秀论文的奖励 7 次；主持和参与研制了多个重要系统并应用于国家大型企事业单位。担任 IEEE Transactions on Dependable Secure Computing 等多个国际期刊的副编辑或编委。

李舟军　北京航空航天大学计算机学院教授，博士生导师，信息安全系主任，智能信息处理研究所副所长。现为国务院学位委员会网络空间安全学科评议组成员，中国网络空间安全协会常务理事，中国网络空间安全协会竞评演练工作委员会副主任委员，中国人工智能学会语言智能专委会副主任委员，ACM，IEEE，AAAI 会员。长期从事网络与信息安全、高可信软件、智能信息处理等领域的研究工作。先后获国内计算机软件界具有重要影响的“中创软件人才奖”、军队院校育才银奖、全国优秀博士学位论文提名、ECIR2010 最佳论文奖、吴文俊人工智能科学技术奖科技进步一等奖。