三、项目简介

近年来，随着 5G 移动互联网的飞速发展和移动智能终端用户（以下称用户）规模的持续扩大，通过对用户敏感数据进行收集、分析，从而推断出用户的潜在兴趣偏好，关注热点、消费水平等，实现主动而有针对性的个性化推荐服务、进一步挖掘数据的潜在价值，一直是移动应用服务提供商的研究热点。**但是随着用户体验服务的不断深入，特别是在移动社交、移动医疗、电子商务、智慧交通等关系到国计民生的重要领域，越来越多的用户开始担心自身的隐私泄露问题。**这主要包括：位置隐私泄露，身份隐私泄露，数据隐私泄露等。

而与此同时，传统的密码学理论、隐私保护技术在面向移动智能终端平台存在着对**非结构性数据加密困难、对海量数据加密计算能力不足、以及加密后数据价值转化率低**等方面的严峻挑战。因此，针对这一问题，本项目面向国家信息网络安全产业发展的重大战略需求，经过多年研究和攻关，并通过产学研用相结合，**在针对移动终端信息隐藏、身份认证、密钥保护、跨域计算等方面的隐私保护处理技术上取得了重要突破，形成了特色鲜明的移动智能终端用户敏感数据隐私保护关键技术体系及系统，对保护移动智能终端用户隐私和信息安全起到了关键性作用。**主要发明创新如下：

1）本发明针对移动终端用户在信息共享过程中，个人敏感数据容易泄露的问题，提出了一种新型的矩阵混淆运算和内积安全计算的隐私保护方案，通过大素数信息隐藏和矩阵元素行列转换，从根本上解决了传统方案加密计算量大，数据匹配粒度粗糙的难题。

2）本发明针对移动终端用户加解密转换过程中，数据明文容易失窃的问题，提出了一种随机密文组件隐私保护方案，通过对用户密钥密文进行代理重加密，实现了对真实明文对应加密文件的信息隐藏和安全共享，从根本上解决了密文转换过程中用户的隐私泄露的难题。

3）本发明针对移动通信过程中用户身份容易被篡改的问题，提出了一种用户伪身份匿名的隐私保护方案，通过哈希值封装比对和双重握手认证机制，从根本上解决了恶意攻击者通过身份欺骗、伪造特征等方式对用户隐私进行窃取的难题。

4）本发明针对移动车联网中车辆节点通信内容容易被攻击篡改的问题，提出了一种车辆通信密文防篡改的车联网隐私保护方案，通过设置多层访问策略树加密，从根本上解决了攻击者通过窃听通信信道而造成的隐私泄露难题。

项目获国家自然科学基金重点、面上、青年项目，湖南省自然科学基金面上、青年项目、永州市科技计划项目等 10 余项项目支持，已获得授权发明专利 4 项，在申请软件著作权 4 项，发表高档次**论文 35 篇，其中 SCI JCR 1 区 4 篇，SCI/EI 检索 20 篇，软件学报、计算机研究与发展、电子学报、通信学报等 CCF A 类、B 类学报 7 篇，SCI 论文单篇最高引用 35 次**。被 IEEE 系列顶级刊物 IEEE **Communication Magazine，IEEE Communications Letter, Elsevier 系列顶级刊物 Future Generation Computer Systems** 以及包括加拿大工程院院士 Laurence Y.在内的美国、加拿大、韩国、法国、西班牙等地的多名学者和研发团队正面评价或列为代表研究文献。项目成果成功应用于湖南省信确电子商务有限公司，湖南省派生信息技术有限公司、湖南省好店长打折网络科技有限公司等单位的产品和软件系统中，应用领域涵盖电子商务、医疗、教育、交通、安全等多个领域的 20 余家单位，社会和经济效益显著。