工程成果	基于可信计算的无线局域网安全管理技术及方法
申请人	李凤华
团队成员	马建峰、李兴华、郭渊博、杨力、刘志宏、姜奇、马卓、董学文、高胜
申请人自述	（请简述工程成果的目的和意义，解决了什么问题，有何贡献或影响，在何处应用，应用效果等。总字数不超过 1000 字，可附页） 该项目属于无线网络安全领域。无线局域网已广泛应用于国家重大行业，是国家信息基础设施的重要组成部分，其安全是影响国家战略安全的主要因素。相对于有线网络，无线局域网面临更多的安全威胁。该项目结合国家战略需求，针对利用可信计算技术来解决无线局域网的接入认证和移动管理环节所面临的安全技术难题，提出了对应的解决方案，形成了以下主要创新点，解决了基于可信计算的无线局域网安全管理问题。 （1）提出了用户可控的可信平台模块 TPM 的体系结构，形成了用户对根密钥的生成、管理技术及安全服务提供方法，实现了 TPM 内部信息的安全预置、备份与恢复和迁移，解决了用户对 TPM 安全的可控性问题，提高了 TPM 的易用性，为可信计算引入到无线局域网扫清了技术上的障碍。 （2）发明了多线程加解密方法，实现了多密钥随机交叉加解密操作，解决了无线局域网中大规模、多用户、高并发认证效率问题。 （3）提出了可证明安全的可信网络连接模型，形成了无线局域网可信接入认证技术，克服了可信计算组织 TCG 所提出的 WLAN 可信网络连接架构存在的安全缺陷。 （4）提出了安全高效的移动管理方法，形成了无线局域网快速可信切换技术，解决了无线局域网终端可信切换效率低，易受攻击的问题。 提出的用户可控的可信平台模块 TPM 的体系结构具有安全强度高，使用方便，管理灵活的特点。发明的多线程加解密方法效

	率高，并发处理能力强。所设计的可信接入认证方案达到了可证明安全的强度，具有度量性强，配置策略灵活的特点。可信切换方法的切换时延低于50毫秒,满足移动多媒体业务连续性的要求。 已获授权6项技术发明专利,登记了3项软件著作权;在IEEE Transactions、ACM等期刊和学术会议上发表论文100多篇，其中SCI检索60多篇，累计他引300多次；出版了3本专著。 取得的成果被国家标准《可信计算规范 第5部分 可信网络连接架构》所采用。由沈绪榜院士为组长的鉴定委员会一致认为所研发的技术整体国际先进，极大地促进了可信计算技术及产业的发展。