中国科学院软件研究所

杰出青年人才发展专项计划年度进展报告书

（2010 年度）

姓名	张振峰	课题名称	
资助金额	190	课题起止时间	2009.9-2013.9
资助类别	应用基础研究	所在部门	信息安全国家重点实验室

研究工作主要进展和阶段性成果（含论文、研究生培养等）

本年度根据项目计划顺利地开展了研究工作，所取得的主要进展和阶段性成果如下。

在无证书签名协议的设计与分析方面，提出了门限环签名协议的增强安全模型下，刻画了一种新的、之前没有被涵盖但又实际可行的敌手能力，设计了一个门限环签名协议，并在新的增强安全模型下证明了其安全性；研究分析了一种面向移动 CPS（Cyber-Physical Systems）应用的无证书签名协议，该协议在当前的无证书签名协议中具有最高的效率，并针对该协议提出了三类有效的攻击方法。

在口令认证协议研究方面，深入研究了基于口令、智能卡和生物特征的三因子认证协议的设计理论，以普通的两方口令认证密钥交换协议作为基本组件，给出了三因子认证密钥交换协议的一般性的构造框架；基于 LWE 困难问题，提出了一个基于 LATTICE 的、可证明安全的口令认证密钥交换协议，实现了真正意义上的密钥协商；提出了基于口令认证与 TPM 远程证明的可信信道设计方案。

具有自恢复功能的密钥分配协议主要面向不可靠或松散的网络环境，解决动态的用户群组进行密钥分配的问题，使得群组成员有能力恢复出丢失的群密钥，这一类协议对于无线传感器等网络具有重要的意义。研究了该类协议的设计理论与分析方法，对一类典型协议提出了有效的合谋攻击；同时，发展了抗合谋的具有自恢复功能的密钥分配协议的设计理论，提出了新的设计方法。

在 INFORM SCIENCES（SCI）、INT J COMPUT COMMUN CONTROL（SCI）、WISA 2010、IEEE GLOBECOM 2010、ISDPE 2010、CMC 2010 等国际期刊和国际会议上发表论文 6 篇。

本年度还开展了基于属性的密码协议、基于格的密码协议的研究工作，取得了初步的研究成果，形成相关论文 2 篇。

在项目争取方面，合作申请到发改委信息安全专项项目一项。

本年度培养指导硕士研究生 6 人，已毕业硕士生一人；指导访学博士研究生 2 人。

下一年度工作计划，包括国内外合作与交流计划

下一年度的主要工作计划如下：

提出高效实用的无证书签名协议，开展有关专利/标准的申请与起草工作；研究具有增强属性的群组口令认证密钥交换协议的安全模型和设计方法。

根据本年度在基于属性的密码协议、基于格的密码协议方面的工作基础，结合我们在基于标识密码协议和可证明安全性理论方面的研究积累，开展基于属性的/基于格的加密方案、数字签名协议研究。

国内外合作与交流计划如下：

拟邀请国外学者合作研究二人次。

拟邀请国内学者合作研究二人次。