



软件研究所中长期发展规划

2009 年杰出青年人才发展专项计划入选者

	姓 名	张振峰
	工作部门	信息安全国家重点实验室
	资助类别	应用基础研究
	资助编号	ISCAS2009-JQ01
	资助金额	190 万元
	支持周期	2009. 9-2013. 9
研究方向	密码学与安全协议	
研究内容	<p>本计划主要进行安全协议的基础理论研究。根据可证明安全性的设计理念，研究无证书密码协议、口令认证协议、具有隐私保护属性的认证协议、基于标识密码协议等安全协议的设计新理论和分析新方法，建立和完善其安全模型规划，深化和发展其可证明安全性理论，以基于计算复杂性的公理化研究方法，突破传统的启发式研究方法的局限性，这是安全协议的核心研究内容之一，并成为了国际标准制定的主要依据；结合复杂应用场景下的安全要求，发展安全协议新的分析方法，是安全协议可证明安全性理论研究的基础，也为安全协议的设计理论提供了源源不断的新思想；面向信息安全保障体系建设的需求，开展相关技术的标准化研究，是安全协议理论与技术发展的结晶，也是安全协议基础理论研究的源动力。</p>	
预期成果	<p>推动和促进无证书密码协议的理论成熟化和技术实用化，发展和完善面向应用的口令认证协议的设计新理论和分析新方法，解决基于标识密码协议应用部署中的关键技术难题，发展新型基于标识应用协议的设计理论，开展隐私保护认证技术的前瞻性基础研究和应用性技术探讨，发展适合我国有关密码标准的关键技术，推动国家信息安全技术标准的发展。拟在国内外权威期刊和重要学术会议上发表论文 8-10 篇，提交标准草案 2-3 项，申请发明专利 3-5 项，培养研究生 6-8 人。</p>	