



软件研究所中长期发展规划

2009 年创新基金领域前沿项目专项计划入选者

	姓 名:	吴文玲
	工作部门:	信息安全国家重点实验室
	资助类别:	竞争择优支持
	资助编号:	ISCAS2009-QY06
	资助金额:	32 万元
	支持周期:	2009 年 9 月-2012 年 9 月
研究方向	密码学	
研究内容	<p>分组密码、消息鉴别码和 Hash 函数是密码学的核心要素，是保障信息机密性和完整性的重要技术。本项目的主要研究内容包括：(1) 分组密码的安全性分析；重点开展对 AES、ARIA 和 SMS4 等分组密码标准算法的安全性分析与评估。(2) 分组密码的设计；探索具备可证明安全性、可并行等特性的新型分组密码结构，设计面向 64 位处理器的分组密码算法。(3) 消息鉴别码算法的设计；研究采用分组密码设计 MAC 算法的有效方法，设计具有平行性、可证明安全性、灵活性的 MAC 算法。(4) MAC 算法的攻击及其相关安全模型；研究可证明安全理论中各种安全模型的内在关系，提炼更合理的安全模型，研究 MAC 算法在具体环境中的实际安全性。(5) Hash 函数的安全性分析；探讨分组密码分析方法在 Hash 函数安全性分析中的新运用，SHA-3 部分候选 Hash 函数算法的安全性分析与评估。</p>	
预期成果	<p>本项目研究兼顾理论安全和实际应用，研究分组密码、消息鉴别码和 Hash 函数的设计理论与分析方法。提出对分组密码更有效的安全性分析方法；提炼更合理的安全模型，完善可证明安全理论；分析 SHA-3 候选算法的安全漏洞，探讨分组密码分析方法在 Hash 函数安全性分析中的新运用；研究新型分组密码整体结构，设计面向 64 位处理器的分组密码算法；设计一个具有可证明安全性且灵活的消息鉴别码算法，完成安全性证明、性能分析、软件实现及测试报告。</p>	