



软件研究所中长期发展规划

2009 年科技新星专项计划入选者

	姓 名:	张文涛
	工作部门:	信息安全国家重点实验室
	资助类别:	青年博士创新基金
	资助编号:	ISCAS2009-DR10
	资助金额:	12 万元
	支持周期:	2009 年 9 月-2012 年 9 月
研究方向	信息安全与密码学	
研究内容	<p>分为三个方面：(1) 分组密码安全性分析方法的研究，扩展已有分析方法的有效性，探索新的分析方法；(2) SHA-3 候选算法中基于分组密码的 Hash 函数的研究，探讨分组密码或分组密码模块在 Hash 函数设计中的运用、及其对 Hash 函数安全性的影响，探询分组密码安全性分析方法在 Hash 函数安全性分析中的新运用；(3) 扩散变换的设计，提出新的扩散层设计方案，力求在安全性和实现性能之间达到更好的平衡。</p>	
预期成果	<p>在国内外重要刊物、或高水平的国际学术会议上发表论文至少三篇；完成两个相关的研究报告。</p>	