



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:	王明生
	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-QY04
	资助金额:	36 万元
	支持周期:	2009 年 9 月-2012 年 9 月
研究方向	符号计算技术和密码系统代数攻击研究	
研究内容	<p>(i) 研究多个输出的流密码的代数免疫度新刻画和从不同角度提出的代数免疫度之间的关系问题。对多输出函数, 一般实际上很难计算它的代数免疫度, 因此研究它们具有的性质, 以及从各种不同的角度来理解就变得相当重要。(ii) 研究针对几个特殊流密码的代数攻击方法。针对特殊的有重要意义的流密码系统如 Trivium 等研究快速有效的多项式方程求解算法。研究向量布尔函数中一些著名的公开问题。(iii) 研究带反馈 (或带记忆) 的流密码的代数攻击问题。发展这类系统抵制代数攻击的准则。(iv) 研究构造密码系统概率多变关系的可能性和条件。</p>	
预期成果	<p>(i) 对流密码系统, 解决多输出情况下, 几个代数免疫度定义的相互关系, 及新的刻画问题和快速的代数攻击方法; (ii) 利用计算代数几何中 Groebner 基和 Wu 特征列中关键思想改进和加速 Shamir 的 Cube 攻击算法; (iii) 解决带记忆反馈情形下 (目前使用的大多数流密码系统都是这种情形), 流密码抵制代数攻击的设计准则; (iv) 关于一些向量布尔函数的猜想的严格证明; (v) 发表 10 篇左右体现研究成果的高质量的研究论文; (vi) 培养 2-3 名博士生, 和多名硕士生。</p>	