工程成果	安全芯片密码检测准则编制及密码芯片侧信道分析检测系统平台研制
申请人	周永彬
团队成员	周永彬、高旭、曹雨晨、孟林、冯明亮
申请人自述	（请简述工程成果的目的和意义，解决了什么问题，有何贡献或影响，在何处应用，应用效果等。总字数不超过 1000 字，可附页） 智能卡密码芯片是一类具有安全功能的典型嵌入式计算设备，在电信、金融、医疗卫生等诸多领域应用十分广泛。安全芯片密码检测准则的制定及密码芯片侧信道安全性分析检测系统平台工具的研制是当前国际学术界与工业界共同关注的关键技术问题。制定科学、合理的安全芯片密码检测准则，可为安全芯片密码测评工作提供可靠的参考基准，亦是开展安全芯片密码测评的重要先决条件；研制相关的分析检测系统平台，可为推动安全芯片密码测评实践提供重要的工具支撑。本项目成果获得之前，我国尚无此类密码技术标准，亦无具有完全自主知识产权的同类综合性分析检测平台。 课题组主持编制了《安全芯片检测准则》（GM/T 0008-2012），国家密码管理局已于 2012 年 11 月 22 日将该标准作为中华人民共和国密码行业标准发布。自颁布至今，国家密码管理局商用密码检测中心已经使用该标准完成了十余款国产密码芯片的安全等级测评工作，为推动我国商用密码应用的水平提供了重要的技术参考。2013 年 12 月，该工作获得密码科技进步奖（省部级）三等奖。 课题组自主研制出面向密码芯片侧信道安全性分析综合分析检测平台，能够对符合 ISO 7816 国际标准的智能卡密码芯片进行侧信息泄漏（能量消耗）的自动采集和集成化的侧信道安全性分析与评估，为此类安全芯片的密码检测提供多种量化度量指标。目前，该系统平台已成为实验室开展相关科研工作的重要环境与基础工具。2013 年下半年，课题组代表实验室多次向多位国家重要部门领导及中国科学院领导进行面向商用密码芯片样片的分析

	攻击现场演示汇报，屡次获得中央领导和院领导的好评。围绕相关工作，课题组研制出原型设备 1 款、自主研制原型系统 1 套、发表学术论文 3 篇(含 1 篇录用)、申请专利 2 项（其中 1 项已完成授权缴费工作)、登记软件著作权 10 项（已获发软件著作权登记证书)。