北京大学高能效计算与应用中心学术报告

Invited Talk, Center for Energy-Efficient Computing and Applications

密码芯片抗旁路攻击技术及SoC低功耗技术

单伟伟 副教授

东南大学电子学院

2015年10月28日 星期三 10:30am

理科五号楼410会议室

摘要： 本次报告主要介绍我们研究的两个方向：密码芯片抗旁路攻击技术及SoC低功耗技术。

密码芯片在信息安全领域发挥着重要问题，但其本身也面临安全风险，近年来旁路攻击（Side-channel Attack, SCA）对密码芯片的安全性提出了挑战，它通过获取密钥设备在加解密操作时泄露的旁路信息（例如功耗、电磁辐射），用统计处理方法分析出关键的密钥，攻击效率且实施简便，因此安全芯片必须具备抗旁路攻击能力。报告首先介绍旁路攻击的原理、常用方法，接着介绍我们组的研究成果——利用可重构技术实现的支持多种算法的抗攻击密码协处理器电路设计。

然后，针对移动智能终端SoC对降低功耗并保持一定的运算性能的迫切需求，介绍了最近几年提出的宽电压范围工作的低功耗技术，以及本组关于近阈值到宽电压自适应电压调节（AVS）技术的研究。

报告人简介： 单伟伟于2003年毕业于天津大学，2003.9清华大学硕博连读，2007.8-2008.8美国马里兰大学 ECE学院联合培养；2009.1月毕业于清华大学微电子所，获博士学位。随后入职东南大学电子科学与工程学院任讲师，2012.4月任副教授，2013年1月硕导、博导。主要研究方向为SoC芯片低功耗技术和信息安全抗攻击技术，主持国家自然科学基金面上项目（近阈值超宽电压电路的PVT偏差弹性设计方法研究）；主持完成国家自然科学基金、江苏省自然科学基金。近年来在IEEE Trans系列期刊、IEICE系列期刊以及DAC等学术期刊和会议上发表第一/通讯作者论文二十余篇，其中SCI收录10篇，授权国家发明专利10余项，授权美国专利2项。获2014年国家科技进步奖二等奖、2011年江苏省科学技术奖一等奖；入选2012年江苏省高校'青蓝工程'优秀青年骨干教师培养对象。