

- >> 首页
- >> 被收录信息
- >> 投稿须知
- >> 模板下载
- >> 信息发布
- >> 常见问题及解答
- >> 合作单位
- >> 产品介绍
- >> 编委会/董事会
- >> 关于我们
- >> 网上订阅
- >> 友情链接

友情链接

- >> 中国期刊网
- >> 万方数据资源库
- >> 台湾中文电子期刊
- >> 四川省计算应用研究中心
- >> 维普资讯网



一种对嵌入式加密芯片的增强DPA攻击方法*

Enhanced DPA technique for embed encrypted CMOS chip

摘要点击: 21 全文下载: 11

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

中文关键词: [差分功耗分析](#) [数据加密标准](#) [离散傅里叶变换](#) [旁路攻击](#)

英文关键词: [differential power analysis\(DPA\)](#) [DES](#) [discrete Fourier transforms](#) [side channel attacks\(SCA\)](#)

基金项目: 国家“863”计划资助项目(2007AA01Z454); 国家自然科学基金资助项目(60571037)

作者

[尹文龙](#), [丁国良](#), [刘昌杰](#), [郭华](#)

单位

[\(军械工程学院 计算机工程系, 石家庄 050003\)](#)

中文摘要:

针对传统DPA攻击方法需要波形数据精确对齐的缺点, 提出了一种基于离散傅里叶变换的增强DPA攻击方法, 并对目前常用的嵌入式芯片以DES加密算法为例进行了DPA攻击实验。实验结果表明采用这种增强的DPA攻击方法能够克服传统DPA攻击方法的缺点。

英文摘要:

This paper presented an enhanced DPA technique to defeat the popular DPA shortcoming, which was that the waveform data must be precise alignment. And made waveform matching based on discrete Fourier transforms. After that performed the standard analysis. The experiment demonstrates the enhanced DPA technique can overcome the shortcoming of popular DPA.

您是第2827010位访问者

主办单位: 四川省计算机研究院 单位地址: 成都市武侯区成科西路3号

服务热线: 028-85249567 传真: 028-85210177 邮编: 610041 Email: arocmag@163.com

蜀ICP备05005319号 本系统由北京勤云科技发展有限公司设计