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

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	单位
尹文龙， 丁国良， 刘昌杰， 郭华	（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 popu-lar DPA.