抗相关性功耗分析的 DES 掩码方案

杨正文，郭　筝

（上海交通大学 电子信息与电气工程学院，上海 200240）

摘　要：以相关性功耗分析为代表的旁路攻击技术对密码设备的安全性造成严重威胁，针对这种情况，本文提出了一种新型的抗相关性功耗攻击的掩码防护方案.该方案是一种流水线式的“非对称掩码技术”，通过流水线式操作，使得加密过程中的每一轮都引入了不同的随机掩码，功耗和操作数之间的相关性被扰乱，从而抵御相关性攻击.我们通过功耗仿真，采集了标准 DES、对称掩码方案及本文提出防护方案对应的功耗仿真曲线，并对其进行相关性功耗攻击.实验结果表明，标准 DES 需要 1 000 条可以攻击成功，对称掩码方案需要 4 000 条功耗曲线可以攻击成功，非对称防护方案则需要　50 000　条曲线才能攻击成功，防护能力提升了 10 倍以上，掩码方案可以有效抵抗相关性功耗分析.

关键词：差分功耗分析；掩码；相关性功耗攻击；流水线

Masking scheme against correlation power analysis on DES

YANG Zheng-wen，GUO Zheng

(College of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China)

Abstract：With the situation that side channel attack poses a serious threat to the security of cryptographic devices, we propose a new scheme of pipelined “asymmetric masking technology” against correlation power analysis and implement it in DES algorithm. Through pipelined operation， different random masks are introduced in each round of the encryption process， so that the correlation between power consumption and processing data is disturbed and we can resist correlation power analysis. Through power simulation, we collected the standard DES, symmetric mask scheme and the power simulation curve corresponding to the proposed protection scheme, and conducted related power consumption attacks. The experimental results show that the standard DES requires 1000 power consumption curves, and the symmetric mask scheme requires 4000 power consumption curves to successfully attack. The protection scheme proposed in this paper requires 50,000 curves to successfully attack, and the protection capability is improved by more than 10 times. We can say that scheme can achieve great protection.

Key words： differential power analysis; masking; correlation power analysis; pipeline

作者简介：

杨正文　男，(1995-)，硕士研究生.研究方向为侧信道攻击、硬件掩码.E-mail:zhengwen_y@163.com.

郭　筝　男，(1980-)，博士，工程师.研究方向为集成电路安全分析和测试.