计算机科学与探索 2009 3 (4): 405-412 ISSN: 1673-9418 CN: 11-5602/TP

学术研究

抗DPA攻击的AES算法研究与实现

郑新建[1+], 张翌维[1], 彭 波[2], 沈绪榜[1]

1. 西安微电子技术研究所，西安 710054
2. 中兴集成电路设计公司，广东 深圳 518057

收稿日期 修回日期 网络版发布日期 2009-7-13 接受日期

摘要 Mask技术破坏了加密过程中的功率消耗与加密的中间变量之间的相关性，提高了加密器件的抗DPA攻击能力。简单地对算法流程添加Mask容易受到高阶DPA攻击的。提出了一种对AES加密过程的各个操作采用多组随机Mask进行屏蔽的方法，并在8 bit的MCU上实现了该抗攻击的AES算法。实验结果表明，添加Mask后的抗DPA攻击AES算法能够有效地抵御DPA和高阶DPA的攻击。

关键词 差分功耗攻击 掩码技术 高级加密标准 S盒

分类号

Research and Implementation of DPA Resistant AES Algorithm

ZHENG Xinjian[1+], ZHANG Yiwei[1], PENG Bo[2], SHEN Xubang[1]

1. Xi’an Microelectronics Technology Institute， Xi’an 710054， China
2. ZTEIC Corporation， Shenzhen， Guangdong 518057， China

Abstract

To improve the DPA （differential power analysis） resistance of a cryptographic device， Mask is used to make the power consumption independent of the intermediate values. High order DPA can attack cryptographic device with simple Masks. A DPA resistant AES （advanced encryption standard） Mask algorithm with several random Masks is proposed. The algorithm is implemented on an 8 bit MCU. The result shows that the DPA resistant AES algorithm can defend DPA and high order DPA analysis efficiently.

Key words differential power analysis （DPA） Mask advanced encryption standard （AES） Sbox

DOI: 10.3778/j.issn.1673-9418.2009.04.007

通讯作者 郑新建 addoil_zh@163.com