计算机工程与应用 2009 45 (16): 106-110 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

采用指令集扩展和随机调度的AES算法实现技术

孙迎红[1], 童元满[2], 王志英[2]
1.湖南涉外经济学院 计算机科学与技术系，长沙 410205
2.国防科学技术大学 计算机学院，长沙 410073

收稿日期 2008-9-23 修回日期 2008-12-22 网络版发布日期 2009-5-27 接受日期

摘要 在随机掩码技术基础上，定义了若干细粒度的随机掩码操作，将AES（Advanced Encryption Standard）算法中各种变换分解为细粒度随机掩码操作的序列，并使得所有的中间结果均被不同的随机量所掩码。为高效实现基于细粒度随机掩码操作分解的AES算法，定义了三种扩展指令，结合指令随机调度方法，给出了AES算法的完整实现流程，并指出这种实现技术可以抗一阶和高阶功耗攻击。实验结果表明，与其他典型防护技术相比，这种实现技术具有安全性、运算性能以及硬件复杂度等方面的综合优势。

关键词 功耗攻击 高级加密标准 随机掩码 指令集扩展

分类号

AES implementation based on instruction extension and randomized scheduling

SUN Ying-hong[1],TONG Yuan-man[2],WANG Zhi-ying[2]

1.Department of Computer Science and Technology，Hunan International Economics University，Changsha 410205，China
2.School of Computer Science，National University of Defense Technology，Changsha 410073，China

Abstract

Based on the random masking scheme，several fine grained masked primitives are defined.Then all the transformations in AES are decomposed to these primitives.And all the intermediate results are masked by different random values.To implement AES based on randomly masked primitives efficiently，three kinds of extended instructions are defined.Combined with random scheduling scheme，the whole execution flow of AES is presented.It is pointed out that this approach can prevent against first order and high order power analysis attack.Experiment results show that it has the advantage of security，performance and hardware complexity in comparison with several other countermeasures.

Key words power analysis attack Advanced Encryption Standard（AES） random mask instruction extension

DOI: 10.3778/j.issn.1002-8331.2009.16.031

扩展功能

本文信息

Supporting info
PDF(895KB)
[HTML全文](0KB)
参考文献

服务与反馈

把本文推荐给朋友
加入我的书架
加入引用管理器
复制索引
Email Alert
文章反馈
浏览反馈信息

相关信息

本刊中 包含“功耗攻击”的相关文章
本文作者相关文章
- 孙迎红
- 童元满
- 王志英

通讯作者 孙迎红 sun_yinghong@yahoo.com.cn