计算机工程与应用 2007 43 (21): 16-17 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

7轮AES-192的飞去来器攻击

张闻宇，黎 琳

山东大学 数学与系统科学学院，济南 250100

收稿日期 修回日期 网络版发布日期 2007-7-9 接受日期

摘要 给出了7轮AES-192的飞去来器攻击。攻击需要239选择明文，2183自适应选择密文，时间复杂度为2183次加密操作，需要237字节的存储空间。这种攻击也可以用于其它SPN结构的没有足够混合的算法。

关键词 高级加密标准 飞去来器 差分

分类号

Boomerang attack on 7 round AES-192

ZHANG Wen-yu，LI Lin

Mathematic and System Science Department of Shandong University，Ji’nan 250100，China

Abstract

This paper shows the boomerang attack on 7 round reduced AES-192.The attack needs 239 chosen plaintexts，2183 adaptively chosen ciphertexts，and the time complexity of this attack is 2183 steps mainly encrypting the texts，237 bytes of memory is needed.This kind of attack can also be applied to other SPN ciphers with incomplete diffusion.

Key words AES boomerang differential

DOI:

通讯作者 张闻宇 E-mail：zhangwy@mail.sdu.edu.cn