山东大学学报(理学版) 2007, 42(4) 6-09 DOI: ISSN: 1671-9352 CN: 37-1389/N

论文

改进的7轮AES-192的碰撞攻击

张闻宇，张海纳

山东大学数学与系统科学学院， 山东济南250100

摘要：

对7轮AES-192的碰撞攻击进行了改进.改进的碰撞攻击是基于Gilbert和Minier的攻击过程并且利用了一些AES-192的密钥特性.改进的攻击可以使用2^{123}字节的存储通过大约2^{120}次加密运算来恢复主密钥，此过程比Gilbert和Minier的攻击过程提高了2^{24}倍而只需增加2^{8}倍的存储量.如果保持存储量不变，改进的攻击过程需要大约2^{127}次加密运算.

关键词： AES 碰撞攻击 区分器

Improved collision attack on 7 round AES-192

ZHANG Wen-yu and ZHANG Hai-na

School of Math. And System Sci., Shandong Univ., Jinan 250100, Shandong, China

Abstract:

An improved collision attack on 7 round AES-192 is given. This attack is based on the result of Gilbert and Minier and the utilization of some properties of AES-192 key schedule. The improved attack can recover the main key by about 2^{120} encryption operations and 2^{123} bytes of memory. Compared with Gilbert-Minier's attack, the time complexity of this attack decreases 2^{24} times with 2^{8} times memory increasing. When the same memory is used as Gilbert-Minier's attack, the time complexity is about 2^{127} encryption operations.

Keywords: AES collision attack distinguisher

收稿日期 2007-03-06 修回日期 1900-01-01 网络版发布日期 2006-10-24

DOI:

基金项目:

通讯作者: 张闻宇

作者简介:

本刊中的类似文章

扩展功能

本文信息

Supporting info

PDF(199KB)

[HTML全文](0KB)

参考文献[PDF]

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

引用本文

Email Alert

文章反馈

浏览反馈信息

本文关键词相关文章

AES

碰撞攻击

区分器

本文作者相关文章

张闻宇

张海纳