电子与信息学报 2010 32 (1): 157-161 ISSN: 1009-5896 CN: 11-4494/TN

论文

3D密码的Square攻击

王美一[1], 唐学海[1], 李 超[1], 屈龙江[1][2]

[1]国防科技大学数学与系统科学系 长沙 410073; [2]东南大学移动通信国家重点实验室 南京 210096

收稿日期 2008-12-31 修回日期 2009-6-29 网络版发布日期 2010-1-12 接受日期

摘要

3D密码是CANS 2008提出的新的分组密码算法，与以往的分组密码算法不同，该密码采用3维结构。该文根据3D密码的结构特性，得到了3D密码的5.25轮和6.25轮新的Square区分器，重新评估了其抗Square攻击的强度。攻击结果表明：新区分器对6轮3D密码攻击的数据复杂度和时间复杂度比已有的结果好，并且还可应用到7轮，8轮和9轮的3D密码攻击中。

关键词 分组密码 3D密码 Square攻击

分类号 TN918.1

Square Attacks on 3D Cipher

Wang Mei-yi[1], Tang Xue-hai[1], Li Chao[1], Qu Long-jiang[1][2]

[1]Department of Mathematics and System Science, National University of Defense Technology, Changsha 410073, China; [2]National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China

Abstract

3D cipher is a new block cipher proposed in CANS 2008. It is different from all known block cipher as it uses the three dimension structure. According to the structure properties of 3D cipher, a new 5.25-round and a new 6.25-round square distinguishers are presented, and the square attacks on reduced- round 3D are improved. Attacking results demonstrate that 6-round attack is better than the known square attacks in data complexity and time complexity. Moreover, these two new distinguishers can be applied to 7/8/9-round 3D cipher.

Key words Block cipher 3D cipher Square attack

DOI: 10.3724/SP.J.1146.2008.01846

通讯作者 王美一 tomorrow_selly@163.com

作者个人主页 王美一[1]; 唐学海[1]; 李 超[1]; 屈龙江[1][2]

扩展功能

本文信息

- Supporting info
- PDF(196KB)
- [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
- 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“分组密码”的 相关文章

本文作者相关文章

- 王美一
- 唐学海
- 李 超
- 屈龙江