电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

电子与信息学报 » 2010, Vol. 32 » Issue (10) :2516-2520 DOI: 10.3724/SP.J.1146.2009.01375

研究简报

3D密码的不可能差分攻击

唐学海[①] 李超[①②] 王美一[①] 屈龙江[①]*

[①](国防科技大学数学与系统科学系 长沙 410073)
[②](信息安全国家重点实验室 北京 100190)

Impossible Differential Attack on 3D Cipher

Tang Xue-hai[①] Li Chao[①②] Wang Mei-yi[①] Qu Long-jiang[①]*

[①](Department of Mathematics and System Science, National University of Defense Technology, Changsha 410073, China)
[②](State Key Laboratory of Information Security, Beijing 100190, China)

摘要 | 参考文献 | 相关文章

Download: PDF (265KB) HTML 1KB Export: BibTeX or EndNote (RIS) Supporting Info

摘要 3D密码是在CANS2008上提出的一个新的分组密码算法，与以往的分组密码算法不同，它采用了3维结构。密码设计者给出了3D密码的一个5轮不可能差分并对6轮3D密码进行了不可能差分攻击。该文通过3D密码的结构特性找到了新的6轮不可能差分。基于新的不可能差分和3D密码的等价结构，可以对7轮和8轮3D密码进行有效的不可能差分攻击。此外，结合其密钥扩展规则，可以将攻击轮数提高至9轮。该文的攻击结果优于密码设计者的结果。

关键词： 分组密码 3D密码 不可能差分攻击

Abstract： 3D cipher is a new block cipher proposed in CANS2008. It is different from all known block cipher as it uses the three dimension structure. The designers give out a 5-round impossible differential and make an impossible differential attack on 6-round 3D cipher. In this paper, some new 6-round impossible differentials are found according to its structure properties. Based on these new impossible differentials and the equivalent structure of 3D cipher, effective impossible differential attacks can be made on 7 and 8-round 3D cipher. Moreover, according to some properties of the key schedule, these attacks can be extended to 9-round 3D cipher. These attack results are better than the designer's.

Keywords： Block cipher 3D cipher Impossible differential attack

Received 2009-10-26;

本文基金:

国家自然科学基金(60803156)和信息安全国家重点实验室开放基金(01-07)资助课题

通讯作者: 唐学海 Email: txh0203@163.com

引用本文:

唐学海, 李超, 王美一, 屈龙江.3D密码的不可能差分攻击[J] 电子与信息学报, 2010,V32(10): 2516-2520

Tang Xue-Hai, Li Chao, Wang Mei-Yi, Qu Long-Jiang.Impossible Differential Attack on 3D Cipher[J] , 2010,V32(10): 2516-2520

链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2009.01375 或 http://jeit.ie.ac.cn/CN/Y2010/V32/I10/2516