计算机工程与应用 2009 45 (4): 89-92 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

MD4杂凑函数的近似碰撞

张 栋[1,2], 李梦东[2], 沈 薇[1,2]
1.西安电子科技大学 通信工程学院，西安 710071
2.北京电子科技学院 信息安全系，北京 100070

收稿日期 2008-7-29 修回日期 2008-10-7 网络版发布日期 2009-1-24 接受日期

摘要 在现代密码学中，Hash函数扮演着重要的角色。而在Hash函数发展过程中，MD4算法又起着基石的作用。通过对MD4算法和王小云逐比特差分分析的介绍，利用相关差分分析的理论知识，对MD4算法产生了一对近似碰撞。找出了该碰撞的差分路径，并确定出满足其差分路径的充分条件。

关键词 Hash函数 MD4算法 差分分析 近似碰撞
分类号

Near-collision of MD4 Hash function

ZHANG Dong[1,2],LI Meng-dong[2],SHEN Wei[1,2]

1.Department of Communication Engineering，Xidian University，Xi’an 710071，China
2.Department of Information Security，Beijing Electronic Science and Technology Institute，Beijing 100070，China

Abstract
Hash functions play an important role in modern cryptography，while MD4 algorithm is the basis of the Hash functions during the development of Hash functions.Using the relevant knowledge of the differential cryptanalysis theories，the MD4 algorithm and X.Y.Wang bit flipping differential cryptanalysis are reviewed in this paper.Finally one near-collisions of MD4 is found.Meanwhile，the differential path of the collisions and sufficient conditions that satisfy the differential path are shown.

Key words Hash function MD4 algorithm differential cryptanalysis near-collision

DOI: 10.3778/j.issn.1002-8331.2009.04.025

通讯作者 张 栋 zhangd@besti.cn