计算机工程与应用 2007 43 (32): 125-127 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

基于四维混沌猫映射分组密码的设计与分析

龙 敏[1], 丘水生[2]

1.长沙理工大学 计算机与通信学院,长沙 410076
2.华南理工大学 电子与信息学院,广州 510640

收稿日期 修回日期 网络版发布日期 2007-10-29 接受日期

摘要 基于四维混沌猫映射提出一种新的128 bit混沌分组密码。128 bit数据重新排列成4×4的十进制矩阵,并对其进行8轮运算。在每一轮运算中,随机选取其中某一行和某一列执行四维猫映射变换,再采用子密钥对其变换结果进行加密。对密码算法进行密文随机性测试,明文与密文的相关性测试,明文的敏感性测试和密钥的敏感性测试。安全性分析表明,该分组密码具有抵抗差分攻击和线性攻击的优良性能,并且具有较大的密钥空间。

关键词 分组密码 混沌加密 混沌映射

分类号

Design and analysis for block cipher based on 4D chaotic cat maps

LONG Min[1],QIU Shui-sheng[2]

1.College of Computer and Communication,Changsha University of Science and Technology,Changsha 410076,China
2.College of Electronic & Engineering,South China University of Technology,Guangzhou 510640,China

Abstract

A novel 128 bit block cipher based on 4D chaotic cat maps is proposed.128 bit data are rearranged to a 4×4 decimal matrix,which is processed by 8 rounds of operations.In each round,one row and one column will be randomly chosen to perform a 4D chaotic cat maps transformation,and then use the sub-key to encrypt it.A series of tests have been performed on the block cipher,such as random test on ciphertext,correlation test between the plaintext and the ciphertext,plaintext sensitivity test and key sensitivity test.Security analysis shows that the cipher has good performance to resist differential attack and linear attack,and it has a large key space.

Key words block cipher chaos encryption chaotic maps

DOI:

通讯作者 龙 敏