电子与信息学报　2006 28 (4): 707-711　ISSN: 1009-5896　CN: 11-4494/TN

论文

一种结合离散混沌映射和Feistel网络的分组加密算法

彭 军[1,2], 廖晓峰[2], 岡本栄司[3], 张 伟[4], 李学明[2]

[1]重庆科技学院电子信息工程学院 重庆 400050;[2]重庆大学计算机科学与工程学院 重庆 400044;[3]日本筑波大学系统与情报工学研究科 日本 305-8573;[4]重庆教育学院计算机与现代教育技术系 重庆 400067

收稿日期 2004-8-23　修回日期 2005-1-4　网络版发布日期 2007-12-5　接受日期

摘要

论文提出了一种新颖的结合一维离散混沌映射与Feistel网络结构的分组密码算法(CFCEA)。分组长度为64bit，密钥长度为128bit，并使用了一个128bit长的辅助密钥。在轮函数中用Logistic混沌映射和3个代数群算子进行混合运算，此外还特别设计了子密钥生成算法。对CFCEA的密码学特性进行了分析，结果表明该算法具有严格的雪崩效应，扩散性能和扰乱性能理想。并且算法在64bit分组长度下差分概率和线性概率的理论上界分别近似为$2^{-52.92}$和$2^{-49.206}$，具备抵抗一定强度的差分和线性密码分析的能力。

关键词　分组密码　Logistic混沌映射　Feistel网络　差分和线性密码分析

分类号　TN918.4

扩展功能

本文信息

- Supporting info
- PDF(327KB)
- [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

· 彭 军
· 廖晓峰
· 岡本栄司
· 张 伟
· 李学明

A Block Encryption Algorithm Combined with the Discrete Chaotic Map and Feistel Network

Peng Jun[1,2], Liao Xiao-Feng[2], Okamoto Eiji[3], Zhang Wei[4], Li Xue-Ming[2]

[1]Department of Electronic Information Engineering, Chongqing University of Science and Technology, Chongqing 400050, China; Department of Computer Science and Engineering, Chongqing University, Chongqing 400044, China; [2]Graduate School of Systems and Information Engineering, University of Tsukuba, Ibaraki 305-8573, Japan; [4]Department of Computer and Modern Education Technology, Chongqing Education College, Chongqing 400067, China

Abstract

In this paper a novel block encryption algorithm, which is called CFCEA, is proposed by combining the one dimensional discrete chaotic map and Feistel network. The algorithm operates on 64bit plaintext blocks, and the master key is 128 bit long, and an auxiliary key with size of 128 bit is exploited. Within the round function, the logistic chaotic map and three algebraic group operations are mixed. Moreover, the subkeys schedule is specially designed for the consideration of the security. The cryptographic properties of the algorithm are analyzed, and the results indicate that this algorithm satisfies the strict avalanche criterion and as a result, the diffusion and confusion properties of the algorithm are very ideal. Furthermore, when the block length is 64bit, the approximately upper bound of differential probability and linear probability of CFCEA is $2^{-52.92}$ and $2^{-49.206}$, respectively. This shows that the algorithm can resist differential and linear cryptanalysis with some strength.

Key words　Block cipher　Logistic chaotic map　Feistel network　Differential and linear cryptanalysis

DOI:

通讯作者

作者个人主页　彭 军[1,2]; 廖晓峰[2]; 岡本栄司[3]; 张 伟[4]; 李学明[2]