计算机工程 2012, 38(3) 22-24,33 DOI: 10.3969/j.issn.1000-3428.2012.03.008 ISSN: 1000-3428 CN: 31-1289/TP

博士论文

基于Feistel网络的十进制加密算法

崔 杰，仲 红

(安徽大学计算机科学与技术学院，合肥 230039)

摘要： 提出一种基于Feistel网络的十进制加密算法。针对十进制数运算的特点，在加密算法中定义4种新的运算，在密钥扩展算法和解密算法中定义2种新的运算，并设计十进制S盒。将该算法应用于短分组加密仿真系统中，实验结果表明，该算法具有较好的密码学特性，加解密的各项扩散率指标均较优，经6轮加密后，该算法达到完全扩散。

关键词： 十进制 Feistel网络 分组密码 扩散率 S盒 密码学

Decimal System Encryption Algorithm Based on Feistel Network

CUI Jie, ZHONG Hong

(School of Computer Science and Technology, Anhui University, Hefei 230039, China)

Abstract: This paper proposes a decimal system encryption algorithm based on Feistel network. Aiming at the characteristics of decimal system operations, four operations are defined in encryption algorithm, two operations are defined in key expansion algorithm and decryption algorithm, and the new decimal system substitution table is designed. The new encryption algorithm is applied to the short-block encryption simulation system, simulation results show that the proposed algorithm has excellent cryptographic properties, all diffusion rate targets reach desired impact, and the diffusion rate of key to ciphertext after 6-round encryption reaches full diffusion. The encryption algorithm can be applied to all areas of decimal system encryption.

Keywords: decimal system Feistel network block cipher diffusion rate S-box cryptology

收稿日期 2011-07-26 **修回日期** **网络版发布日期** 2012-02-05

DOI: 10.3969/j.issn.1000-3428.2012.03.008

基金项目:

国家自然科学基金资助项目(61173187, 61173188)；安徽省高等学校优秀青年人才基金资助项目(2010SQRL017)；安徽大学“211工程”基金资助项目

通讯作者:

作者简介: 崔 杰(1980－)，男，讲师、博士研究生，主研方向：网络与信息安全；仲 红，教授

通讯作者E-mail: cuijie@mail.ustc.edu.cn

参考文献：

[1] Kanda M. Practical Security Evaluation Against Differential and Linear Attacks for Feistel Ciphers with SPN Round Function[C]// Proc. of Selected Areas in Cryptography. New York, USA: Springer-Verlag, 2000: 158-179.
[2] 师国栋, 康 绯, 顾海文. 分组密码统一描述模型研究[J]. 计算机工程, 2010, 36(1): 154-156.
[3] 刘连浩, 罗 安, 陈松乔. 基于十进制的加密技术研究[J]. 小型微型计算机系统, 2006, 27(7): 1229-1231.
[4] Knudsen L R. Practically Secure Feistel Ciphers[C]//Proc. of Lecture Notes in Computer Science.

扩展功能
本文信息
Supporting info
PDF(243KB)
[HTML] 下载
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
引用本文
Email Alert
文章反馈
浏览反馈信息
本文关键词相关文章
十进制
Feistel网络
分组密码
扩散率
S盒
密码学
本文作者相关文章
崔杰
仲红
PubMed
Article by Cui, J.
Article by Zhong, G.

New York, USA: Springer- Verlag, 1994: 211-221.
[5] 高靖哲, 赵新杰, 矫文成, 等. 针对CLEFIA的多字节差分故障分析[J]. 计算机工程, 2010, 36(19): 156-158.
[6] 吴文玲, 贺也平. 一类广义Feistel密码的安全性评估[J]. 电子与信息学报, 2002, 24(9): 1177-1184.
[7] 李 超, 屈龙江, 李 强. 对DES的一种新的线性分析[J]. 国防科学技术大学学报, 2004, 26(3): 43-47.
[8] 张 鹏, 孙 兵, 李 超. 对特殊类型Feistel密码的Square攻击[J]. 国防科学技术大学学报, 2010, 32(4): 137-141.
[9] 刘连浩, 崔 杰, 刘上力. 一种AES S盒改进方案的设计[J].中南大学学报: 自然科学版, 2007, 38(2): 339-344.
[10] Daemen J, Rijmen V. AES Proposal: Rijndael, Version2[EB/OL]. (1999-07-10). http://www.esat.kuleuvan.ac.be/~rijndael.

本刊中的类似文章

1. 郑秀林, 连至助, 鲁艳蓉, 袁征.CLEFIA-128算法的不可能差分密码分析[J]. 计算机工程, 2012,38(3): 141-144
2. 贾艳艳, 董丽华, 胡予濮.多个二元序列的二次复杂度研究[J]. 计算机工程, 2011,37(4): 31-33
3. 申艳光, 刘永红, 江涛.n元Bent函数的级联构造[J]. 计算机工程, 2011,37(4): 125-127
4. 毕晓君, 盛磊, 陈剑.基于改进粒子群优化算法的S盒优化设计[J]. 计算机工程, 2011,37(23): 149-151
5. 张兴爱, 张应辉, 史来婧.广播多重签名方案中阈下信道的封闭协议[J]. 计算机工程, 2011,37(22): 102-104
6. 顾洋, 刘嘉勇.一种改进的多秘密共享方案[J]. 计算机工程, 2011,37(21): 111-113
7. 王琴.一种基于身份的代理签密体制[J]. 计算机工程, 2011,37(19): 120-121,125
8. 韩睿, 赵耿, 刘山鸣, 赵菲.基于混沌映射的分组密码算法[J]. 计算机工程, 2011,37(16): 120-122
9. 张聪娥, 刘军霞.Akelarre分组密码算法的奇偶校验分析[J]. 计算机工程, 2011,37(16): 111-113
10. 曾永红;叶旭鸣.抗差分功耗分析攻击的AES S盒电路设计[J]. 计算机工程, 2010,36(9): 20-22

文章评论

反馈人		邮箱地址	
反馈标题		验证码	4413

Copyright by 计算机工程