电子与信息学报 2004 26 (6): 912-916 ISSN: 1009-5896 CN: 11-4494/TN

论文

Twofish算法中密钥相关S-盒的差分性质分析及其改进

周旋①,李超①②

①国防科技大学理学院数学与系统科学系,长沙,410073;②中国科学院软件研究所计算机科学重点实验室,北京,100080

收稿日期 2003-2-27 修回日期 2003-8-8 网络版发布日期 2008-5-13 接受日期

摘要
该文从理论上证明了Twofish算法中,密钥越长,密钥相关S-盒的差分概率就越小,提出了一种新的与密钥作用的方式来产生密钥相关S-盒的方法,理论与测试结果表明新的S-盒的"异或"差分概率和"模加"差分概率比原算法的差分概率要小.

关键词 Twofish 差分分析 S-盒

分类号 TN918 O441

扩展功能
本文信息
Supporting info
PDF(1144KB)
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
相关信息
本刊中 包含“Twofish”的 相关文章
本文作者相关文章
· 周旋
· 李超

Differential Analysis and Modification of the Key-Dependent S-Boxes of Twofish

Zhou Xuan①, Li Chao①②

①Dept. of Math. and System Sci., Nat. Univ. of Defense Tech., Changsha 410073, China;②Key Lab. of Computer Sci., Inst. of Software, OAS, Beijing 100080, China

Abstract
This paper proves that the longer the key of Twofish is,the smaller the differ-ential probabilities of the key-dependent S-boxes are. A new method is proposed to produce the key-dependent S-boxes. Theory and simulation results show that the XOR differential probability and modular addition differential probability of the modified S-boxes are smaller than those of the original S-boxes.

Key words

Twofish Differential analysis S-boxes

DOI:

通讯作者
作者个人主页