计算机工程与应用　2007 43 (25): 143-146　ISSN: 1002-8331　CN: 11-2127/TP

网络、通信与安全

AES S盒的分析及改进方案设计

崔 杰[1,2]，刘连浩[2]，刘上力[2]，马虹博[2]

1.安徽大学 计算机科学与技术学院，合肥 230039
2.中南大学 信息科学与工程学院，长沙 410083

收稿日期　修回日期　网络版发布日期 2007-8-20　接受日期

摘要　研究了AES S盒的构造原理和主要代数性质，指出了AES S盒的仿射变换对周期为4，迭代输出周期不大于88，严格雪崩准则距离为432，代数表达式只有9项等。基于这些不足提出了构造S盒的改进方案。改进S盒的仿射变换对周期为16，迭代输出周期为256，而且S盒和逆S盒代数表达式项数均达到254项。将改进S盒与AES的S盒在平衡性、严格雪崩准则、非线性度、抗代数攻击阻力等10种代数性质上进行比较，实验结果表明改进S盒具有更好的性质。

关键词　S盒　多输出布尔置换　仿射变换　代数表达式

分类号

Analysis of AES S-box and design of its improved method

CUI Jie[1,2]，LIU Lian-hao[2]，LIU Shang-li[2]，MA Hong-bo[2]

1.School of Computer Science and Technology，Anhui University，Hefei 230039，China
2.School of Information Science and Engineering，Central South University，Changsha 410083，China

Abstract

This paper studies the construction principle and main algebraic properties of AES S-box，points out the S-box has these characteristics that periods of affine transformed pair is 4，periods of iterative-output is less than 88，strict avalanche criterion distance is 432，the algebraic expression has only 9 items and so on.Based on that，an improved S-box has been constructed.Periods of affine transformed pair is 16 and periods of iterative-output is 256 and both the algebraic expression of S-box and InvS-box have 254 items in the improved S-box.The improved S-box has been compared with AES S-box in 10 algebraic properties，such as balanceness，strict avalanche criterion，non-linear degree，resistance against the XSL attack etc.The experimental results suggest that the improved S-box has better characteristics.

Key words　S-box　multi-output boolean permutation　affine transformation　algebraic expression

DOI:

扩展功能

本文信息

- Supporting info
- PDF(1157KB)
- [HTML全文](0KB)
- 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“S盒”的 相关文章
- 本文作者相关文章
  - 崔 杰
  - 刘连浩
  - 刘上力
  - 马虹博

通讯作者　崔 杰 E-mail：cvjxabcd@126.com