信号处理 2011, 27(9) 1428-1433 DOI: ISSN: 1003-0530 CN: 11-2406/TN

短文与研究通讯

基于AES算法中S盒的分析研究与改进

张丽红,凌朝东

华侨大学信息科学与工程学院

摘要：

由于AES S盒代数式只有9项过于简单且仿射变换对周期和迭代输出周期过短的原因，提出了一种新的构造S盒的解决方法。该方法通过在有限域上利用拉格朗日插值公式完全展开的系数求解方法得出了S盒和逆S盒的代数式系数表。与AES S盒构造原理导出的代数式相比，该方法具有直观且简单通用的特性。MATLAB仿真结果显示，新S盒的构造时间最短。其仿射变换周期和迭代输出周期分别高达16和256。S盒和逆S盒的严格雪崩准则距离分别降为376和304。S盒的代数式项数提高到253项。表明新S盒具有更复杂的代数结构、较好的差分特性以及非线性，同时根据仿射变换次数和S盒的构造时间进一步说明新S盒的设计既简洁又高效。

关键词： 高级加密标准 S盒 MATLAB 拉格朗日插值 仿射变换 代数式

The analysis and improvement of S box based on AES

ZHANG Li-Hong, LING Chao-Dong

College of Information Science & Engineering, Huaqiao University, Quanzhou

Abstract:

For an AES S box, the algebraic expression, which only has 9 items, is too simple, and the period of affine transform pair and iterative output is too short. For these reasons, a new solution to construct a S box is proposed. The algebraic expression coefficients of the S box and Inv S box are obtained using the coefficients of fully expanded Lagrange interpolation formula in finite field. Compared with deriving the algebraic expression from the construction principle of AES S box, this new method is intuitive and simple universal. The MATLAB simulation results show that the new S box has the shortest construction time. The period of affine transform pair and iterative output are up to 16 and 256 respectively. The strict avalanche criterion distance of S box and Inv S box reduce separately to 376 and 304. S box’s algebraic expression items are improved to 253. All of these prove that the new S box has a more complex algebraic structure, better difference characteristics and nonlinearity. At the same time, the affine transform times and the construction time of S box further explain the conciseness and high efficiency of the new S box design.

Keywords: Advanced Encryption Standard S box MATLAB Lagrange interpolation affine transform algebraic expression

收稿日期 2011-05-21 修回日期 2011-09-01 网络版发布日期 2011-09-25

DOI:

基金项目:

国家自然科学基金项目(60772164);厦门市科技计划项目（3502Z20080010）

通讯作者:

作者简介:

作者Email: zlh840@qq.com

参考文献：

本刊中的类似文章

1．邹刚, 姚伟, 孙即祥, 敖永红.一种基于共轭梯度交替迭代的协同不变性算法[J]. 信号处理, 2010,26(7): 1060-1065

2． 韩洲, 李元祥, 周则明, 沈霁.基于改进先验形状CV模型的目标分割[J]. 信号处理, 2011,27(9): 1395-1401

文章评论

反馈人		邮箱地址	
反馈标题		验证码	6596