Journal of Systems Science and Complexity 1997 10 (2): 120-128 ISSN: 1000-0577 CN: 11-2019/O1

论文

CONSTRUCTION OF SAC PERMUTATIONS

GONG Guang(1),DAI Zongduo(2)

(1)Department of Applied Mathematics, University of Electronic Science and Technology of China, Chengdu 610054,China;(2)State Key Laborotory of Infrmation Security, the Graduate School,Academia Sinica, Beijing 100039, China

收稿日期 修回日期 网络版发布日期 接受日期

摘要 Nonlinear permutations of GF(2^n) with strong cryptographic properties have important applications in cryptology such as DES-like block ciphers, hush functions and stream ciphers. In paPer [1], we proved that the exponential function can provide a class of permutations satisfying the Strict Avalanche Criterion (SAC permutations) with algebraic nonlinear degree 2. In this paper, we further construct three classes of SAC permutations that are derived from the Dickson polynomials, GMW functions and the exponential functions with maximal algebraic nonlinear degree, respectively.

关键词 The Strict Avalanche Criterion, Dickson

分类号

扩展功能

本文信息

Supporting info

PDF(0KB)

[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“The Strict Avalanche Criterion, Dickson”的 相关文章

本文作者相关文章

- GONG Guang
- DAI Zongduo

CONSTRUCTION OF SAC PERMUTATIONS

GONG Guang(1),DAI Zongduo(2)

(1)Department of Applied Mathematics, University of Electronic Science and Technology of China, Chengdu 610054,China;(2)State Key Laborotory of Infrmation Security, the Graduate School,Academia Sinica, Beijing 100039, China

Abstract Nonlinear permutations of GF(2^n) with strong cryptographic properties have important applications in cryptology such as DES-like block ciphers, hush functions and stream ciphers. In paPer [1], we proved that the exponential function can provide a class of permutations satisfying the Strict Avalanche Criterion (SAC permutations) with algebraic nonlinear degree 2. In this paper, we further construct three classes of SAC permutations that are derived from the Dickson polynomials, GMW functions and the exponential functions with maximal algebraic nonlinear degree, respectively.

Key words The Strict Avalanche Criterion Dickson polynomial GMW function exponential function.

DOI:

通讯作者