

论文

次数最大的平衡相关免疫函数的构造

潘永涛, 戚文峰

郑州信息工程大学信息工程学院应用数学系 郑州 450002

收稿日期 2005-5-16 修回日期 2005-11-24 网络版发布日期 2007-11-12 接受日期

摘要

Maitra和Sarkar于1999年提出了一种递归构造 n 元平衡相关免疫布尔函数的方法。该文给出了一种新的递归构造方法,构造出非线性度很高的 n 元 m 阶 $n-m-1$ 次的平衡相关免疫函数。与原构造方法相比,该文构造方法得到的函数性质相同,数量更大。

关键词 [布尔函数](#) [代数次数](#) [相关免疫](#) [非线性度](#) [平衡性](#)

分类号 [TN918](#)

Construction of Balanced Correlation-Immune Functions with Highest Degree

Pan Yong-tao, Qi Wen-feng

Department of Applied Mathematics, Information Engineering University, Zhengzhou 450002, China

Abstract

Maitra and Sarkar provided a recursive construction method of balanced correlation-immune Boolean functions on n variables in 1999. In this paper, a new method is provided to construct balanced m -th order correlation-immune Boolean functions on n variables with high nonlinearity and algebraic degree $n-m-1$. Compared with the original one, this method can get more functions with the same characteristics.

Key words [Boolean function](#) [Algebraic degree](#) [Correlation-immunity](#) [Nonlinearity](#) [Balancedness](#)

DOI :

通讯作者

作者个人主页 潘永涛; 戚文峰

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF \(257KB\)](#)

▶ [\[HTML全文\]\(0KB\)](#)

▶ [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](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中 包含“布尔函数”的 相关文章](#)

▶ 本文作者相关文章

· [潘永涛](#)

· [戚文峰](#)