计算机工程与应用 2007 43 (8期): 59-61 ISSN: 1002-8331 CN: 11-2127/TP

学术探讨

布尔函数的代数免疫性研究

罗卫华 李超 周海银

国防科技大学理学院数学与系统科学系 南京邮电学院计算机科学与技术系

收稿日期 2006-4-10 修回日期 网络版发布日期 2007-3-6 接受日期

摘要 代数免疫性是评判布尔函数安全性的一个重要指标，本文研究了布尔函数的零化函数的性质，得到了代数免疫度的一些结果，同时研究了代数免疫度与布尔函数的重量的关系。

关键词 布尔函数 代数攻击 代数免疫 零化函数 汉明重量

分类号

The Algebraic Immunity Study Of Boolean Functions

Chao Li

Abstract

The algebraic immunity is an important criteria for deciding the security of Boolean functions. In this paper we study the properties of annihilators of Boolean functions, and get some results about the algebraic immunity. Meanwhile we also study the relations between the algebraic immunity and the Hamming weight of Boolean functions.

Key words Boolean Functions Algebraic Attacks Algebraic Immunity Annihilators Hamming weight

DOI:

通讯作者 罗卫华 lwhstar@yahoo.com.cn

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“布尔函数”的相关文章

本文作者相关文章

· 罗卫华 李超 周海银