

<<频谱理论及其在密码学中的应用>>

图书基本信息

书名：<<频谱理论及其在密码学中的应用>>

13位ISBN编号：9787030086594

10位ISBN编号：7030086597

出版时间：2000-10-01

出版时间：科学出版社

作者：冯登国

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<频谱理论及其在密码学中的应用>>

内容概要

本书系统而全面地介绍了频谱理论及其在密码学中的应用，内容主要包括：（1）利用频谱技术对布尔函数的各种非线性准则之间的关系及其特征进行了深入的刻画，并在此基础上构造了一批满足某些密码学特性的布尔函数；讨论了非线性组合函数的最大相关分析问题，给出了一个非常有效的逼近算法。

（2）介绍了广义一阶Walsh谱的概念，利用这种谱对多输出函数的密码学特性进行了深入的刻画；构造了一批具有差分均匀性较小、非线性次数

<<频谱理论及其在密码学中的应用>>

书籍目录

前言

第1章绪论

1.1密码学简介

1.2频谱理论在密码学中的应用概况

1.3本书的安排

研究问题

第2章一阶Walsh谱及其应用

2.1布尔函数的表示

2.2一阶Walsh谱的定义及其重要性质

2.3布尔函数的线性逼近

2.4Bent函数的结构和构造

2.5部分Bent函数的结构

2.6布尔函数的线性结构和退化性

2.7布尔函数的雪崩效应和扩散特性

2.8相关免疫布尔

版权说明

本站所提供下载的PDF图书仅提供预览和简介, 请支持正版图书。

更多资源请访问:<http://www.tushu007.com>