<<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

<<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

版权说明