<<有限域小波及其在密码学和译码中的应>>

图书基本信息

书名：<<有限域小波及其在密码学和译码中的应用>>

13位ISBN编号：9787030343833

10位ISBN编号：7030343832

出版时间：2012-6

出版时间：科学出版社

作者：（美）法拉马兹　等编著

页数：284

字数：426000

内容概要

《有限域小波及其在密码学和译码中的应用》探讨了有限域小波与滤波器组理论，开创了“有限域小波变换理论”，此理论提出了一个定义在有限域上的一般的小波分解序列。
《有限域小波及其在密码学和译码中的应用》还介绍了此理论在纠错代码和数据安全性上的首次应用。

《有限域小波及其在密码学和译码中的应用》可作为应用数学、密码学、差错控制编码领域研究者的参考书，对于从事密码项目开发的实际工作者也有很大的价值。

作者简介

无

书籍目录

章节摘录

From a practical point of view,a complete classification of orthogonal filter banks is of greatinterest.The underlying reason is based on the observation that some filter banks are more usefulthan others in specific applications.We are interested in finding a minimal set of parameterized PU building blocks such that their multiplication generates all PU matrices.Such factorization enables the designer of the filter-bank system to easily optimize the free parameters of each buildingblock to enforce certain behavior(e.g.,maximizing the minimum distance in error-correcting codes).Furthermore,the parameters of each individual PU building block can be changed independentlywhile the PR property is preserved.Constant PU matrices are unitary matrices that can be realized using planar rotations over thereal field[199].A factorization of univariate PU matrices over the complex field has been performed in[199]by providing a degree-1 building block.It was conjectured that there also exists asimilar factorization for multivariate PU matrices.Nevertheless,Venkataraman and Levy disprovedthis conjecture by a counter example[202].A complete factorization of bivariate PU matrices over the complex field,using a two-level factorization,is provided in[59].It is shown that contrary to the general expectation,all bivariate PU matrices over the complex field can be generated by themultiplication of IIR PU building blocks in each of the two variables in arbitrary orders.A similarlevel-by-level factorization approach was taken in[58]for 2 x 2 PU matrices over fields of characteristic 2.Although a first-level factorization is always possible,a complete factorization seems tobe difficult to find.The factorization of PU matrices over finite fields is not a trivial extension of the complex-fieldtechniques.In[166],authors show that the factorization of PU matrices over GF(p),for a primep,using the previously introduced elementary PU degree-1 and degree-2 building blocks is notcomplete.In other words,there are orthogonal filter banks that cannot be represented by cascadingthese building blocks.The main results of this chapter are summarized below：1.In Sec.4.2,we introduce the elementary unitary building block over IF2,that acts like theHouseholder matrix.Any unitary matrix over IF2r can be represented as a product of theunitary building block and permutations of the identity matrix.

版权说明