

<<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

出版单位：科学出版社

作者：（美）法拉马兹 等编著

页数：284

字数：426000

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>

<<有限域小波及其在密码学和译码中的应>>

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

- Preface
- Figures
- Tables
- Algorithms
- Acronyms
- 1 Introduction and Some Algebra Preliminaries
 - 1.1 Notations
 - 1.1.1 Set Notation
 - 1.1.2 Matrix Notation
 - 1.1.3 Asymptotic Notation
 - 1.1.4 General Notation
 - 1.2 Abstract Algebraic Background
 - 1.2.1 Group
 - 1.2.2 Ring
 - 1.2.3 Field
 - 1.2.4 Irreducible and Primitive Polynomials
 - 1.2.5 Construction of Extension Fields
 - 1.2.6 Module
 - 1.2.7 Algebra
 - 1.3 Linear Algebra Background
 - 1.3.1 Involution
 - 1.3.2 Sesquilinear Form
 - 1.3.3 Unitary Matrix
 - 1.3.4 Paraunitary Matrix
- I Finite-Field Wavelets
- 2 Background Review and Motivation
 - 2.1 Wavelets for Discrete-Time Signals
 - 2.2 Cyclic Wavelet Transforms
 - 2.3 Review of Transforms over Finite Fields
 - 2.3.1 Discrete Fourier Transform over Finite Fields
 - 2.3.2 Base-Field Transforms over Finite Fields
 - 2.3.3 Related Work on Finite-Field Wavelets
- 3 Finite-Field Wavelet Basis Functions
 - 3.1 Finite-Field Discrete-Time Basis
 - 3.1.1 Non-Degenerate Bilinear Form
 - 3.1.2 Orthonormal Wavelet Basis over Finite Fields
 - 3.1.3 Completeness of the Orthonormal Set
 - 3.2 Construction of Mother Wavelet and Scaling Function
 - 3.3 Summary
- 4 Theory of Paraunitary Filter Banks over Fields of Characteristic 2
 - 4.1 Background Review
 - 4.1.1 Degree-1 Paraunitary Building Block over $GF(2)$
 - 4.1.2 Degree-2 Paraunitary Building Blocks over $GF(2)$
 - 4.1.3 Lapped Orthogonal Transforms over $GF(2)$

- 4.2 Unitary Matrices over $GF(2r)$
- 4.3 Paraunitary Matrices over Fields of Characteristic 2
 - 4.3.1 Properties of 2×2 Paraunitary Matrices over $GF(2r)$
- 4.4 Factorization of Paraunitary Matrices over $GF(2r)$
 - 4.4.1 Degree-1 Paraunitary Building Block over $GF(2r)$
 - 4.4.2 Degree-2 Paraunitary Building Block over $GF(2r)$
 - 4.4.3 Degree- $2r$ Paraunitary Building Block over $GF(2r)$
 - 4.4.4 Factorization of 2×2 Paraunitary Matrices over $GF(2r)$
 - 4.4.5 Degree- Mr Paraunitary Building Block over $GF(2r)$
 - 4.4.6 Factorization of $M \times M$ Paraunitary Matrices over $GF(2r)$
- 4.5 Summary
- II Multivariate Cryptography
- 5 Introduction
 - 5.1 Historical Background and Motivation
 - 5.2 RSA
 - 5.3 Elliptic Curve Cryptography
 - 5.4 Multivariate Cryptography
- 6 Wavelet Self-Synchronizing Stream Cipher
 - 6.1 Background Review
 - 6.1.1 Classification of Stream Ciphers
 - 6.2 Wavelet Self-Synchronizing Stream Cipher (WSSC)
 - 6.2.1 Modified Wavelet Transform
 - 6.2.2 Basic Round of the WSSC
 - 6.2.3 Multiple Rounds of the WSSC
 - 6.2.4 Key Setup
 - 6.3 Cryptanalysis of the WSSC
 - 6.3.1 Interpolation Attack
 - 6.3.2 Algebraic Attacks
 - 6.3.3 Delta Attack
 - 6.3.4 Time-Memory Tradeoff Attack
 - 6.3.5 Divide-and-Conquer Attack
 - 6.3.6 Correlation and Distinguishing Attacks
 - 6.4 Performance Evaluation
 - 6.5 Summary
- 7 Wavelet Block Cipher
 - 7.1 Background Review
 - 7.1.1 Feistel Cipher and Data Encryption Standard (DES)
 - 7.1.2 Advanced Encryption Standard (AES)
 - 7.2 Wavelet Block Cipher (WBC)
 - 7.2.1 Linear Components of the WBC
 - 7.2.2 Nonlinear Components of the WBC
 - 7.3 Two-Round Wavelet Block Cipher
 - 7.3.1 Key Setup
 - 7.4 Cryptanalysis of the WBC
 - 7.4.1 Differential and Linear Attacks
 - 7.4.2 Divide-and-Conquer Attack

- 7.4.3 Interpolation Attack
- 7.4.4 Delta Attack
- 7.5 Performance Evaluation
- 7.6 Summary
- 8 Paraunitary Public-Key Cryptography
 - 8.1 Background Review
 - 8.1.1 Signature Based on Birational Permutations
 - 8.1.2 Tame Transformation Methods
 - 8.1.3 Tractable Rational Map Cryptosystem
 - 8.1.4 C^* Algorithm and its Variants
 - 8.2 Paraunitary Asymmetric Cryptosystem (PAC)
 - 8.2.1 Bijective Mappings
 - 8.2.2 Polynomial Vector
 - 8.2.3 Setup Algorithms
 - 8.3 Probabilistic PAC
 - 8.4 On the Computational Security of the PAC
 - 8.5 A Practical Instance of the PAC
 - 8.5.1 Constructing the Polynomial Vector
 - 8.5.2 Complexity of the PAC
 - 8.6 Cryptanalysis of the Instance of the PAC
 - 8.6.1 Grobner Basis
 - 8.6.2 Univariate Polynomial Representation of the Public Polynomials
 - 8.6.3 XL and FXL Algorithms
 - 8.6.4 An Attack for Small r
 - 8.7 Paraunitary Digital Signature Scheme (PDSS)
 - 8.7.1 Polynomial Vector
 - 8.7.2 Setup Algorithm
 - 8.7.3 A Practical Instance of the PDSS
 - 8.8 Summary
- III Error-Control Coding
- 9 Some Basic Concepts of Error-Control Coding
- 10 Double-Circulant Wavelet Block Codes
 - 10.1 Structure of Double-Circulant Wavelet Coding
 - 10.1.1 Wavelet Structures for Encoding and Decoding
 - 10.2 Maximum-Distance Separable Codes
 - 10.3 Double-Circulant Self-Dual Codes
 - 10.3.1 Fundamental Structure of Self-Dual Wavelet Codes
 - 10.3.2 Maximum-Distance Separable Self-Dual Codes
 - 10.4 Decoding Wavelet Codes
 - 10.4.1 Bounded-Distance Decoding of $(20, 10, 6)$ Double-Circulant Wavelet Code
 - 10.4.2 Bounded-Distance Decoding of the Wavelet-Golay Code
 - 10.5 Summary
- 11 Arbitrary-Rate Wavelet Block Codes
 - 11.1 Structure of Wavelet Coding
 - 11.1.1 Wavelet Structure for Encoding and Decoding

- 11.2 Rate-1/L Maximum-Distance Separable Codes
- 11.3 Arbitrary-Rate Wavelet Block Codes
- 11.4 Arbitrary-Rate Maximum-Distance Separable Codes
- 11.5 Decoding Arbitrary-Rate Wavelet Block Codes
 - 11.5.1 Bounded-Distance Decoding of the (12, 4, 6) Wavelet Code
 - 11.5.2 Symbol Error Correction in the (7, 3, 5) MDS Code
 - 11.5.3 Tail-Biting Trellises for Wavelet Block Codes
- 11.6 Summary
- 12 Wavelet Convolutional Codes
 - 12.1 Structure of Wavelet Convolutional Codes
 - 12.2 Algebraic Properties of Wavelet Convolutional Encoders
 - 12.3 Syndrome Generators and Dual Encoders
 - 12.4 Self-Dual and Self-Orthogonal Convolutional Codes
 - 12.5 Time-Varying Wavelet Convolutional Codes and Bipartite Trellises
 - 12.6 Summary
- Appendices
 - A Proofs of Chap. 4 in Part I
 - B Efficient Generation of PU Matrices
 - C Toy Examples of the PAC and the PDSS
 - D Proofs of Chap. 10 in Part III
 - E Brief Review of Trellis Structures
- Bibliography
- Index

章节摘录

From a practical point of view, a complete classification of orthogonal filter banks is of great interest. The underlying reason is based on the observation that some filter banks are more useful than 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 building block 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 independently while the PR property is preserved. Constant PU matrices are unitary matrices that can be realized using planar rotations over the real 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 a similar factorization for multivariate PU matrices. Nevertheless, Venkataraman and Levy disproved this 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 the multiplication of IIR PU building blocks in each of the two variables in arbitrary orders. A similar level-by-level factorization approach was taken in [58] for 2×2 PU matrices over fields of characteristic 2. Although a first-level factorization is always possible, a complete factorization seems to be difficult to find. The factorization of PU matrices over finite fields is not a trivial extension of the complex-field techniques. In [166], authors show that the factorization of PU matrices over $GF(p)$, for a prime p , using the previously introduced elementary PU degree-1 and degree-2 building blocks is not complete. In other words, there are orthogonal filter banks that cannot be represented by cascading these building blocks. The main results of this chapter are summarized below:

1. In Sec. 4.2, we introduce the elementary unitary building block over IF_2 , that acts like the Householder matrix. Any unitary matrix over IF_{2^r} can be represented as a product of the unitary building block and permutations of the identity matrix.

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>