

国外电子信息精品著作(影印版)

有限域小波及其在 密码学和译码中的应用

Finite-Field Wavelets with Applications
in Cryptography and Coding

Faramarz Fekri
Farshid Delgosha



科学出版社

国外电子信息精品著作(影印版)

Finite-Field Wavelets with Applications

in Cryptography and Coding

**有限域小波及其在密码学
和译码中的应用**

Faramarz Fekri

Farshid Delgosha

科学出版社

北京

图字:01-2012-2728

内 容 简 介

本书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。本书还介绍了此理论在纠错码和数据安全性上的首次应用。

本书可作为应用数学、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。

Original edition, entitled FINITE-FIELD WAVELETS WITH APPLICATIONS IN CRYPTOGRAPHY AND CODING, 1E, 9780130600202 by FEKRI, FARAMARZ; DELGOSHA, FARSHID, published by Pearson Education, Inc, publishing as Prentice Hall, Copyright © 2011 Pearson Education, Inc.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

China edition published by PEARSON EDUCATION ASIA LTD., and CHINA SCIENCE PUBLISHING & MEDIA LTD. (SCIENCE PRESS) Copyright © 2012

本版本仅售于中国大陆地区(不包含台湾、香港与澳门地区)。

图书在版编目(CIP)数据

有限域小波及其在密码学和译码中的应用 = Finite-Field Wavelets with Applications in Cryptography and Coding: 英文/(美)法拉马兹(Fekri, F.)等编著. —影印版. —北京:科学出版社, 2012

(国外电子信息精品著作)

ISBN: 978-7-03-034383-3

I. 有… II. 法… III. 有限域-小波理论-应用-密码-译码-英文
IV. TN918.3

中国版本图书馆 CIP 数据核字(2012)第 103233 号

责任编辑:张宇 余丁 / 责任印制:张倩 / 封面设计:陈敬

科学出版社出版

北京东黄城根北街 16 号

邮政编码: 100717

<http://www.sciencep.com>

源海印刷有限责任公司印刷

科学出版社发行 各地新华书店经销

*

2012 年 6 月第 一 版 开本: 787×1092 1/16

2012 年 6 月第一次印刷 印张: 19 1/2

字数: 426 000

定价: 65.00 元

(如有印装质量问题,我社负责调换)

《国外电子信息精品著作》序

20 世纪 90 年代以来，信息科学技术成为世界经济的中坚力量。随着经济全球化的进一步发展，以微电子、计算机、通信和网络技术为代表的信息技术，成为人类社会进步过程中发展最快、渗透性最强、应用面最广的关键技术。信息技术的发展带动了微电子、计算机、通信、网络、超导等产业的发展，促进了生命科学、新材料、能源、航空航天等高新技术产业的成长。信息产业的发展水平不仅是社会物质生产、文化进步的基本要素和必备条件，也是衡量一个国家的综合国力、国际竞争力和发展水平的重要标志。在中国，信息产业在国民经济发展中占有举足轻重的地位，成为国民经济重要支柱产业。然而，中国的信息科学支持技术发展的力度不够，信息技术还处于比较落后的水平，因此，快速发展信息科学技术成为我国迫在眉睫的大事。

要使我国的信息技术更好地发展起来，需要科学工作者和工程技术人员付出艰辛的努力。此外，我们要从客观上为科学工作者和工程技术人员创造更有利于发展的环境，加强对信息技术的支持与投资力度，其中也包括与信息技术相关的图书出版工作。

从出版的角度考虑，除了较好较快地出版具有自主知识产权的成果外，引进国外的优秀出版物是大有裨益的。洋为中用，将国外的优秀著作引进到国内，促进最新的科技成就迅速转化为我们自己的智力成果，无疑是值得高度重视的。科学出版社引进一批国外知名出版社的优秀著作，使我国从事信息技术的广大科学工作者和工程技术人员能以较低的价格购买，对于推动我国信息技术领域的科研与教学是十分有益的事。

此次科学出版社在广泛征求专家意见的基础上，经过反复论证、仔细遴选，共引进了接近 30 本外版书，大体上可以分为两类，第一类是基础理论著作，第二类是工程应用方面的著作。所有的著作都涉及信息领域的最新成果，大多数是 2005 年后出版的，力求“层次高、

内容新、参考性强”。在内容和形式上都体现了科学出版社一贯奉行的严谨作风。

当然，这批书只能涵盖信息科学技术的一部分，所以这项工作还应该继续下去。对于一些读者面较广、观点新颖、国内缺乏的好书还应该翻译成中文出版，这有利于知识更好更快地传播。同时，我也希望广大读者提出好的建议，以改进和完善丛书的出版工作。

总之，我对科学出版社引进外版书这一举措表示热烈的支持，并盼望这一工作取得更大的成绩。

A large, stylized black ink signature of the name '王越' (Wang Yue) in cursive script.

中国科学院院士

中国工程院院士

2006年12月

To my wife, Saeideh, and my mother, Shafiqeh

-Faramarz Fekri

To my love, Nubia, and my mother, Fatemeh

-Farshid Delgosha

Preface

The basic commodity of the scalable information infrastructure of the future will certainly be represented in discrete alphabet form. Such information representations must be transmitted, stored, and manipulated securely without error. Symmetric and asymmetric cryptosystems, as well as error-control codes have already been indispensable components of many systems. However, notions of complexity, scalability, and adaptability are becoming critical challenges for coding and data security algorithms. Specifically, designing such algorithms with low power and low complexity for applications in widely used resource-limited hand-held devices and sensor networks is an increasingly difficult task.

Finite-field wavelet transforms connect two areas: wavelets and finite-alphabet processing. They were inspired by wavelet transforms defined over the real and the complex fields. Wavelets and filter banks that operate on real or complex signals are already well established as powerful signal processing tools. They give an efficient signal representation that is localized in both time and frequency. Therefore, they have found widespread applications in areas such as audio and video compression and time–frequency analysis, and have also become a host to others. Like its real-field counterpart, the essence of this book is to show that processing based on a newly developed theory of wavelet transforms over finite alphabets can play a key role in symmetric cryptography, public-key cryptosystems, digital signature schemes, error-control coding, and much more. The book defines wavelet transform over finite fields and presents a framework for new approaches to algebraic cryptography and error-control coding. It is hoped that this introduction of the rich set of finite-alphabet processing techniques will serve as catalyst, stimulating further development in both theory and practice of new coding and security schemes for resource-limited devices in particular.

The book is intended as a source for researchers and scientists in areas of applied mathematics, cryptography, and error-control coding. It can also be valuable for practitioners who wish to develop cryptographic schemes. The writing style and the appendices are attempted to make it as self-contained as possible. Some background in linear algebra, finite fields, signal processing, wavelets

and filter banks, cryptography, and coding theory is helpful. However, this familiarity can also be picked up as needed.

Chapter 1 provides the notation used throughout the book, reviews some background in abstract and linear algebra, and formally defines the unitary and paraunitary matrices. Readers interested in more in-depth knowledge are referred to [10, 109, 125, 177]. The rest of the book is divided into three parts. Part I studies the discrete-time wavelet transform over arbitrary fields and the construction of unitary and paraunitary matrices over fields of characteristic two. Chapter 2 provides reviews of discrete Fourier transforms over finite fields and the related work on wavelets and filter banks over finite fields. Chapter 3 analyzes discrete-time wavelet basis functions for infinite-dimensional signal spaces over a general class of finite fields $\text{GF}(p^r)$ with emphasis on $\text{GF}(2^r)$. Chapter 4 undertakes the theory of multi-channel paraunitary filter banks over $\text{GF}(2^r)$. It introduces the necessary and sufficient elementary (prime) building blocks to construct orthogonal filter banks over these fields. For background in signal processing, filter banks, and wavelets, [156, 192, 199, 203] are helpful references.

Part II is completely devoted to multivariate cryptography via wavelets and paraunitary matrices. Knowledge of basic concepts in cryptograph such as symmetric cryptography, stream cipher, block cipher, public-key cryptography, and digital signature are necessary, which can be obtained from [140, 190]. After a brief introduction and review of self-synchronizing stream ciphers, Part II presents a new proposal for a wavelet-based stream cipher. In Chap. 7, the authors adopt a similar structure for the development of a wavelet-based block cipher. In fact, the similarities between the wavelet stream and block ciphers allow the designer to implement them both on a single chip as a bimodal cipher. At the end of Part II, paraunitary matrices from Part I are used to study the module of multivariate polynomial vectors and provide general frameworks for the design of new public key and signature schemes. The security of such systems is based on the difficulty of solving systems of multivariate polynomial equations over finite fields. As a matter of fact, the algebraic nature of the design is exploited to provide mathematical evidence, for the first time, that relates the security of authors' schemes to the difficulty of the claimed mathematical problem. In addition, practical instances of these general designs are suggested and their efficiency are shown in comparison with other existing designs.

Part III undertakes the application of wavelets and filter banks onto error-control coding. To obtain the necessary background, one may refer to [128, 207]. The use of two-band wavelets and filter banks in the construction of half-rate block codes over an arbitrary finite field is presented in Chap. 10. This chapter applies two-band orthogonal wavelet systems to generate double-circulant self-dual codes. It also describes a bounded-distance decoding technique for these codes. Then, using multi-band orthogonal filter banks, a structure to generate arbitrary-rate block codes is developed in Chap. 11. Along with other results concerning arbitrary-rate block codes, the implications of the wavelet coding technique for the construction of tail-biting trellises that simplify soft-decision decoding of some block codes are also discussed. The application of finite-field wavelets is extended to the class of convolutional codes in Chap. 12. Some algebraic properties of wavelet convolutional codes are also explored. Furthermore, new types of time-varying convolutional codes with unusual trellises that reduce the decoding latency are introduced.

The authors wish to acknowledge John Cozzens' program at NSF and the Georgia Tech Broadband Institute (GTBI) for their support of this work. They are very grateful to many people who contributed to the work. Specially, the authors wish to thank Ronald W. Schafer, Russell

M. Mersereau, and Steven W. McLaughlin at Georgia Tech, who contributed generously to the development of the ideas in wavelets and error-control coding. They also thank Kevin Chan and Mina Sartipi, who provided many valuable technical ideas and helped the development of the wavelet block cipher and wavelet convolutional codes, respectively, during their graduate studies at Georgia Tech. Finally, they greatly appreciate Tom Robbins, Alice Dworkin, Andrew Gilfillan, and his colleagues at Pearson Prentice Hall for their support and for steering the project into the final stage. Their reviewers enhanced the quality of the book further.

FARAMARZ FEKRI
FARSHID DELGOSHA
April 2010

Acronyms

Part I

ADFT	algebraic discrete Fourier transform
BFT	binary-field transform
CCP	cyclic convolution property
CWT	cyclic wavelet transform
DFT	discrete Fourier transform
DTWT	discrete-time wavelet transform
DWT	discrete wavelet transform
FFT	fast Fourier transform
FIR	finite impulse response
IDFT	inverse discrete Fourier transform
IIR	infinite impulse response
LOT	lapped orthogonal transform
LSB	least significant bit
PR	perfect reconstruction
PU	paraunitary

Part II

AES	advanced encryption standard
CFB	cipher feedback
DB	decryption block

DES	data encryption standard
EB	encryption block
ECC	elliptic curve cryptography
ECDSA	elliptic curve digital signature algorithm
FSM	finite state machine
FXL	fixing and extended relinearization
HFE	hidden-field equations
LDPC	low-density parity-check
LFSR	linear feedback shift register
NC	nonlinear combiner
NF	nonlinear filter
OFB	output feedback
OWF	one-way function
PAC	paraunitary asymmetric cryptosystem
PDSS	paraunitary digital-signature scheme
SSC	self-synchronizing stream cipher
TLU	table lookup
TOWF	trapdoor one-way function
WBC	wavelet block cipher
WSSC	wavelet self-synchronizing stream cipher
XL	extended linearization

Part III

AWGN additive white gaussian noise
BCH Bose Chaudhuri Hocquenghem
CI circularly invertible

LTI linear time-invariant
MDS maximum-distance separable
ML maximum likelihood
MLD maximum-likelihood decoding
PUM partial-unit-memory

Contents

Preface	ix	
Figures	xiii	
Tables	xvii	
Algorithms	xix	
Acronyms	xxi	
1	Introduction and Some Algebra Preliminaries	1
1.1	Notations	3
1.1.1	Set Notation	3
1.1.2	Matrix Notation	5
1.1.3	Asymptotic Notation	8
1.1.4	General Notation	9
1.2	Abstract Algebraic Background	9
1.2.1	Group	9
1.2.2	Ring	11
1.2.3	Field	13
1.2.4	Irreducible and Primitive Polynomials	14
1.2.5	Construction of Extension Fields	15
1.2.6	Module	16
1.2.7	Algebra	17

1.3	Linear Algebra Background	18
1.3.1	Involution	18
1.3.2	Sesquilinear Form	19
1.3.3	Unitary Matrix	22
1.3.4	Paraunitary Matrix	23
I	Finite-Field Wavelets	25
2	Background Review and Motivation	27
2.1	Wavelets for Discrete-Time Signals	28
2.2	Cyclic Wavelet Transforms	31
2.3	Review of Transforms over Finite Fields	34
2.3.1	Discrete Fourier Transform over Finite Fields	35
2.3.2	Base-Field Transforms over Finite Fields	37
2.3.3	Related Work on Finite-Field Wavelets	38
3	Finite-Field Wavelet Basis Functions	43
3.1	Finite-Field Discrete-Time Basis	44
3.1.1	Non-Degenerate Bilinear Form	44
3.1.2	Orthonormal Wavelet Basis over Finite Fields	46
3.1.3	Completeness of the Orthonormal Set	48
3.2	Construction of Mother Wavelet and Scaling Function	48
3.3	Summary	57
4	Theory of Paraunitary Filter Banks over Fields of Characteristic 2	58
4.1	Background Review	61
4.1.1	Degree-1 Paraunitary Building Block over $\mathbf{GF}(2)$	61
4.1.2	Degree-2 Paraunitary Building Blocks over $\mathbf{GF}(2)$	61
4.1.3	Lapped Orthogonal Transforms over $\mathbf{GF}(2)$	62
4.2	Unitary Matrices over $\mathbf{GF}(2^r)$	62
4.3	Paraunitary Matrices over Fields of Characteristic 2	66
4.3.1	Properties of 2×2 Paraunitary Matrices over $\mathbf{GF}(2^r)$	69
4.4	Factorization of Paraunitary Matrices over $\mathbf{GF}(2^r)$	71
4.4.1	Degree-1 Paraunitary Building Block over $\mathbf{GF}(2^r)$	72
4.4.2	Degree-2 Paraunitary Building Block over $\mathbf{GF}(2^r)$	73
4.4.3	Degree- $2r$ Paraunitary Building Block over $\mathbf{GF}(2^r)$	75
4.4.4	Factorization of 2×2 Paraunitary Matrices over $\mathbf{GF}(2^r)$	75
4.4.5	Degree- $M\tau$ Paraunitary Building Block over $\mathbf{GF}(2^r)$	80
4.4.6	Factorization of $M \times M$ Paraunitary Matrices over $\mathbf{GF}(2^r)$	86
4.5	Summary	88

II	Multivariate Cryptography	89
5	Introduction	91
5.1	Historical Background and Motivation	91
5.2	RSA	93
5.3	Elliptic Curve Cryptography	94
5.4	Multivariate Cryptography	94
6	Wavelet Self-Synchronizing Stream Cipher	97
6.1	Background Review	97
6.1.1	Classification of Stream Ciphers	98
6.2	Wavelet Self-Synchronizing Stream Cipher (WSSC)	105
6.2.1	Modified Wavelet Transform	106
6.2.2	Basic Round of the WSSC	109
6.2.3	Multiple Rounds of the WSSC	111
6.2.4	Key Setup	112
6.3	Cryptanalysis of the WSSC	114
6.3.1	Interpolation Attack	114
6.3.2	Algebraic Attacks	116
6.3.3	Delta Attack	118
6.3.4	Time–Memory Tradeoff Attack	120
6.3.5	Divide-and-Conquer Attack	122
6.3.6	Correlation and Distinguishing Attacks	122
6.4	Performance Evaluation	123
6.5	Summary	123
7	Wavelet Block Cipher	125
7.1	Background Review	125
7.1.1	Feistel Cipher and Data Encryption Standard (DES)	126
7.1.2	Advanced Encryption Standard (AES)	126
7.2	Wavelet Block Cipher (WBC)	127
7.2.1	Linear Components of the WBC	128
7.2.2	Nonlinear Components of the WBC	130
7.3	Two-Round Wavelet Block Cipher	130
7.3.1	Key Setup	132
7.4	Cryptanalysis of the WBC	133
7.4.1	Differential and Linear Attacks	133
7.4.2	Divide-and-Conquer Attack	135
7.4.3	Interpolation Attack	135
7.4.4	Delta Attack	137
7.5	Performance Evaluation	137
7.6	Summary	138

8	Paraunitary Public-Key Cryptography	139
8.1	Background Review	139
8.1.1	Signature Based on Birational Permutations	140
8.1.2	Tame Transformation Methods	141
8.1.3	Tractable Rational Map Cryptosystem	141
8.1.4	C^* Algorithm and its Variants	141
8.2	Paraunitary Asymmetric Cryptosystem (PAC)	146
8.2.1	Bijjective Mappings	149
8.2.2	Polynomial Vector φ	150
8.2.3	Setup Algorithms	151
8.3	Probabilistic PAC	152
8.4	On the Computational Security of the PAC	153
8.5	A Practical Instance of the PAC	156
8.5.1	Constructing the Polynomial Vector Ψ	157
8.5.2	Complexity of the PAC	159
8.6	Cryptanalysis of the Instance of the PAC	160
8.6.1	Gröbner Basis	161
8.6.2	Univariate Polynomial Representation of the Public Polynomials	161
8.6.3	XL and FXL Algorithms	162
8.6.4	An Attack for Small r	162
8.7	Paraunitary Digital Signature Scheme (PDSS)	163
8.7.1	Polynomial Vector φ	165
8.7.2	Setup Algorithm	166
8.7.3	A Practical Instance of the PDSS	166
8.8	Summary	168
III	Error-Control Coding	169
9	Some Basic Concepts of Error-Control Coding	171
10	Double-Circulant Wavelet Block Codes	175
10.1	Structure of Double-Circulant Wavelet Coding	176
10.1.1	Wavelet Structures for Encoding and Decoding	176
10.2	Maximum-Distance Separable Codes	181
10.3	Double-Circulant Self-Dual Codes	186
10.3.1	Fundamental Structure of Self-Dual Wavelet Codes	186
10.3.2	Maximum-Distance Separable Self-Dual Codes	188
10.4	Decoding Wavelet Codes	189
10.4.1	Bounded-Distance Decoding of $(20, 10, 6)$ Double-Circulant Wavelet Code	189
10.4.2	Bounded-Distance Decoding of the Wavelet–Golay Code	192
10.5	Summary	196

11	Arbitrary-Rate Wavelet Block Codes	197
11.1	Structure of Wavelet Coding	198
11.1.1	Wavelet Structure for Encoding and Decoding	198
11.2	Rate- $\frac{1}{2}$ Maximum-Distance Separable Codes	202
11.3	Arbitrary-Rate Wavelet Block Codes	206
11.4	Arbitrary-Rate Maximum-Distance Separable Codes	209
11.5	Decoding Arbitrary-Rate Wavelet Block Codes	212
11.5.1	Bounded-Distance Decoding of the (12, 4, 6) Wavelet Code	212
11.5.2	Symbol Error Correction in the (7, 3, 5) MDS Code	215
11.5.3	Tail-Biting Trellises for Wavelet Block Codes	217
11.6	Summary	220
12	Wavelet Convolutional Codes	221
12.1	Structure of Wavelet Convolutional Codes	222
12.2	Algebraic Properties of Wavelet Convolutional Encoders	224
12.3	Syndrome Generators and Dual Encoders	229
12.4	Self-Dual and Self-Orthogonal Convolutional Codes	230
12.5	Time-Varying Wavelet Convolutional Codes and Bipartite Trellises	232
12.6	Summary	244
	Appendices	245
A	Proofs of Chap. 4 in Part I	247
B	Efficient Generation of PU Matrices	253
C	Toy Examples of the PAC and the PDSS	259
D	Proofs of Chap. 10 in Part III	264
E	Brief Review of Trellis Structures	266
	Bibliography	270
	Index	279

Figures

2.1	<i>L</i> -band wavelet decomposition	28
2.2	<i>L</i> -band maximally decimated filter bank	30
2.3	Multi-resolution decomposition and reconstruction using a two-band tree structure	39
3.1	Polyphase representation of two-band filter bank	48
4.1	<i>M</i> -channel maximally decimated filter bank: (a) Time-domain representation; (b) polyphase representation	59
6.1	General model of synchronous stream ciphers: (a) Encryption; (b) decryption	100
6.2	LFSR of length <i>L</i>	100
6.3	OFB mode of block ciphers	103
6.4	Canonical model of SSC: (a) Encryption; (b) decryption	104
6.5	CFB mode of block ciphers	105
6.6	Modified DTWT and its inverse: (a) Transform; (b) inverse transform	106
6.7	Basic round of the WSSC: (a) Encryption; (b) decryption	109
6.8	Transforming the WSSC encryption to the canonical form of SSCs in Fig. 6.4a: (a) Original form; (b) H_2 moved past the junction point <i>A</i> ; (c) canonical form	110
6.9	Multiple rounds of the WSSC: (a) Encryption; (b) decryption	111
6.10	Modified <i>L</i> -band DTWT and its inverse: (a) Transform; (b) inverse transform	114
6.11	Two decryption rounds of the WSSC	119
7.1	Feistel cipher. (a) Encryption; (b) Decryption	127
7.2	Wavelet decomposition of an image by a two-stage, two-band, orthogonal filter bank over GF(256)	128
7.3	Multirate filter implementation of the elementary EB	129