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代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。

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。

王越

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, Shafigheh

-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 cryotography 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 $\mathsf{GF}(p^r)$ with emphasis on $\mathsf{GF}(2^r)$. Chapter 4 undertakes the theory of multi-channel paraunitary filter banks over $\mathsf{GF}(2^r)$. 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. McLauglin 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

Figures