Springer Series on
SIGNALS AND COMMUNICATION TECHNOLOGY

SIGNALS AND COMMUNICATION TECHNOLOGY

Multimedia Database Retrieval
A Human-Centered Approach
P. Muneesawang and L. Guan
ISBN 0-387-25627-X

Broadband Fixed Wireless Access
A System Perspective
M. Engels and F. Petre
ISBN 0-387-33956-6

Distributed Cooperative Laboratories
Networking, Instrumentation, and Measurements
F. Davoli, S. Palazzo and S. Zappatore (Eds.)
ISBN 0-387-29811-8

The Variational Bayes Method in Signal Processing
V. Šmídl and A. Quinn
ISBN 3-540-28819-8

Topics in Acoustic Echo and Noise Control
Selected Methods for the Cancellation of Acoustical Echoes, the Reduction of Background Noise, and Speech Processing
E. Hänsler and G. Schmidt (Eds.)
ISBN 3-540-33212-x

EM Modeling of Antennas and RF Components for Wireless Communication Systems
F. Gustrau, D. Manteuffel
ISBN 3-540-28614-4

Interactive Video Methods and Applications
R. I Hammoud (Ed.)
ISBN 3-540-33214-6

ContinuousTime Signals
Y. Shmaliy
ISBN 1-4020-4817-3

Voice and Speech Quality Perception
Assessment and Evaluation
U. Jekosch
ISBN 3-540-24095-0

Advanced ManMachine Interaction
Fundamentals and Implementation
K.-F. Kraiss
ISBN 3-540-30618-8

Orthogonal Frequency Division Multiplexing for Wireless Communications
Y. (Geoffrey) Li and G.L. Stüber (Eds.)
ISBN 0-387-29095-8

Circuits and Systems Based on Delta Modulation
Linear, Nonlinear and Mixed Mode Processing
D.G. Zrilic ISBN 3-540-23751-8

Functional Structures in Networks
AMLn—A Language for Model Driven Development of Telecom Systems
T. Muth ISBN 3-540-22545-5

RadioWave Propagation for Telecommunication Applications
H. Sizun ISBN 3-540-40758-8

Electronic Noise and Interfering Signals
Principles and Applications
G. Vasilescu ISBN 3-540-40741-3

DVB
The Family of International Standards for Digital Video Broadcasting, 2nd ed.
U. Reimers ISBN 3-540-43545-X

Digital Interactive TV and Metadata
Future Broadcast Multimedia
A. Lugmayr, S. Niiranen, and S. Kalli
ISBN 3-387-20843-7

Adaptive Antenna Arrays
Trends and Applications
S. Chandran (Ed.) ISBN 3-540-20199-8

Digital Signal Processing with Field Programmable Gate Arrays
U. Meyer-Baese ISBN 3-540-21119-5

Neuro-Fuzzy and Fuzzy Neural Applications in Telecommunications
P. Stavroulakis (Ed.) ISBN 3-540-40759-6

SDMA for Multipath Wireless Channels
Limiting Characteristics and Stochastic Models
I.P. Kovalyov ISBN 3-540-40225-X

Digital Television
A Practical Guide for Engineers
W. Fischer ISBN 3-540-01155-2

Speech Enhancement
J. Benesty (Ed.)
ISBN 3-540-24039-X

Multimedia Communication Technology
Representation, Transmission and Identification of Multimedia Signals
J.R. Ohm ISBN 3-540-01249-4

continued after index

Francisco Rodríguez-Henríquez
N.A. Saqib
A. Díaz-Pèrez
Çetin Kaya Koç

Cryptographic Algorithms on Reconfigurable Hardware

Springer

Francisco Rodríguez-Henríquez
Arturo Díaz Pérez

Departamento de Computación
Centro de Investigación y de Estudios Avanzados del IPN
Av. Instituto Politécnico Nacional No. 2508
Col. San Pedro Zacatenco. CP 07300
México, D.F.
MEXICO

Nazar Abbas Saqib
Centre for Cyber Technology and Spectrum Management
(CCT & SM)
National University of Sciences and Technology (NUST)
#295, Street 35, F-11/3, Islamabad-44000
Pakistan

Çetin Kaya Koç
Oregon State University
Corvallis, OR 97331, USA
&
Istanbul Commerce University
Eminönü, Istanbul 34112, Turkey

Cryptographic Algorithms on Reconfigurable Hardware

Library of Congress Control Number: 2006929210

ISBN 0-387-33883-7 e-ISBN 0-387-36682-2
ISBN 978-0-387-33883-5

Printed on acid-free paper.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

springer.com

Dedication

A mi esposa Nareli y mi hija Ana Iremi, por su amor y estoica paciencia;
A mis padres y hermanos, por compartir las mismas esperanzas.
Francisco Rodríguez-Henríquez

To Afshan (wife),Fizza (daughter), Ahmer (son) and Aashir (son), I love you all.
Nazar A. Saqib

To Mary, Maricarmen and Liliana, my wife and daughters, my love will keep alive for you all.
Arturo Díaz-Pérez

With my love to Laurie, Murat, and Cemre.
Çetin K. Koç

Contents

List of Figures

List of Tables

List of Algorithms