

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

Continuous Time 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

AML_n—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

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.

© 2006 Springer Science+Business Media, LLC

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC, 233 Spring Street, New York, NY 10013, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

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	XIII
List of Tables	XIX
List of Algorithms	XX
Acronyms	XXIII
Preface	XXV
1 Introduction	1
1.1 Main goals	1
1.2 Monograph Organization	3
1.3 Acknowledgments	4
2 A Brief Introduction to Modern Cryptography	7
2.1 Introduction	8
2.2 Secret Key Cryptography	9
2.3 Hash Functions	11
2.4 Public Key Cryptography	12
2.5 Digital Signature Schemes	15
2.5.1 RSA Digital Signature	16
2.5.2 RSA Standards	17
2.5.3 DSA Digital Signature	18
2.5.4 Digital Signature with Elliptic Curves	19
2.5.5 Key Exchange	23
2.6 A Comparison of Public Key Cryptosystems	24
2.7 Cryptographic Security Strength	26
2.8 Potential Cryptographic Applications	27
2.9 Fundamental Operations for Cryptographic Algorithms	29

2.10	Design Alternatives for Implementing Cryptographic Algorithms	31
2.11	Conclusions	32
3	Reconfigurable Hardware Technology	35
3.1	Antecedents	36
3.2	Field Programmable Gate Arrays	38
3.2.1	Case of Study I: Xilinx FPGAs	39
3.2.2	Case of Study II: Altera FPGAs	44
3.3	FPGA Platforms versus ASIC and General-Purpose Processor Platforms	48
3.3.1	FPGAs versus ASICs	48
3.3.2	FPGAs versus General-Purpose Processors	49
3.4	Reconfigurable Computing Paradigm	50
3.4.1	FPGA Programming	52
3.4.2	VHSIC Hardware Description Language (VHDL)	52
3.4.3	Other Programming Models for FPGAs	53
3.5	Implementation Aspects for Reconfigurable Hardware Designs	53
3.5.1	Design Flow	53
3.5.2	Design Techniques	55
3.5.3	Strategies for Exploiting FPGA Parallelism	58
3.6	FPGA Architecture Statistics	59
3.7	Security in Reconfigurable Hardware Devices	61
3.8	Conclusions	62
4	Mathematical Background	63
4.1	Basic Concepts of the Elementary Theory of Numbers	63
4.1.1	Basic Notions	64
4.1.2	Modular Arithmetic	67
4.2	Finite Fields	70
4.2.1	Rings	70
4.2.2	Fields	70
4.2.3	Finite Fields	70
4.2.4	Binary Finite Fields	71
4.3	Elliptic curves	73
4.3.1	Definition	73
4.3.2	Elliptic Curve Operations	74
4.3.3	Elliptic Curve Scalar Multiplication	76
4.4	Elliptic Curves over $GF(2^m)$	77
4.4.1	Point Addition	78
4.4.2	Point Doubling	78
4.4.3	Order of an Elliptic Curve	79
4.4.4	Elliptic Curve Groups and the Discrete Logarithm Problem	79
4.4.5	An Example	79

4.5	Point Representation	82
4.5.1	Projective Coordinates	83
4.5.2	López-Dahab Coordinates	84
4.6	Scalar Representation	85
4.6.1	Binary Representation	85
4.6.2	Recoding Methods	85
4.6.3	ω -NAF Representation	87
4.7	Conclusions	88
5	Prime Finite Field Arithmetic	89
5.1	Addition Operation	90
5.1.1	Full-Adder and Half-Adder Cells	90
5.1.2	Carry Propagate Adder	91
5.1.3	Carry Completion Sensing Adder	92
5.1.4	Carry Look-Ahead Adder	94
5.1.5	Carry Save Adder	96
5.1.6	Carry Delayed Adder	97
5.2	Modular Addition Operation	98
5.2.1	Omura’s Method	99
5.3	Modular Multiplication Operation	100
5.3.1	Standard Multiplication Algorithm	101
5.3.2	Squaring is Easier	104
5.3.3	Modular Reduction	105
5.3.4	Interleaving Multiplication and Reduction	108
5.3.5	Utilization of Carry Save Adders	110
5.3.6	Brickell’s Method	114
5.3.7	Montgomery’s Method	116
5.3.8	High-Radix Interleaving Method	123
5.3.9	High-Radix Montgomery’s Method	124
5.4	Modular Exponentiation Operation	124
5.4.1	Binary Strategies	125
5.4.2	Window Strategies	126
5.4.3	Adaptive Window Strategy	129
5.4.4	RSA Exponentiation and the Chinese Remainder Theorem	132
5.4.5	Recent Prime Finite Field Arithmetic Designs on FPGAs	136
5.5	Conclusions	138
6	Binary Finite Field Arithmetic	139
6.1	Field Multiplication	139
6.1.1	Classical Multipliers and their Analysis	141
6.1.2	Binary Karatsuba-Ofman Multipliers	142
6.1.3	Squaring	151
6.1.4	Reduction	152

6.1.5	Modular Reduction with General Polynomials	156
6.1.6	Interleaving Multiplication	159
6.1.7	Matrix-Vector Multipliers	161
6.1.8	Montgomery Multiplier	164
6.1.9	A Comparison of Field Multiplier Designs	165
6.2	Field Squaring and Field Square Root for Irreducible Trinomials	166
6.2.1	Field Squaring Computation	167
6.2.2	Field Square Root Computation	168
6.2.3	Illustrative Examples	171
6.3	Multiplicative Inverse	173
6.3.1	Inversion Based on the Extended Euclidean Algorithm .	175
6.3.2	The Itoh-Tsujii Algorithm	176
6.3.3	Addition Chains	178
6.3.4	ITMIA Algorithm	178
6.3.5	Square Root ITMIA	179
6.3.6	Extended Euclidean Algorithm versus Itoh-Tsujii Algorithm	181
6.3.7	Multiplicative Inverse FPGA Designs	183
6.4	Other Arithmetic Operations	183
6.4.1	Trace function	183
6.4.2	Solving a Quadratic Equation over $GF(2^m)$	184
6.4.3	Exponentiation over Binary Finite Fields	185
6.5	Conclusions	186
7	Reconfigurable Hardware Implementation of Hash Functions	189
7.1	Introduction	189
7.2	Some Famous Hash Functions	191
7.3	MD5	193
7.3.1	Message Preprocessing	194
7.3.2	MD Buffer Initialization	196
7.3.3	Main Loop	197
7.3.4	Final Transformation	198
7.4	SHA-1, SHA-256, SHA-384 and SHA-512	201
7.4.1	Message Preprocessing	202
7.4.2	Functions	204
7.4.3	SHA-1	205
7.4.4	Constants	206
7.4.5	Hash Computation	207
7.5	Hardware Architectures	210
7.5.1	Iterative Design	211
7.5.2	Pipelined Design	212
7.5.3	Unrolled Design	212
7.5.4	A Mixed Approach	213
7.6	Recent Hardware Implementations of Hash Functions	213

7.7	Conclusions	220
8	General Guidelines for Implementing Block Ciphers in FPGAs	221
8.1	Introduction	221
8.2	Block Ciphers	222
8.2.1	General Structure of a Block Cipher	223
8.2.2	Design Principles for a Block Cipher	224
8.2.3	Useful Properties for Implementing Block Ciphers in FPGAs	227
8.3	The Data Encryption Standard	232
8.3.1	The Initial Permutation (IP^{-1})	233
8.3.2	Structure of the Function f_k	234
8.3.3	Key Schedule	237
8.4	FPGA Implementation of DES Algorithm	238
8.4.1	DES Implementation on FPGAs	238
8.4.2	Design Testing and Verification	240
8.4.3	Performance Results	240
8.5	Other DES Designs	240
8.6	Conclusions	244
9	Architectural Designs For the Advanced Encryption Standard	245
9.1	Introduction	245
9.2	The Rijndael Algorithm	247
9.2.1	Difference Between AES and Rijndael	247
9.2.2	Structure of the AES Algorithm	248
9.2.3	The Round Transformation	249
9.2.4	ByteSubstitution (BS)	249
9.2.5	ShiftRows (SR)	251
9.2.6	MixColumns (MC)	252
9.2.7	AddRoundKey (ARK)	253
9.2.8	Key Schedule	254
9.3	AES in Different Modes	254
9.3.1	CTR Mode	255
9.3.2	CCM Mode	256
9.4	Implementing AES Round Basic Transformations on FPGAs	259
9.4.1	S-Box/Inverse S-Box Implementations on FPGAs	260
9.4.2	MC/IMC Implementations on FPGA	264
9.4.3	Key Schedule Optimization	267
9.5	AES Implementations on FPGAs	268
9.5.1	Architectural Alternatives for Implementing AES	269
9.5.2	Key Schedule Algorithm Implementations	273
9.5.3	AES Encryptor Cores - Iterative and Pipeline Approaches	276

9.5.4	AES Encryptor/Decryptor Cores- Using Look-Up Table and Composite Field Approaches for S-Box	278
9.5.5	AES Encryptor/Decryptor, Encryptor, and Decryptor Cores Based on Modified MC/IMC	281
9.5.6	Review of This Chapter Designs	284
9.6	Performance	285
9.6.1	Other Designs	285
9.7	Conclusions	288
10	Elliptic Curve Cryptography	291
10.1	Introduction	291
10.2	Hessian Form	294
10.3	Weierstrass Non-Singular Form	296
10.3.1	Projective Coordinates	296
10.3.2	The Montgomery Method	297
10.4	Parallel Strategies for Scalar Point Multiplication	300
10.5	Implementing scalar multiplication on Reconfigurable Hardware	302
10.5.1	Arithmetic-Logic Unit for Scalar Multiplication	303
10.5.2	Scalar multiplication in Hessian Form	304
10.5.3	Montgomery Point Multiplication	306
10.5.4	Implementation Summary	306
10.6	Koblitz Curves	308
10.6.1	The τ and τ^{-1} Frobenius Operators	309
10.6.2	$\omega\tau$ NAF Scalar Multiplication in Two Phases	312
10.6.3	Hardware Implementation Considerations	313
10.7	Half-and-Add Algorithm for Scalar Multiplication	317
10.7.1	Efficient Elliptic Curve Arithmetic	318
10.7.2	Implementation	321
10.7.3	Performance Estimation	324
10.8	Performance Comparison	326
10.9	Conclusions	328
	References	329
	Index	359

List of Figures

2.1	A Hierarchical Six-Layer Model for Information Security	
	Applications	8
2.2	Secret Key Cryptography	10
2.3	Recovering Initiator's Private Key	11
2.4	Generating a Pseudorandom Sequence	12
2.5	Public Key Cryptography	12
2.6	Basic Digital Signature/Verification Scheme	13
2.7	Public key cryptography Main Primitives	14
2.8	Diffie-Hellman Key Exchange Protocol	24
2.9	Elliptic Curve Variant of the Diffie-Hellman Protocol	25
3.1	A Taxonomy of Programmable Logic Devices	38
3.2	Xilinx Virtex II Architecture	40
3.3	Xilinx CLB	41
3.4	Slice Structure	42
3.5	VirtexE Logic Cell (LC)	42
3.6	CLB Configuration Modes	42
3.7	Stratix Block Diagram	45
3.8	Stratix LE	46
3.9	Design flow	54
3.10	Hardware Design Methodology	56
3.11	2-bit Multiplexer Using (a) Tristate Buffer. (b) LUT	57
3.12	Basic Architectures for (a) Iterative Looping (b) Loop Unrolling	58
3.13	Round-pipelining for (a) One Round (b) n Rounds	59
4.1	Elliptic Curve Equation $y^2 = x^3 + ax + b$ for Different a and b	73
4.2	Adding two Distinct Points on an Elliptic curve ($Q \neq -P$)	74
4.3	Adding two Points P and Q when $Q = -P$	75
4.4	Doubling a Point P on an Elliptic Curve	75
4.5	Doubling $P(x, y)$ when $y = 0$	76

XIV List of Figures

4.6	Elliptic Curve Scalar Multiplication kP , for $k = 6$ and for the Elliptic Curve $y^2 = x^3 - 3x + 3$	77
4.7	Elements in the Elliptic Curve of Equation (4.15)	81
5.1	Full-Adder and Half-Adder Cells	91
5.2	Carry Propagate Adder	92
5.3	Carry Completion Sensing Adder	93
5.4	Detecting Carry Completion	93
5.5	Carry Look-Ahead Adder	95
5.6	Carry Save Adder	96
5.7	Carry Delayed Adder	99
5.8	High-Radix Interleaving Method	123
5.9	Partitioning Algorithm	130
6.1	Binary Karatsuba-Ofman Strategy	148
6.2	Karatsuba-Ofman Multiplier $GF(2^{191})$	150
6.3	Programmable Binary Karatsuba-Ofman Multiplier	151
6.4	Squaring Circuit	152
6.5	Reduction Scheme	154
6.6	Pentanomial Reduction	155
6.7	A Method to Reduce k Bits at Once	156
6.8	$\alpha \cdot A(\alpha)$ Multiplication	160
6.9	LSB-First Serial/Parallel Multiplier	162
6.10	Finite State Machine for the Binary Euclidean Algorithm	182
6.11	Architecture of the Itoh-Tsujii Algorithm	182
7.1	Hash Function	190
7.2	Requirements of a Hash Function	191
7.3	Basic Structure of a Hash Function	191
7.4	MD5	193
7.5	Message Block = $32 \times 16 = 512$ Bits	195
7.6	Auxiliary Functions in Reconfigurable Hardware (a) $F(X,Y,Z)$ (b) $G(X,Y,Z)$ (c) $H(X,Y,Z)$ (d) $I(X,Y,Z)$	197
7.7	One MD5 Operation	198
7.8	Padding Message in SHA-1 and SHA-256	202
7.9	Padding Message in SHA-384 and SHA-512	204
7.10	Implementing SHA-1 Auxiliary Functions in Reconfigurable Hardware	205
7.11	Σ_0 , Σ_1 , σ_0 , and σ_1 in Reconfigurable Hardware	206
7.12	Single Operation for SHA-1	208
7.13	Single Operation for SHA-256	209
7.14	Iterative Approach for Hash Function Implementation	211
7.15	Hash Function Implementation (a) Unrolled Design (b) Combining k Stages	212
7.16	A Mixed Approach for Hash Function Implementation	213

8.1	General Structure of a Block Cipher	223
8.2	Same Resources for 2,3,4-in/1-out Boolean Logic in FPGAs	228
8.3	Three Approaches for the Implementation of S-Box in FPGAs	229
8.4	Permutation Operation in FPGAs	229
8.5	Shift Operation in FPGAs	230
8.6	Iterative Design Strategy	231
8.7	Pipeline Design Strategy	231
8.8	Sub-pipeline Design Strategy	231
8.9	DES Algorithm	234
8.10	DES Implementation on FPGA	239
8.11	Functional Simulation	241
8.12	Timing Verification	241
9.1	Basic Structure of Rijndael Algorithm	248
9.2	Basic Algorithm Flow	249
9.3	BS Operates at Each Individual Byte of the State Matrix	250
9.4	ShiftRows Operates at Rows of the State Matrix	252
9.5	MixColumns Operates at Columns of the State Matrix	252
9.6	ARK Operates at Bits of the State Matrix	253
9.7	Counter Mode Operations	255
9.8	Authentication and Verification Process for the CCM Mode	257
9.9	Encryption and Decryption Processes for the CCM Mode	258
9.10	S-Box and Inv. S-Box Using Same Look-Up Table	261
9.11	Block Diagram for 3-Stage MI Manipulation	262
9.12	Three-Stage Approach to Compute Multiplicative Inverse in Composite Fields	262
9.13	Basic Organization of a Block Cipher	269
9.14	Iterative Design Strategy	270
9.15	Loop Unrolling Design Strategy	271
9.16	Pipeline Design Strategy	271
9.17	Sub-pipeline Design Strategy	272
9.18	Sub-pipeline Design Strategy with Balanced Stages	272
9.19	KGEN Architecture	274
9.20	Key Schedule for an Encryptor Core in Iterative Mode	274
9.21	Key Schedule for a Fully Pipeline Encryptor Core	275
9.22	Key Schedule for a Fully Pipeline Encryptor/Decryptor Core	276
9.23	Key Schedule for a Fully Pipeline Encryptor/Decryptor Core with Modified IMC	276
9.24	Iterative Approach for AES Encryptor Core	277
9.25	Fully Pipeline AES Encryptor Core	278
9.26	S-Box and Inv S-Box Using (a) Different MI (b) Same MI	279
9.27	Data Path for Encryption/Decryption	280
9.28	Block Diagram for 3-Stage MI Manipulation	280
9.29	Three-stage to Compute Multiplicative Inverse in Composite Fields	280

XVI List of Figures

9.30 $GF(2^2)^2$ and $GF(2^2)$ Multipliers 281

9.31 Gate Level Implementation for x^2 and λx 281

9.32 AES Algorithm Encryptor/Decryptor Implementation 282

9.33 The Data Path for Encryptor Core Implementation 283

9.34 The Data Path for Decryptor Core Implementation 283

10.1 Hierarchical Model for Elliptic Curve Cryptography 293

10.2 Basic Organization of Elliptic Curve Scalar Implementation 303

10.3 Arithmetic-Logic Unit for Scalar Multiplication on FPGA
Platforms 304

10.4 An illustration of the τ and τ^{-1} Abelian Groups (with m an
Even Number) 310

10.5 A Hardware Architecture for Scalar Multiplication on the
NIST Koblitz Curve K-233 316

10.6 Point Halving Scalar Multiplication Architecture 322

10.7 Point Halving Arithmetic Logic Unit 322

10.8 Point Halving Execution 324

10.9 Point Addition Execution 325

10.10 Point Doubling Execution 325

List of Tables

2.1	A Comparison of Security Strengths (Source: [258])	27
2.2	A Few Potential Cryptographic Applications	29
2.3	Primitives of Cryptographic Algorithms (Symmetric Ciphers) . .	30
2.4	Comparison between Software, VLSI, and FPGA Platforms	31
3.1	FPGA Manufacturers and Their Devices	39
3.2	Xilinx FPGA Families Virtex-5, Virtex-4, Virtex II Pro and Spartan 3E	40
3.3	Dual-Port BRAM Configurations	43
3.4	Altera Stratix Devices	45
3.5	Comparing Cryptographic Algorithm Realizations on different Platforms	48
3.6	High Level FPGA Programming Software	53
4.1	Elements of the field $F = GF(2^4)$, Defined Using the Primitive Trinomial of Eq. ((4.12))	80
4.2	Scalar Multiples of the Point P of Equation (4.16)	82
4.3	A Toy Example of the Recoding Algorithm	86
4.4	Comparing Different Representations of the Scalar k	88
5.1	Modular Exponentiation Comparison Table	137
5.2	Modular Exponentiation: Software vs Hardware Comparison Table	138
6.1	The Computation of $C(x)$ Using Equation (6.5)	142
6.2	Space and Time Complexities for Several $m = 2^k$ -bit Hybrid Karatsuba-Ofman Multipliers	148
6.3	Fastest Reconfigurable Hardware $GF(2^m)$ Multipliers	165
6.4	Most Compact Reconfigurable Hardware $GF(2^m)$ Multipliers . .	166
6.5	Summary of Complexity Results	170

XVIII List of Tables

6.6	Irreducible Trinomials $P(x) = x^m + x^n + 1$ of Degree $m \in [160, 571]$ Encoded as $m(n)$, with m a Prime Number	171
6.7	Squaring matrix M of Eq. (6.40)	172
6.8	Square Root Matrix M^{-1} of Eq. (6.41)	173
6.9	Square and Square Root Coefficient Vectors	174
6.10	$\beta_i(a)$ Coefficient Generation for $m-1=192$	180
6.11	$\gamma_i(a)$ Coefficient Generation for $m-1=192$	181
6.12	BEA Versus ITMIA: A Performance Comparison	183
6.13	Design Comparison for Multiplicative Inversion in $GF(2^m)$	184
7.1	Some Known Hash Functions	192
7.2	Bit Representation of the Message M	194
7.3	Padded Message (M)	195
7.4	Message in Little Endian Format	196
7.5	Initial Hash Values in Little Endian Format	197
7.6	Auxiliary Functions for Four MD5 Rounds	197
7.7	Four Operations Associated to Four MD5 Rounds	198
7.8	Round 1	199
7.9	Round 2	199
7.10	Round 3	200
7.11	Round 4	200
7.12	Final Transformation	201
7.13	Comparing Specifications for Four Hash Algorithms	201
7.14	Initial Hash Values for SHA-1	203
7.15	Initial Hash Values for SHA-256	203
7.16	Initial Hash Values for SHA-384	204
7.17	Initial Hash Values for SHA-512	205
7.18	SHA-256 Constants	207
7.19	SHA-384 & SHA-512 Constants	208
7.20	MD5 Hardware Implementations	214
7.21	Representative SHA-1 hardware Implementations	216
7.22	Representative RIPEMD-160 FPGA Implementations	217
7.23	Representative SHA-2 FPGA Implementations	218
7.24	Representative Whirlpool FPGA Implementations	219
8.1	Key Features for Some Famous Block Ciphers	227
8.2	Initial Permutation for 64-bit Input Block	235
8.3	E-bit Selection	235
8.4	DES S-boxes	236
8.5	Permutation P	237
8.6	Inverse Permutation	237
8.7	Permuted Choice one PC-1	238
8.8	Number of Key Bits Shifted per Round	238
8.9	Permuted Choice two (PC-2)	238
8.10	Test Vectors	240

8.11 DES Comparison: Fastest Designs	242
8.12 DES Comparison: Compact Designs	243
8.13 DES Comparison: Efficient Designs	243
8.14 TripleDES Designs	244
9.1 Selection of Rijndael Rounds	248
9.2 A Roadmap to Implemented AES Designs	273
9.3 Specifications of AES FPGA implementations	284
9.4 AES Comparison: High Performance Designs	286
9.5 AES Comparison: Compact Designs	287
9.6 AES Comparison: Efficient Designs	288
9.7 AES Comparison: Designs with Other Modes of Operation	288
10.1 $GF(2^m)$ Elliptic Curve Point Multiplication Computational Costs	302
10.2 Point addition in Hessian Form	305
10.3 Point doubling in Hessian Form	305
10.4 kP Computation, if Test-Bit is '1'	306
10.5 kP Computation, If Test-Bit is '0'	307
10.6 Design Implementation Summary	308
10.7 Parallel López-Dahab Point Doubling Algorithm	319
10.8 Parallel López-Dahab Point Addition Algorithm	319
10.9 Operations Supported by the ALU Module	323
10.10 Cycles per Operation	324
10.11 Fastest Elliptic Curve Scalar Multiplication Hardware Designs	326
10.12 Most Compact Elliptic Curve Scalar Multiplication Hardware Designs	326
10.13 Most Efficient Elliptic Curve Scalar Multiplication Hardware Designs	327

List of Algorithms

2.1	RSA Key Generation	17
2.2	RSA Digital Signature	17
2.3	RSA Signature Verification	18
2.4	DSA Domain Parameter Generation	19
2.5	DSA Key Generation	19
2.6	DSA Signature Generation	20
2.7	DSA Signature Verification	20
2.8	ECDSA Key Generation	21
2.9	ECDSA Digital Signature Generation	22
2.10	ECDSA Signature Verification	23
4.1	Euclidean Algorithm (Computes the Greatest Common Divisor)	65
4.2	Extended Euclidean Algorithm as Reported in [228]	69
4.3	Basic Doubling & Add algorithm for Scalar Multiplication	85
4.4	The Recoding Binary algorithm for Scalar Multiplication	86
4.5	ω -NAF Expansion Algorithm	87
5.1	The Standard Multiplication Algorithm	102
5.2	The Standard Squaring Algorithm	104
5.3	The Restoring Division Algorithm	106
5.4	The Nonrestoring Division Algorithm	108
5.5	The Interleaving Multiplication Algorithm	109
5.6	The Carry-Save Interleaving Multiplication Algorithm	110
5.7	The Carry-Save Interleaving Multiplication Algorithm Revisited	113
5.8	Montgomery Product	117
5.9	Montgomery Modular Multiplication: Version I	117
5.10	Montgomery Modular Multiplication: Version II	118
5.11	Specialized Modular Inverse	118
5.12	Montgomery Modular Exponentiation	120
5.13	Add-and-Shift Montgomery Product	122
5.14	Binary Add-and-Shift Montgomery Product	122
5.15	Word-Level Add-and-Shift Montgomery Product	124
5.16	MSB-First Binary Exponentiation	126

5.17	LSB-First Binary Exponentiation	127
5.18	MSB-First 2^k -ary Exponentiation	127
5.19	Sliding Window Exponentiation	131
6.1	$mul_{2^k}(C, A, B)$: $m = 2^k n$ -bit Karatsuba-Ofman Multiplier	144
6.2	$mul_{gen.d}(C, A, B)$: m -bit Binary Karatsuba-Ofman Multiplier	149
6.3	Constructing a Look-Up Table that Contains All the 2^k Possible Scalars in Equation (6.23)	157
6.4	Generating a Look-Up Table that Contains All the 2^k Possible Scalars Multiplications $S \cdot P$	158
6.5	Modular Reduction Using General Irreducible Polynomials	159
6.6	LSB-First Serial/Parallel Multiplier	161
6.7	Montgomery Modular Multiplication Algorithm	164
6.8	Binary Euclidean Algorithm	176
6.9	Itoh-Tsujii Multiplicative Inversion Addition-Chain Algorithm	179
6.10	Square Root Itoh-Tsujii Multiplicative Inversion Algorithm	181
6.11	MSB-first Binary Exponentiation	185
6.12	Square root LSB-first Binary Exponentiation	186
6.13	Squaring and Square Root Parallel Exponentiation	187
10.1	Doubling & Add algorithm for Scalar Multiplication: MSB-First	295
10.2	Doubling & Add algorithm for Scalar Multiplication: LSB-First	295
10.3	Montgomery Point Doubling	297
10.4	Montgomery Point Addition	298
10.5	Montgomery Point Multiplication	299
10.6	Standard Projective to Affine Coordinates	299
10.7	$\omega\tau$ NAF Expansion[133, 132]	312
10.8	$\omega\tau$ NAF Scalar Multiplication [133, 132]	313
10.9	$\omega\tau$ NAF Scalar Multiplication: Parallel Version	314
10.10	$\omega\tau$ NAF Scalar Multiplication: Hardware Version	314
10.11	$\omega\tau$ NAF Scalar Multiplication: Parallel HW Version	315
10.12	Point Halving Algorithm	320
10.13	Half-and-Add LSB-First Point Multiplication Algorithm	321