

1	About Cryptographic Engineering	1
	Çetin Kaya Koç	
1.1	Introduction	1
1.2	Chapter Contents	2
1.3	Exercises and Projects	4
2	Random Number Generators for Cryptographic Applications	5
	Werner Schindler	
2.1	Introduction	5
2.2	General Requirements	6
2.3	Classification	7
2.4	Deterministic Random Number Generators (DRNGs)	7
2.4.1	Pure DRNGs	8
2.4.2	Hybrid DRNGs	11
2.4.3	A Word of Warning	13
2.5	Physical True Random Number Generators (PTRNGs)	14
2.5.1	The Generic Design	14
2.5.2	Entropy and Guesswork	16
2.6	Non-physical True Random Number Generators (NPTRNGs): Basic Properties	18
2.7	Standards and Evaluation Guidances	20
2.8	Exercises	20
2.9	Projects	21
	References	21
3	Evaluation Criteria for Physical Random Number Generators	25
	Werner Schindler	
3.1	Introduction	25
3.2	Generic Design	26
3.3	Evaluation Criteria for the Principle Design	27
3.4	The Stochastic Model	29

3.5	Algorithmic Postprocessing	37
3.6	Online Test, Tot Test, and Self Test	41
3.6.1	Online Tests	42
3.7	Alternative Security Philosophies	49
3.8	Side-channel Attacks and Fault Attacks	50
3.9	Exercises	51
3.10	Projects	51
	References	52
4	True Random Number Generators for Cryptography	55
	Berk Sunar	
4.1	Introduction	55
4.2	TRNG Building Blocks	56
4.3	Desirable Features	57
4.4	Survey of TRNG Designs	57
4.4.1	Baggini and Bucci	58
4.4.2	The Intel TRNG Design	58
4.4.3	The Tkacik TRNG Design	59
4.4.4	The Epstein et al. TRNG Design	60
4.4.5	The Fischer–Drutarovský Design	61
4.4.6	The Golić FIGARO Design	62
4.4.7	The Kohlbrenner–Gaj Design	63
4.4.8	The Bucci–Luzzi Testable TRNG Design Framework ..	64
4.4.9	The Rings Design	65
4.4.10	The PUF–RNG Design	66
4.4.11	The Yoo et al. Design	67
4.4.12	The Dichtl and Golić RNG Design	67
4.5	Postprocessing Techniques	68
4.6	Exercises	70
	References	71
5	Fast Finite Field Multiplication	75
	Serdar Sürer Erdem, Tuğrul Yanık, and Çetin Kaya Koç	
5.1	Introduction	75
5.2	Finite Fields	76
5.3	Multiplication in Prime Fields	77
5.3.1	Integer Multiplication	78
5.3.2	Integer Squaring	80
5.3.3	Integer Modular Reduction	80
5.4	Multiplication in Binary Extension Fields	87
5.4.1	Polynomial Multiplication over $\mathbb{F}_2$	88
5.4.2	Polynomial Squaring over $\mathbb{F}_2$	90
5.4.3	Polynomial Modular Reduction over $\mathbb{F}_2$	90
5.5	Multiplication in General Extension Fields	96
5.5.1	Field Multiplication in OEF	97
5.5.2	Coefficient Multiplication and Reductions	98

5.6	Karatsuba–Ofman Algorithm	99
5.6.1	Complexity	100
5.6.2	Number of Scalar Multiplications	100
5.7	Exercises	102
5.8	Projects	103
	References	103
6	Efficient Unified Arithmetic for Hardware Cryptography	105
	Erkay Savaş and Çetin Kaya Koç	
6.1	Introduction	105
6.2	Fundamentals of Extension Fields	106
6.3	Addition and Subtraction	107
6.4	Multiplication	110
6.4.1	Montgomery Multiplication Algorithm	110
6.4.2	Dual-Radix Multiplier	116
6.4.3	Support for Ternary Extension Fields, $GF(3^n)$	118
6.5	Inversion	119
6.5.1	Montgomery Inversion for $GF(p)$ and $GF(2^n)$	119
6.6	Conclusions	122
6.7	Exercises	122
6.8	Projects	123
	References	123
7	Spectral Modular Arithmetic for Cryptography	125
	Gökay Saldamlı and Çetin Kaya Koç	
7.1	Introduction	125
7.2	Notation and Background	126
7.2.1	Evaluation Polynomials	126
7.2.2	Discrete Fourier Transform (DFT)	129
7.2.3	Properties of DFT: Time–frequency dictionary	131
7.3	Spectral Modular Arithmetic	135
7.3.1	Time Simulations and Spectral Algorithms	135
7.3.2	Modular Reduction	136
7.3.3	Spectral Modular Reduction	137
7.3.4	Time Simulation of Spectral Modular Reduction	139
7.3.5	Spectral Modular Reduction in a Finite Ring Spectrum ..	141
7.3.6	Spectral Modular Multiplication (SMM)	143
7.3.7	Spectral Modular Exponentiation	145
7.3.8	Illustrative Example	149
7.4	Applications to Cryptography	153
7.4.1	Mersenne and Fermat rings	154
7.4.2	Pseudo Number Transforms	155
7.4.3	Parameter Selection for RSA	156
7.4.4	Parameter Selection for ECC over Prime Fields	157
7.5	Spectral Extension Field Arithmetic	158
7.5.1	Binary Extension Fields	158

7.5.2	Midsize Characteristic Extension Fields	161
7.5.3	Parameter Selection for ECC over Extension Fields	164
7.6	Notes	165
7.7	Exercises	166
7.8	Projects	167
	References	168
8	Elliptic and Hyperelliptic Curve Cryptography	171
	Nigel Boston and Matthew Darnall	
8.1	Introduction	171
8.2	Diffie – Hellman Key Exchange	172
8.3	Introduction to Elliptic and Hyperelliptic Curves	172
8.4	The Jacobian of a Curve	173
8.4.1	The Principal Subgroup and $Jac(C)$	174
8.5	Computing on $Jac(C)$	174
8.6	Group Law for Elliptic Curves	176
8.7	Techniques for Computations in Hyperelliptic Curves	178
8.7.1	Explicit Formulae	178
8.7.2	Projective Coordinates	178
8.7.3	Other Optimization Techniques	179
8.8	Counting Points on $Jac(C)$	179
8.9	Attacks	181
8.9.1	Baby-Step Giant-Step Attack	181
8.9.2	Pollard Rho and Lambda Attacks	181
8.9.3	Pohlig–Hellman Attack	182
8.9.4	Menezes–Okamoto–Vanstone Attack	182
8.9.5	Semaev, Satoh–Araki, Smart Attack	183
8.9.6	Attacks employing Weil descent	183
8.10	Good Curves	184
8.11	Exercises	184
8.12	Projects	185
	References	185
9	Instruction Set Extensions for Cryptographic Applications	191
	Sandro Bartolini, Roberto Giorgi, and Enrico Martinelli	
9.1	Introduction	191
9.1.1	Instruction Set Architecture	191
9.2	Applications and Benchmarks	194
9.2.1	Benchmarks	195
9.2.2	Potential Performance	195
9.3	ISE for Cryptographic Applications	196
9.3.1	Instructions for Information Confusion and Diffusion	196
9.3.2	ISE for AES	203
9.3.3	ISE for ECC applications	212
9.4	Exercises	227
9.5	Projects	228
	References	229

10	FPGA and ASIC Implementations of AES	235
	Kris Gaj and Pawel Chodowiec	
10.1	Introduction	235
10.2	AES Cipher Description	236
10.2.1	Basic Features	236
10.2.2	Round Operations	237
10.2.3	Iterative Structure	242
10.2.4	Key Scheduling	243
10.3	FPGA and ASIC Technologies	247
10.4	Parameters of Hardware Implementations	250
10.4.1	Throughput and Latency	250
10.4.2	Area	250
10.5	Hardware Architectures of Symmetric Block Ciphers	251
10.5.1	Hardware Architectures vs. Block Cipher Modes of Operation	251
10.5.2	Basic Iterative Architecture	252
10.5.3	Loop Unrolling	253
10.5.4	Pipelining	254
10.5.5	Limits on the Maximum Clock Frequency of Pipelined Architectures	258
10.5.6	Compact Architectures with Resource Sharing	260
10.6	Implementation of Basic Operations of AES in Hardware	261
10.6.1	SubBytes and InvSubBytes	261
10.6.2	MixColumns and InvMixColumns	270
10.7	Hardware Architectures of a Single Round of AES	274
10.7.1	S-Box-Based Architecture	274
10.7.2	T-Box-Based Architecture	276
10.7.3	Compact Architectures	282
10.8	Implementation of Key Scheduling	286
10.9	Optimum Choice of a Hardware Architecture for AES	286
10.10	Exercises	289
10.11	Projects	290
	References	291
11	Secure and Efficient Implementation of Symmetric Encryption Schemes using FPGAs	295
	François-Xavier Standaert	
11.1	Introduction	295
11.2	Efficient FPGA Implementations	297
11.2.1	Exploiting the Slice Structure	297
11.2.2	Exploiting Embedded Blocks	300
11.2.3	Exploiting Further Features	302
11.2.4	Combining the Tricks: The Flexibility Versus Efficiency Tradeoff	303
11.3	Fair Evaluation of a Cryptographic FPGA Design	303

11.3.1	Design Goals	304
11.3.2	Performance Evaluation	304
11.4	Security of FPGAs Against Side-Channel Attacks	305
11.4.1	Applicability of the Attack and FPGA Properties	306
11.4.2	Countermeasures	310
11.4.3	Measuring Side-Channel Resistance	311
11.5	Other Security Issues	312
11.5.1	Fault Attacks	312
11.5.2	Bitstream Security	312
11.6	Conclusions and Open Questions	315
11.7	Exercises	315
11.8	Projects	317
	References	318
12	Block Cipher Modes of Operation from a Hardware Implementation Perspective	321
	Debrup Chakraborty and Francisco Rodríguez-Henríquez	
12.1	Introduction	321
12.2	Block Ciphers	326
12.3	Introduction to AES	327
12.3.1	Byte Substitution (BS) Step	328
12.3.2	Shift Rows (SR) Step	328
12.3.3	Mix Columns (MC) Step	328
12.3.4	Add Round Key (ARK) Step	329
12.3.5	Key Scheduling Algorithm	329
12.4	A Background in Binary Extension Finite Fields	330
12.4.1	Rings	330
12.4.2	Fields	331
12.4.3	Finite Fields	331
12.4.4	Binary Finite Field Arithmetic	331
12.5	Traditional Modes of Operations	332
12.5.1	Electronic Code Book Mode	333
12.5.2	Cipher Block Chaining Mode	333
12.5.3	Cipher Feedback Mode	334
12.5.4	Output Feedback Mode	334
12.5.5	Counter Mode	335
12.6	Security Requirements for Modes of Operations	336
12.6.1	The Adversary	336
12.6.2	Privacy Only Modes	337
12.6.3	Authenticated Encryption	338
12.6.4	Disk Encryption Schemes	339
12.6.5	Security Proofs	341
12.7	Some Modern Modes	341
12.7.1	The Offset Codebook Mode	343
12.7.2	ECB-Mask-ECB Mode	344

12.8	The CCM Mode: A Case Study	347
12.8.1	The CCM Mode	347
12.8.2	AES Encryptor Core Implementation	350
12.8.3	Hardware Implementation of the CCM Mode	353
12.8.4	Experimental Results and Comparison	357
12.9	Conclusions	358
12.10	Exercises	359
12.11	Projects	360
	References	365
13	Basics of Side-Channel Analysis	365
	Marc Joye	
13.1	Introduction	365
13.2	Timing Analysis	366
13.2.1	Attack on a Password Verification	367
13.2.2	Attack on an RSA Signature Scheme	368
13.3	Simple Power Analysis	369
13.3.1	Reverse-Engineering of an Algorithm	370
13.3.2	Attack on a Private RSA Exponentiation	371
13.3.3	Attack on a DES Key Schedule	373
13.4	Differential Power Analysis	373
13.4.1	Bit Tracing	374
13.4.2	Attack on an AES Implementation	376
13.4.3	Attack on an RSA Signature Scheme (2)	376
13.5	Countermeasures	377
13.6	Exercises	378
13.7	Projects	379
	References	381
14	Improved Techniques for Side-Channel Analysis	381
	Pankaj Rohatgi	
14.1	Introduction	381
14.2	CMOS Devices: Side-Channel Leakage Perspective	382
14.2.1	Intentional Current Flows	382
14.2.2	Leakage Current Flows	383
14.2.3	Information Leakage in Power and EM Side-Channels	383
14.3	Characterizing Side-Channel Leakage Using Maximum Likelihood	385
14.3.1	Adversarial Model	385
14.3.2	Maximum Likelihood and Best Attack Strategy	385
14.3.3	Gaussian Assumption	386
14.4	Template Attacks	387
14.4.1	Classical Template Attacks: The Case of RC4	389
14.4.2	Single-Bit Templates and Applications	393
14.5	Improved DPA/DEMA Metric	395
14.5.1	Improving DPA	395

14.6	Multi-Channel Attacks	397
14.6.1	Multiple Channel Selection	397
14.6.2	Multi-Channel Template Attacks	399
14.6.3	Multi-Channel DPA	400
14.7	Toward Information Leakage Assessment	401
14.7.1	Practical Considerations	402
14.8	Projects	403
	References	405
15	Electromagnetic Attacks and Countermeasures	407
	Pankaj Rohatgi	
15.1	Introduction and History	407
15.2	EM Emanations Background	409
15.2.1	Types of EM Emanations	409
15.2.2	EM Propagation	410
15.3	EM Capturing Equipment	413
15.4	EM Leakage Examples	415
15.4.1	Examples: Amplitude Modulation	415
15.4.2	Examples: Angle Modulation	422
15.5	Multiplicity of EM Channels and Comparison with Power Channel	424
15.6	Using EM to Bypass Power Analysis Countermeasures	427
15.7	Quantifying EM Exposure	427
15.8	Countermeasures	428
15.9	Projects	429
	References	430
16	Leakage from Montgomery Multiplication	431
	Colin D. Walter	
16.1	Introduction	431
16.2	Montgomery Reduction	431
16.3	Montgomery Modular Multiplication	433
16.4	Exponentiation	435
16.5	Space and Time Comparisons	437
16.6	Side Channel Analysis	438
16.7	Frequencies of Conditional Subtractions	440
16.8	Variance in Frequencies and SCA Errors	442
16.9	A Surprising Improvement	443
16.10	Conclusions	445
16.11	Exercises	445
16.12	Projects	446
	References	448
17	Randomized Exponentiation Algorithms	451
	Colin D. Walter	
17.1	Introduction	451

17.2	The Big Mac Attack	452
17.3	Digit Representation and Exponentiation Algorithms	454
17.4	Liardet-Smart	457
17.4.1	Attacking the Algorithm	459
17.5	Oswald-Aigner Exponentiation	460
17.5.1	Attacking the Algorithm	461
17.6	Ha-Moon	462
17.6.1	Attacking the Algorithm	463
17.7	Itoh's Overlapping Windows	464
17.7.1	Attacking the Algorithm	465
17.8	Randomized Table Method	466
17.8.1	Attacking the Algorithm	466
17.9	The MIST Algorithm	467
17.9.1	Attacking the Algorithm	468
17.10	Conclusions	469
17.11	Exercises	469
17.12	Projects	470
	References	472
18	Microarchitectural Attacks and Countermeasures	475
	Onur Aciğmez and Çetin Kaya Koç	
18.1	Introduction	475
18.2	Overview and Brief History	476
18.3	Cache Analysis	478
18.3.1	Basics of Cache	478
18.3.2	Overview of Cache Attacks	480
18.3.3	A Brief Survey on Cache Analysis	481
18.3.4	Time-Driven and Trace-Driven Attacks	482
18.3.5	Exploiting Internal Collisions in Time-Driven Attacks	483
18.3.6	Access-Driven Attacks	485
18.3.7	Percival's Hyper-Threading Attack on RSA	489
18.4	Branch Prediction Analysis	490
18.4.1	The Concept of Branch Prediction	490
18.4.2	Simple Branch Prediction Analysis	492
18.5	I-cache Analysis	494
18.6	Exploiting Shared Functional Units	496
18.7	Comparing Microarchitectural Analysis Types	497
18.8	Countermeasures for Microarchitectural Analysis	498
18.9	Exercises	499
18.10	Projects	500
	References	501

Authors' Biographies	505
-----------------------------	-----

Index	513
--------------	-----