
Contents

Preface	xvii
List of Figures	xxi
List of Tables	xxv
I Fundamentals of Cryptography	1
1 Introduction to Cryptography	3
1.1 History of Cryptography	3
1.1.1 Classical Cryptography	4
1.1.2 Modern Cryptography	7
1.2 Background Review	9
1.2.1 Big Oh Notation	9
1.2.2 Polynomial	9
1.2.3 Super Polynomial	10
1.2.4 Negligible	10
Exercises	11
2 Structure of Security Proof	13
2.1 Overview of Security Proof	14
2.1.1 Why Proving Security?	14
2.1.2 Security Goals	14
2.1.3 Attack Models	16
2.1.4 How Can We Build a Cryptographic Scheme? Lego Approach!	17
2.1.5 Computational Assumptions	17
2.2 Proof by Reduction	18
2.2.1 What Is Reduction?	19
2.2.2 Outline of Security Proof by Reduction	19
2.3 Random Oracle Methodology	20
2.3.1 Security Proof in the Random Oracle Model	21
2.4 Sequence of Games	22
2.4.1 Hybrid Argument	24
2.5 The Generic Group Model	25
Exercise	26

3	Private-Key Encryption (1)	27
3.1	Defining Computationally-Secure Encryption	27
3.2	Pseudorandomness	29
3.3	A Private-Key Encryption Scheme Based on Pseudorandom Generator	30
	Exercises	33
4	Private-Key Encryption (2)	35
4.1	Stream Ciphers	35
4.2	Stronger Security Notions	36
4.2.1	Security for Multiple Encryptions	36
4.2.2	Security for Chosen-Plaintext Attack	38
4.3	Constructing CPA-Secure Encryption Scheme	42
4.4	Advanced Encryption Standard	47
	Exercises	49
5	Private-Key Encryption (3)	51
5.1	Block Ciphers and Modes of Operation	51
5.1.1	Electronic Code Book (ECB) Mode	52
5.1.2	Cipher Block Chaining (CBC) Mode	52
5.1.3	Counter (CTR) Mode	54
5.2	CPA-Securities of Modes of Operation	55
5.2.1	IND-CPA Adversary	55
5.2.2	A Block Cipher <i>Per Se</i> Is Not IND-CPA Secure	56
5.2.3	ECB Is Not IND-CPA Secure	56
5.2.4	CBC Is IND-CPA Secure	57
5.2.5	CTR Is IND-CPA Secure	57
5.3	Security Against Chosen-Ciphertext Attack (CCA)	59
5.3.1	IND-CCA Adversary	61
5.3.2	A CPA-Secure Encryption Scheme from Any Pseudo- random Function Is Not CCA-Secure	62
5.3.3	A CPA-Secure Encryption Scheme Using CBC Mode (Random Version) Is Not CCA-Secure	62
	Exercises	64
6	Message Authentication Code	65
6.1	Overview	65
6.1.1	Encryption vs. Message Authentication	66
6.2	Message Authentication Code	67
6.3	Constructing Secure Message Authentication Code	70
6.3.1	Fixed-Length MAC	70
6.3.2	Variable-Length MAC	72
6.4	CBC-MAC	75
6.5	Obtaining Encryption and Message Authentication	77

6.5.1	Constructing CCA-Secure Encryption Schemes Using MAC	79
-------	--	----

7 Hash Function 87

7.1	Definitions	88
7.1.1	Collision Resistance	88
7.1.2	Weaker Notions of Security	89
7.2	Design of Collision-Resistant Hash Functions	90
7.2.1	Compression Function Proved Secure Under the Discrete Log Assumption	90
7.2.2	Compression Functions Based on Secure Block Ciphers	92
7.2.3	Proprietary Compression Functions	92
7.3	The Merkle-Damgard Transform	93
7.4	Generic Attacks on Hash Functions	95
7.4.1	Birthday Attacks for Finding Collisions	95
7.4.2	Small-Space Birthday Attacks	96
7.5	Message Authentication Using Hash Functions	96
7.5.1	Hash-and-MAC	96
7.5.2	HMAC	97
7.6	Applications of Hash Function	98
7.6.1	Fingerprinting and Deduplication	99
7.6.2	Merkle Trees	99
7.6.3	Password Hashing	101
7.6.4	Key Derivation	101
7.6.5	Commitment Schemes	102
	Exercises	102

8 Introduction to Number Theory 103

8.1	Preliminaries	103
8.1.1	Division, Prime, and Modulo	104
8.1.2	Greatest Common Divisor	105
8.1.3	Euclidean Algorithm	105
8.1.4	Extended Euclidean Algorithm	105
8.1.5	Fermat's Little Theorem	105
8.1.6	Euler's Theorem	106
8.1.7	Exponentiation and Logarithm	106
8.1.8	Set of Residues $\mathbb{Z}_n$	107
8.1.9	Inverse Modulo	108
8.1.10	Euler's Criterion	110
8.2	Algebraic Structure	110
8.2.1	Group	110
8.2.2	Ring	112
8.2.3	Field	112
8.2.4	$\mathbb{GF}(2^n)$	113
8.2.5	Elliptic Curve	114

9	Public-Key Encryption	117
9.1	Discrete Logarithm and Its Related Assumptions	118
9.2	The Diffie-Hellman Key Exchange Protocol	120
9.3	Overview of Public-Key Encryption	123
9.3.1	Security Against CPA	124
9.3.2	Security Against CCA	127
9.3.3	Hybrid Encryption and the KEM/DEM Paradigm	128
9.4	Public-Key Encryption Schemes	129
9.4.1	The El Gamal Encryption	129
9.4.2	The Plain (<i>aka</i> Textbook) RSA Encryption	133
9.4.2.1	RSA Cryptosystem Based on Elliptic Curve	135
9.4.3	The Padded RSA Encryption	136
9.4.4	The CPA-Secure RSA Encryption Under the RSA Assumption in the Random Oracle Model	137
9.4.5	The CCA-Secure RSA Encryption Under the RSA Assumption in the Random Oracle Model	140
9.4.6	The RSA-OAEP Encryption	144
9.4.7	The Cramer-Shoup Encryption	145
9.4.8	The Paillier Encryption	155
	Exercises	157
10	Digital Signature	159
10.1	Overview	160
10.2	Definitions	160
10.3	The El Gamal Signatures	162
10.4	The RSA Signatures	168
10.4.1	Plain RSA	169
10.4.2	Full Domain Hash RSA	169
10.4.3	Probabilistic Signature Scheme (PSS)	171
10.5	Blockchain: Application of Hash Function and Public-Key Encryption	171
10.5.1	Blockchain 1.0: Early Development of Blockchain Technology	171
10.5.1.1	The Use of Cryptography in Blockchain	174
10.5.1.2	Other Consensus Algorithms	175
10.5.2	Blockchain 2.0: Smart Contract Beyond Cryptocurrency	176
10.5.3	Private, Consortium, and Public Blockchain	176
	Exercises	177
II	Identity-Based Encryption and Its Variants	179
11	Identity-Based Encryption (1)	181
11.1	Overview	181
11.2	Preliminaries	183
11.2.1	Bilinear Map (Weil and Tate Pairing)	183

11.2.2	Hardness Assumption	184
11.3	Identity-Based Encryption	184
11.4	Boneh-Franklin IBE [24]	185
12	Identity-Based Encryption (2)	199
12.1	Overview	199
12.2	Preliminaries	201
12.2.1	Security Model	201
12.2.2	Hardness Assumptions	202
12.2.3	How to Achieve a Tight Reduction?	204
12.3	Gentry’s IBE [48]	206
12.3.1	Construction 1: Chosen-Plaintext Security	206
12.3.2	Security 1: Chosen-Plaintext Security	208
12.3.3	Construction 2. Chosen-Ciphertext Security	213
12.3.4	Security 2: Chosen-Ciphertext Security	215
	Exercises	225
13	Identity-Based Encryption (3)	227
13.1	Overview	227
13.2	Preliminaries	229
13.2.1	Security Model	230
13.2.2	Hardness Assumptions	230
13.3	Dual System Encryption	231
13.4	Waters’ IBE [99]	235
13.4.1	Proof of IBE Security	240
	Exercises	256
14	Hierarchical Identity-Based Encryption	257
14.1	Overview	258
14.2	Preliminaries	259
14.2.1	General Construction of HIBE	259
14.2.2	Security Model for HIBE	260
14.2.3	Composite Order Bilinear Groups	261
14.2.4	Hardness Assumptions	262
14.2.5	A “Master Theorem” for Hardness in Composite Order Bilinear Groups [60]	263
14.3	Waters’ Realization	268
14.4	Waters’ HIBE with Composite Order	269
14.4.1	Proof of HIBE Security	274
14.5	The Generic Group Model	284
14.5.1	The Decision Linear Diffie-Hellman Assumption	284
14.5.2	The Linear Problem in Generic Bilinear Groups	285
	Exercises	288

15 Identity-Based Encryption (4)	289
15.1 Overview	289
15.2 Preliminaries	291
15.2.1 Security Model	291
15.2.2 Hardness Assumption	293
15.3 Boneh-Boyen IBE [19]	293
15.3.1 Proof of IBE Security	295
16 Tight Reduction	299
16.1 Overview	300
16.2 Why Is Tight Reduction Important?	300
16.3 Obstacles and Solutions in Tight Reduction	301
16.3.1 All-and-Any Strategy	301
16.3.1.1 Relationship Between Security Models and Strategies	302
16.3.2 Searching Method	303
16.3.3 Self-Decryption Paradox	304
16.4 All-and-Any Strategy Techniques in the Random Oracle Model	304
16.4.1 Katz-Wang Technique	305
16.4.2 Park-Lee Technique	306
Exercises	307
17 Transformation Technique	309
17.1 Canetti-Halevi-Katz Transformation [32]	309
17.1.1 Definitions	310
17.1.1.1 Binary Tree Encryption	310
17.1.1.2 One-Time Signature	312
17.1.2 Chosen-Ciphertext Security from IBE	312
17.1.3 Chosen-Ciphertext Security for BTE Schemes	316
18 Broadcast Encryption	321
18.1 Introduction	322
18.2 Subset-Cover Revocation Framework [78]	323
18.2.1 Problem Definition	323
18.2.2 The Framework	323
18.2.3 Two Subset-Cover Algorithms	325
18.2.3.1 Complete Subtree (CS) Method	327
18.2.3.2 Subset Difference (SD) Method	330
18.3 Identity-Based Broadcast Encryption	337
18.3.1 Preliminaries	337
18.3.1.1 Definition	337
18.3.1.2 Security Model	338
18.3.1.3 Hardness Assumptions	339
18.3.2 Delerablée's Scheme [37]	341
18.3.3 Security Analysis of Delerablée's Scheme	342

Exercises	347
19 Attribute-Based Encryption	349
19.1 Overview	350
19.2 Access Structure	351
19.2.1 Secret Sharing Scheme	351
19.2.2 Access Trees	351
19.2.3 Satisfying the Access Tree	352
19.3 Preliminaries	354
19.3.1 The Generic Bilinear Group Model	354
19.3.2 The Decisional Bilinear Diffie-Hellman (DBDH) Assumption	355
19.3.3 Selective-Set Model for KP-ABE	355
19.3.4 Security Model for CP-ABE	355
19.4 KP-ABE [55]	356
19.4.1 Security Analysis of KP-ABE	359
19.4.2 Probability Analysis	362
19.5 CP-ABE [14]	362
20 Secret Sharing	371
20.1 Overview	371
20.2 Efficient Secret Sharing	372
20.2.1 Shamir's Secret Sharing [90]	372
20.2.1.1 Mathematical Definition	373
20.2.1.2 The Construction	373
20.2.1.3 Example	373
20.2.2 Blakley's Secret Sharing [16]	375
20.2.2.1 The Construction	375
20.2.2.2 Example	376
Exercise	377
21 Predicate Encryption and Functional Encryption	379
21.1 Overview	380
21.1.1 Predicate Encryption	380
21.1.2 Functional Encryption	381
21.2 Preliminaries	383
21.2.1 Hardness Assumptions	383
21.2.2 Definition of Predicate Encryption	385
21.2.3 Definition of Functional Encryption	387
21.3 Predicate-Only Encryption [62]	388
21.3.1 Proof of Predicate-Only Encryption Security	390
21.4 Predicate Encryption [62]	397
21.4.1 Proof of Predicate Encryption Security	399
21.5 Functional Encryption	404
21.5.1 Proof of Functional Encryption Security	405

21.5.2 Applications of Functional Encryption	409
21.5.2.1 Distance Measurement	409
21.5.2.2 Exact Threshold	410
21.5.2.3 Weighted Average	410
III Post-Quantum Cryptography	411
22 Introduction to Lattice	413
22.1 Preliminaries	413
22.2 Lattice Problems	414
22.3 NTRU Cryptosystem	415
Exercises	417
23 Lattice-Based Cryptography	419
23.1 Overview	419
23.2 Preliminaries	420
23.2.1 Distributions	421
23.3 Lattice-Based Cryptography	421
23.3.1 Learning with Errors (LWE)	422
23.3.2 Learning with Rounding (LWR)	424
23.3.3 Ring Variants of LWE and LWR	425
23.4 (LWE+LWR)-Based Public-Key Encryption [34]	425
23.4.1 The Construction	426
23.4.2 Correctness	427
23.4.3 Security	427
23.5 Ring Variant of Lizard	428
23.5.1 The Construction	430
24 Introduction to Linear Codes	433
24.1 Fundamentals of Coding Theory	434
24.2 Basics of Linear Codes	434
24.2.1 Generator Matrix and Parity-Check Matrix	435
24.3 Types of Decoding	439
24.3.1 Maximum-Likelihood Decoding	439
24.3.2 Minimum-Distance Decoding	439
24.3.3 Syndrome Decoding	440
24.4 Hamming Geometry and Code Performance	440
24.5 Types of Codes	441
24.5.1 Hamming Code	441
24.5.2 Cyclic Codes	442
24.5.3 Generalized Reed-Solomon (GRS) Codes	442
24.5.4 Goppa Codes	443
24.5.4.1 Construction of Goppa Codes	443
24.5.4.2 Binary Goppa Codes	443
24.5.4.3 Parity-Check Matrix of Goppa Codes	444
24.6 Hard Problems	445

Exercises	445
25 Code-Based Cryptography	449
25.1 McEliece Cryptosystem [75]	450
25.1.1 Key Generation	450
25.1.2 Encryption	451
25.1.3 Decryption	451
25.2 Niederreiter Cryptosystem	452
25.2.1 Key Generation	452
25.2.2 Encryption	453
25.2.3 Decryption	453
25.3 Security Analysis of McEliece and Niederreiter	454
25.4 QC-MDPC McEliece Cryptosystem	454
25.4.1 MDPC and QC-MDPC Codes	455
25.4.1.1 MDPC Code	455
25.4.1.2 MDPC Code Construction	456
25.4.1.3 QC-MDPC Code Construction	456
25.4.2 QC-MDPC McEliece Cryptosystem [101]	456
25.4.2.1 Key Generation	456
25.4.2.2 Encryption	457
25.4.2.3 Decryption	457
Exercises	458
IV Implementations of Selected Algorithms	461
26 Selected Algorithms	463
26.1 Introduction	463
26.2 Boneh-Franklin IBE	464
26.3 Boneh-Boyen IBE	464
26.4 Broadcast Encryption	464
26.5 Ciphertext-Policy Attribute-Based Encryption (CP-ABE) . .	465
26.6 Predicate Encryption (PE)	465
26.7 Rivest-Shamir-Adleman (RSA)	466
26.8 Elliptic Curve Digital Signature Algorithm (ECDSA)	466
26.9 QC-MDPC McEliece	466
26.10 NTRUEncrypt	467
26.11 Number Theoretic Transform	467
26.12 The Paillier Encryption	468
26.13 AES Block Cipher	468
26.14 wolfSSL	469
Bibliography	471
Index	481