

Contents

Part I Setting the Stage

1	Digital Signatures: Background and Definitions	3
1.1	Digital Signature Schemes: A Quick Introduction	3
1.1.1	Properties of Digital Signatures	4
1.2	Computational Security	6
1.2.1	Computational Notions of Security	7
1.2.2	Notation	8
1.3	Defining Signature Schemes	9
1.4	Motivating the Definitions of Security	11
1.5	Formal Definitions of Security	14
1.5.1	Security against Random-Message Attacks	14
1.5.2	Security against Known-Message Attacks	15
1.5.3	Security against Adaptive Chosen-Message Attacks	16
1.6	Relations Between the Notions	18
1.7	Achieving CMA-Security from Weaker Primitives	19
1.7.1	CMA-Security from RMA-security	19
1.7.2	CMA-Security from KMA-Security	23
1.8	From Unforgeability to Strong Unforgeability	27
1.9	Extending the Message Length	30
1.10	Further Reading	32
2	Cryptographic Hardness Assumptions	35
2.1	“Generic” Cryptographic Assumptions	35
2.1.1	One-Way Functions and Permutations	36
2.1.2	Trapdoor Permutations	39
2.1.3	Clawfree (Trapdoor) Permutations	41
2.2	Specific Assumptions	43
2.2.1	Hardness of Factoring	44
2.2.2	The RSA Assumption	50
2.2.3	The Discrete Logarithm Assumption	52

2.3	Hash Functions	53
2.3.1	Definitions	53
2.3.2	The Merkle-Damgård Transform	54
2.3.3	Constructing Collision-Resistant Hash Functions	56
2.3.4	Constructing Universal One-Way Hash Functions	58
2.4	Applications of Hash Functions to Signature Schemes	61
2.4.1	Increasing the Message Length	61
2.4.2	Reducing the Public-Key Length	64
2.5	Further Reading	66

Part II Digital Signature Schemes without Random Oracles

3	Constructions Based on General Assumptions	69
3.1	Lamport's One-Time Signature Scheme	70
3.2	Signatures from One-Time Signatures	74
3.2.1	“Chain-Based” Signatures	75
3.2.2	“Tree-Based” Signatures	77
3.2.3	A Stateless Solution	82
3.3	Signatures from One-Way Functions	83
3.3.1	Putting the Pieces Together	83
3.3.2	Thoughts on the Construction	83
3.4	Further Reading	84
4	Signature Schemes Based on the (Strong) RSA Assumption	87
4.1	Introduction	87
4.1.1	Technical Preliminaries	87
4.1.2	Outline of the Chapter	90
4.2	Signature Schemes Based on the RSA Assumption	90
4.2.1	The Dwork-Naor Scheme	91
4.2.2	The Cramer-Damgård Scheme	97
4.2.3	The Hohenberger-Waters Scheme	106
4.3	Schemes Based on the Strong RSA Assumption	108
4.3.1	The Strong RSA Assumption	109
4.3.2	Security Against Known-Message Attacks	109
4.3.3	The Cramer-Shoup Scheme	112
4.3.4	The Fischlin Scheme	114
4.3.5	The Gennaro-Halevi-Rabin Scheme	117
4.4	Further Reading	118
5	Constructions Based on Bilinear Maps	121
5.1	Introduction	121
5.1.1	Technical Preliminaries	121
5.1.2	Outline of the Chapter	122
5.2	The Boneh-Boyen Scheme	123
5.3	The Waters Scheme	127
5.4	Further Reading	131

Part III Digital Signature Schemes in the Random Oracle Model

6	The Random Oracle Model	135
6.1	Security Proofs in the Random Oracle Model	137
6.2	Is the Random Oracle Methodology Sound?	138
6.2.1	Negative Results	140
6.3	The Random Oracle Model in Practice	141
6.4	Further Reading	142
7	Full-Domain Hash (and Related) Signature Schemes	143
7.1	The Full-Domain Hash (FDH) Signature Scheme	143
7.1.1	An Instantiation Using Bilinear Maps	145
7.2	An Improved Security Reduction for FDH	147
7.3	Probabilistic FDH	149
7.4	A Simpler Variant with a Tight Reduction	151
7.5	Further Reading	152
8	Signature Schemes from Identification Schemes	155
8.1	Identification Schemes	156
8.2	From Identification Schemes to Signatures	159
8.2.1	The Fiat-Shamir Transform	159
8.2.2	Two Useful Criteria	163
8.2.3	One-Time Signature Schemes without Random Oracles	169
8.3	Some Secure Identification Schemes	171
8.3.1	The Fiat-Shamir Scheme	172
8.3.2	The Guillou-Quisquater Scheme	176
8.3.3	The Micali/Ong-Schnorr Scheme	178
8.3.4	The Schnorr Scheme	180
8.4	Further Reading	182
	References	185
	Index	191



<http://www.springer.com/978-0-387-27711-0>

Digital Signatures

Katz, J.

2010, XIII, 192 p., Hardcover

ISBN: 978-0-387-27711-0