

Contents

<i>List of Contributors</i>	<i>page</i> x
<i>Preface</i>	xi
1 Introduction <i>Joppe W. Bos and Martijn Stam</i>	1
1.1 Biographical Sketch	1
1.2 Outline	9
 Part I Cryptanalysis	
2 Lattice Attacks on NTRU and LWE:	
A History of Refinements <i>Martin R. Albrecht and Léoucas</i>	15
2.1 Introduction	15
2.2 Notation and Preliminaries	17
2.3 Lattice Reduction: Theory	18
2.4 Practical Behaviour on Random Lattices	20
2.5 Behaviour on LWE Instances	29
2.6 Behaviour on NTRU Instances	34
3 History of Integer Factorisation <i>Samuel S. Wagstaff, Jr</i>	41
3.1 The Dark Ages: Before RSA	41
3.2 The Enlightenment: RSA	47
3.3 The Renaissance: Continued Fractions	50
3.4 The Reformation: A Quadratic Sieve	55
3.5 The Revolution: A Number Field Sieve	58
3.6 An Exquisite Diversion: Elliptic Curves	62
3.7 The Future: How Hard Can Factoring Be?	67

4	Lattice-Based Integer Factorisation:		
	An Introduction to Coppersmith's Method	<i>Alexander May</i>	78
4.1	Introduction to Coppersmith's Method		79
4.2	Useful Coppersmith-Type Theorems		80
4.3	Applications in the Univariate Case		85
4.4	Multivariate Applications: Small Secret Exponent RSA		95
4.5	Open Problems and Further Directions		100
5	Computing Discrete Logarithms	<i>Robert Granger and Antoine Joux</i>	106
5.1	Introduction		106
5.2	Elliptic Curves		110
5.3	Some Group Descriptions with Easier Discrete Logarithms		118
5.4	Discrete Logarithms for XTR and Algebraic Tori		122
5.5	Discrete Logarithms in Finite Fields of Fixed Characteristic		130
5.6	Conclusion		139
6	RSA, DH and DSA in the Wild	<i>Nadia Heninger</i>	140
6.1	Introduction		140
6.2	RSA		141
6.3	Diffie–Hellman		154
6.4	Elliptic-Curve Diffie–Hellman		170
6.5	(EC)DSA		174
6.6	Conclusion		181
7	A Survey of Chosen-Prefix Collision Attacks	<i>Marc Stevens</i>	182
7.1	Cryptographic Hash Functions		182
7.2	Chosen-Prefix Collisions		186
7.3	Chosen-Prefix Collision Abuse Scenarios		190
7.4	MD5 Collision Attacks		212
Part II Implementations			
8	Efficient Modular Arithmetic	<i>Joppe W. Bos, Thorsten Kleinjung and Dan Page</i>	223
8.1	Montgomery Multiplication		224
8.2	Arithmetic for RSA		225
8.3	Arithmetic for ECC		237
8.4	Special Arithmetic		243

Contents

ix

9	Arithmetic Software Libraries	Victor Shoup	251
9.1	Introduction		251
9.2	Long-Integer Arithmetic		254
9.3	Number-Theoretic Transforms		259
9.4	Arithmetic in $\mathbb{Z}_p[X]$ for Multi-Precision p		270
9.5	Arithmetic in $\mathbb{Z}_p[X]$ for Single-Precision p		282
9.6	Matrix Arithmetic over \mathbb{Z}_p		286
9.7	Polynomial and Matrix Arithmetic over Other Finite Rings		289
9.8	Polynomial and Matrix Arithmetic over \mathbb{Z}		289
9.9	The Future of NTL		291
10	XTR and Tori	Martijn Stam	293
10.1	The Birth of XTR		293
10.2	The Magic of XTR		297
10.3	The Conservative Use of Tori		304
10.4	Pairings with Elliptic Curves		308
10.5	Over the Edge: Cyclotomic Subgroups Recycled		311
11	History of Cryptographic Key Sizes	Nigel P. Smart and Emmanuel Thomé	314
11.1	Introduction		314
11.2	Attacking Symmetric Algorithms with Software and Hardware		315
11.3	Software Attacks on Factoring and Discrete Logarithms		318
11.4	Hardware for Factoring		323
11.5	Attacking Cryptosystems Based on Elliptic Curves		325
11.6	Post-Quantum Cryptography		329
11.7	Key-Size Recommendation		332
	<i>References</i>		335
	<i>Index</i>		383