

Contents

Preface	xi
Introduction	xiii
I Background on Groups, Complexity, and Cryptography	1
1 Background on Public Key Cryptography	3
1.1 From key establishment to encryption	4
1.2 The Diffie-Hellman key establishment	5
1.3 The ElGamal cryptosystem	6
1.4 Authentication	7
2 Background on Combinatorial Group Theory	9
2.1 Basic definitions and notation	9
2.2 Presentations of groups by generators and relators	11
2.3 Algorithmic problems of group theory	11
2.3.1 The word problem	11
2.3.2 The conjugacy problem	12
2.3.3 The decomposition and factorization problems	12
2.3.4 The membership problem	13
2.3.5 The isomorphism problem	14
2.4 Nielsen's and Schreier's methods	14
2.5 Tietze's method	16
2.6 Normal forms	17
3 Background on Computational Complexity	19
3.1 Algorithms	19
3.1.1 Deterministic Turing machines	19
3.1.2 Non-deterministic Turing machines	20
3.1.3 Probabilistic Turing machines	21
3.2 Computational problems	21
3.2.1 Decision and search computational problems	21

3.2.2	Size functions	23
3.2.3	Stratification	25
3.2.4	Reductions and complete problems	26
3.2.5	Many-one reductions	27
3.2.6	Turing reductions	27
3.3	The worst case complexity	28
3.3.1	Complexity classes	28
3.3.2	Class NP	29
3.3.3	Polynomial-time many-one reductions and class NP	30
3.3.4	NP -complete problems	31
3.3.5	Deficiency of the worst case complexity	33
II Non-commutative Cryptography		35
4	Canonical Non-commutative Cryptography	37
4.1	Protocols based on the conjugacy search problem	37
4.2	Protocols based on the decomposition problem	39
4.2.1	“Twisted” protocol	40
4.2.2	Hiding one of the subgroups	41
4.2.3	Using the triple decomposition problem	42
4.3	A protocol based on the factorization search problem	43
4.4	Stickel’s key exchange protocol	43
4.4.1	Linear algebra attack	45
4.5	The Anshel-Anshel-Goldfeld protocol	47
4.6	Authentication protocols based on the conjugacy problem	49
4.6.1	A Diffie-Hellman-like scheme	49
4.6.2	A Fiat-Shamir-like scheme	50
4.6.3	An authentication scheme based on the twisted conjugacy problem	51
4.7	Relations between different problems	52
5	Platform Groups	55
5.1	Braid groups	55
5.1.1	A group of braids and its presentation	56
5.1.2	Dehornoy handle free form	59
5.1.3	Garside normal form	60
5.2	Thompson’s group	61
5.3	Groups of matrices	65
5.4	Small cancellation groups	67
5.4.1	Dehn’s algorithm	67
5.5	Solvable groups	68
5.5.1	Normal forms in free metabelian groups	68
5.6	Artin groups	71

<i>Contents</i>	ix
5.7 Grigorchuk's group	72
6 Using Decision Problems in Public Key Cryptography	77
6.1 The Shpilrain-Zapata scheme	78
6.1.1 The protocol	78
6.1.2 Pool of group presentations	81
6.1.3 Tietze transformations: elementary isomorphisms	82
6.1.4 Generating random elements in finitely presented groups	84
6.1.5 Isomorphism attack	87
6.1.6 Quotient attack	88
6.2 Public key encryption and encryption emulation attacks	89
III Generic Complexity and Cryptanalysis	95
7 Distributional Problems and the Average Case Complexity	99
7.1 Distributional computational problems	99
7.1.1 Distributions and computational problems	99
7.1.2 Stratified problems with ensembles of distributions	101
7.1.3 Randomized many-one reductions	102
7.2 Average case complexity	103
7.2.1 Polynomial on average functions	103
7.2.2 Average case behavior of functions	109
7.2.3 Average case complexity of algorithms	109
7.2.4 Average case vs worst case	110
7.2.5 Average case behavior as a trade-off	111
7.2.6 Deficiency of average case complexity	114
8 Generic Case Complexity	117
8.1 Generic Complexity	117
8.1.1 Generic sets	117
8.1.2 Asymptotic density	118
8.1.3 Convergence rates	120
8.1.4 Generic complexity of algorithms and algorithmic problems	121
8.1.5 Deficiency of the generic complexity	122
8.2 Generic- versus average case complexity	123
8.2.1 Comparing generic and average case complexities	123
8.2.2 When average polynomial time implies generic polynomial time	124
8.2.3 When generically easy implies easy on average	125

9	Generic Complexity of NP-complete Problems	129
9.1	The linear generic time complexity of subset sum problem	129
9.2	A practical algorithm for subset sum problem	131
9.3	3-Satisfiability	131
IV	Asymptotically Dominant Properties and Cryptanalysis	135
10	Asymptotically Dominant Properties	139
10.1	A brief description	139
10.2	Random subgroups and generating tuples	141
10.3	Asymptotic properties of subgroups	142
10.4	Groups with generic free basis property	143
10.5	Quasi-isometrically embedded subgroups	145
11	Length-Based and Quotient Attacks	149
11.1	Anshel-Anshel-Goldfeld scheme	149
11.1.1	Description of the Anshel-Anshel-Goldfeld scheme	149
11.1.2	Security assumptions of the AAG scheme	150
11.2	Length-based attacks	152
11.2.1	A general description	152
11.2.2	LBA in free groups	155
11.2.3	LBA in groups from \mathcal{FB}_{exp}	156
11.3	Computing the geodesic length in a subgroup	157
11.3.1	Related algorithmic problems	158
11.3.2	Geodesic length in braid groups	159
11.4	Quotient attacks	161
11.4.1	Membership problems in free groups	162
11.4.2	Conjugacy problems in free groups	164
11.4.3	The MSP and SCSP* problems in groups with “good” quotients	167
	Bibliography	169
	Abbreviations and Notation	179
	Index	181



<http://www.springer.com/978-3-7643-8826-3>

Group-based Cryptography

Myasnikov, A.; Shpilrain, V.; Ushakov, A.

2008, XV, 183 p., Softcover

ISBN: 978-3-7643-8826-3

A product of Birkhäuser Basel