Contents

Introduction —— v

Jeffrey D. Achter and Rachel Pries
Generic Newton polygons for curves of given p-rank —— 1
1 Introduction —— 1
2 Structures in positive characteristic —— 3
2.1 The p-rank —— 3
2.2 Newton polygons —— 4
2.3 Semicontinuity and purity —— 7
2.4 Notation on stratifications and Newton polygons —— 8
3 Stratifications on the moduli space of Abelian varieties —— 9
3.1 The p-ranks of Abelian varieties —— 9
3.2 Newton polygons of Abelian varieties —— 10
4 The p-rank stratification of the moduli space of stable curves —— 11
4.1 The moduli space of stable curves —— 11
4.2 The p-rank stratification of $\overline{\mathcal{M}}_g$ —— 12
4.3 Connectedness of p-rank strata —— 13
4.4 Open questions about the p-rank stratification —— 13
5 Stratification by Newton polygon —— 14
5.1 Newton polygons of curves of small genus —— 14
5.2 Generic Newton polygons —— 15
6 Hyperelliptic curves —— 16
7 Some conjectures about Newton polygons of curves —— 18
7.1 Nonexistence philosophy —— 19
7.2 Supersingular curves —— 20
7.3 Other nonexistence results —— 20

Alp Bassa, Peter Beelen, and Nhut Nguyen
Good towers of function fields —— 23
1 Introduction —— 23
2 The Drinfeld modular towers $(X_0(P^n))_{n\geq0}$ —— 25
3 An example of a classical modular tower —— 32
4 A tower obtained from Drinfeld modules over a different ring —— 33
4.1 Explicit Drinfeld modules of rank 2 —— 33
4.2 Finding an isogeny —— 36
4.3 Obtaining a tower —— 38

Bibliografische Informationen
http://d-nb.info/1048115917

digitalisiert durch
DEUTSCHE
NATIONAL
BIBLIOTHEK

Claude Carlet and Sylvain Guilley
Correlation-immune Boolean functions for easing counter measures to side-channel attacks — 41
1 Introduction — 42
2 Preliminaries — 45
2.1 The combiner model of pseudo-random generator in a stream cipher and correlation-immune functions — 45
2.2 Side-channel attacks — 49
2.3 Masking counter measure — 51
3 Methods for allowing masking to resist higher order side-channel attacks — 53
3.1 Leakage squeezing for first-order masking — 53
3.2 Leakage squeezing for second-order masking — 55
3.3 Rotating S-box masking — 56
4 New challenges for correlation-immune Boolean functions — 58
4.1 Basic facts on CI functions, orthogonal arrays and dual distance of codes — 58
4.2 Known constructions of correlation-immune functions — 61
4.3 Synthesis of minimal weights of d-CI Boolean functions — 65

Jung Hee Cheon, Taechan Kim, and Yongsoo Song
The discrete logarithm problem with auxiliary inputs — 71
1 Introduction — 72
2 Algorithms for the ordinary DLP — 73
2.1 Generic algorithms — 73
2.2 Nongeneric algorithms — 76
3 The DLPwAI and Cheon's algorithm — 78
3.1 $p-1$ cases — 79
3.2 Generalized algorithms — 80
4 Polynomials with small value sets — 82
4.1 Fast multipoint evaluation in a blackbox manner — 82
4.2 An approach using polynomials of small value sets — 83
5 Approach using the rational polynomials: Embedding to elliptic curves — 84
6 Generalized DLPwAI — 85
6.1 Representation of a multiplicative subgroup of $\mathbb{Z}_{p-1}^{\times}$ — 85
6.2 A group action on $\mathbb{Z}_p^*$ and polynomial construction — 86
6.3 Main result — 86
7 Applications and implications — 87
7.1 Strong Diffie–Hellman problem and its variants — 87
7.2 Attack on the existing schemes using Cheon's algorithm — 88
8 Open problems and further work — 89

Massimo Giulietti and Gábor Korchmáros

Garden of curves with many automorphisms — 93

1 Introduction — 93

2 Notation and background — 94

3 Upper bounds on the size of G depending on g — 95

4 Upper bounds on the size of the p-subgroups of G depending on the p-rank — 96

5 Examples of curves with large automorphism groups — 97

5.1 Curves with unitary automorphism group — 97

5.2 Curves with Suzuki automorphism group — 98

5.3 Curves with Ree automorphism group — 99

5.4 The Giulietti–Korchmáros curve — 99

5.5 The generalized GK curve — 100

5.6 A curve admitting $\mathrm{SU}(3, p)$ as an automorphism group — 101

5.7 General hyperelliptic curves with a $\mathbb{K}$-automorphism 2-group of order $2g + 2$ — 101

5.8 A curve with genus $g = (2^h - 1)^2$ admitting a $\mathbb{K}$-automorphism 2-group of order of order $2(g - 1) + 2^{h+1} - 2$ — 101

5.9 General bielliptic curves with a dihedral $\mathbb{K}$-automorphism 2-group of order $4(g - 1)$ — 102

5.10 A curve of genus g with a semidihedral $\mathbb{K}$-automorphism 2-group of order $2(g - 1)$ — 104

6 Characterizations — 105

6.1 Curves with many automorphisms with respect to their genus — 105

6.2 Curves with a large nontame automorphism group — 106

6.3 Theorem 6.2 and some generalizations of Deligne–Lusztig curves — 107

6.4 Group-theoretic characterizations — 109

7 The possibilities for G when the p-rank is 0 — 110

8 Large automorphism p-groups in positive p-rank — 112

8.1 $p = 2$ — 112

8.2 $p = 3$ — 116

8.3 $p > 3$ — 117

Tor Helleseth

Nonlinear shift registers – A survey and challenges — 121

1 Introduction — 121

2 Nonlinear shift registers — 123

2.1 The binary de Bruijn graph — 124

2.2 The pure cycling register — 126

2.3 The complementary cycling register — 126

2.4 De Bruijn sequences — 126

3 Mykkeltveit's proof of Golomb's conjecture — 129
4 The D-morphism — 132
5 Conjugate pairs in PCR — 134
6 Finite fields and conjugate pairs — 135
6.1 Cycle joining and cyclotomy — 137
7 Periodic structure of NLFSRs — 139
8 Conclusions — 142

Florian Pausinger and Alev Topuzoğlu
Permutations of finite fields and uniform distribution modulo 1 — 145
1 Introduction — 145
2 Preliminaries — 146
3 Good and weak families of permutations — 150
4 Existence of good families — 151
5 Permutation polynomials of Carlitz rank 3 — 152
6 Bounds for $f(S_p^\sigma)$ — 154
7 Computational results — 156
8 Concluding remarks — 157

Alexander Pott, Kai-Uwe Schmidt, and Yue Zhou
Semifields, relative difference sets, and bent functions — 161
1 Introduction — 161
2 Semifields — 162
3 Relative difference sets — 165
4 Relative difference sets and semifields — 167
5 Planar functions in odd characteristic — 171
6 Planar functions in characteristic 2 — 172
7 Component functions of planar functions — 173
8 Concluding remarks and open problems — 175

Ron Steinfeld
NTRU cryptosystem: Recent developments and emerging mathematical problems in finite polynomial rings — 179
1 Introduction — 179
2 Notation and preliminaries — 181
2.1 Notation — 181
2.2 Probability and algorithms — 181
2.3 Rings — 182
2.4 Lattices — 182

3 Review of the NTRU cryptosystem — 183
3.1 The NTRU construction — 183
3.2 Security of NTRU: Computational/statistical problems and known attacks — 185
4 Recent developments in security analysis of NTRU — 189
4.1 Overview — 189
4.2 Gaussian distributions modulo lattices and Fourier analysis — 192
4.3 Statistical hardness of the NTRU decision key cracking problem — 195
4.4 Computational hardness of the ciphertext cracking problem — 198
5 Recent developments in applications of NTRU — 200
5.1 NTRU-based homomorphic encryption — 200
5.2 NTRU-based multilinear maps — 204
6 Conclusions — 207

Gabriel D. Villa-Salvador
Analog of the Kronecker–Weber theorem in positive characteristic — 213
1 Introduction — 213
2 The classical case — 215
3 A proof of the Kronecker–Weber theorem based on ramification groups — 216
4 Cyclotomic function fields — 219
5 The maximal Abelian extension of k — 221
6 Reciprocity law — 223
7 The proof of David Hayes — 224
8 Witt vectors and the conductor — 225
8.1 The conductor — 228
8.2 The conductor according to Schmid — 228
9 The Kronecker–Weber–Hayes theorem — 229
10 Final remarks — 235

Index — 239