Stream Ciphers and Number Theory

Thomas W. CUSICK
State University of New York at Buffalo

Cunsheng DING
The National University of Singapore

Ari RENVALL
University of Turku

1998
ELSEVIER
Amsterdam – Lausanne – New York – Oxford – Shannon – Singapore – Tokyo

Contents

Preface **VII**

1 Introduction **1**
1.1 Applications of Number Theory 1
1.2 An Outline of this Book 5

2 Stream Ciphers **11**
2.1 Stream Cipher Systems 11
2.1.1 Additive Synchronous Stream Ciphers 13
2.1.2 Additive Self-Synchronous Stream Ciphers 14
2.1.3 Nonadditive Synchronous Stream Ciphers 14
2.1.4 Stream Ciphering with Block Ciphers 16
2.1.5 Cooperatively Distributed Ciphering 18
2.2 Some Keystream Generators 21
2.2.1 Generators Based on Counters 22
2.2.2 Some Number-Theoretic Generators 23
2.3 Cryptographic Aspects of Sequences 25
2.3.1 Minimal Polynomial and Linear Complexity 25
2.3.2 Pattern Distribution of Key Streams 29
2.3.3 Correlation Functions 31
2.3.4 Sphere Complexity and Linear Cryptanalysis 32
2.3.5 Higher Order Complexities 35
2.4 Harmony of Binary NSGs 36
2.5 Security and Attacks 40

3 Primes, Primitive Roots and Sequences **43**
3.1 Cyclotomic Polynomials 43
3.2 Two Basic Problems from Stream Ciphers 44
3.3 A Basic Theorem and Main Bridge 47
3.4 Primes, Primitive Roots and Binary Sequences 50
3.5 Primes, Primitive Roots and Ternary Sequences 55

3.6 Primes, Negord and Sequences 58
3.7 Prime Powers, Primitive Roots and Sequences 60
3.8 Prime Products and Sequences 62
3.8.1 Binary Sequences and Primes 63
3.8.2 Ternary Sequences and Primes 64
3.9 On Cryptographic Primitive Roots 65
3.10 Linear Complexity of Sequences over Z_m 67
3.11 Period and its Cryptographic Importance 75

4 Cyclotomy and Cryptographic Functions 77
4.1 Cyclotomic Numbers 77
4.2 Cyclotomy and Cryptography 79
4.2.1 Cyclotomy and Difference Parameters 79
4.2.2 Cyclotomy and the Differential Cryptanalysis 81
4.2.3 Cryptographic Cyclotomic Numbers 82
4.3 Cryptographic Functions from Z_p to Z_d 82
4.3.1 The Case $d = 2$ 84
4.3.2 The Case $d = 3$ 85
4.3.3 The Case $d = 4$ 86
4.3.4 The Case $d = 5$ 87
4.3.5 The Case $d = 6$ 89
4.3.6 The Case $d = 8$ 89
4.3.7 The Case $d = 10$ 91
4.3.8 The Case $d = 12$ 93
4.4 Cryptographic Functions from Z_{pq} to Z_d 93
4.4.1 Whiteman's Generalized Cyclotomy and Cryptography . 94
4.4.2 Cryptographic Functions from Z_{pq} to Z_2 99
4.4.3 Cryptographic Functions from Z_{pq} to Z_4 102
4.5 Cryptographic Functions from Z_{p^2} to Z_2 104
4.6 Cryptographic Functions Defined on $GF(p^m)$ 107
4.7 The Origin of Cyclotomic Numbers 107

5 Special Primes and Sequences 113
5.1 Sophie Germain Primes and Sequences 113
5.1.1 Their Importance in Stream Ciphers 114
5.1.2 Their Relations with Other Number-theoretic Problems 115
5.1.3 The Existence Problem 116
5.1.4 A Search for Cryptographic Sophie Germain Primes . . 116
5.2 Tchebychef Primes and Sequences 117
5.2.1 Their Cryptographic Significance 117
5.2.2 Existence and Search Problem 118
5.3 Other Primes of Form $k \times 2^n + 1$ and Sequences 119
5.4 Primes of Form $(a^n - 1)/(a - 1)$ and Sequences 123

5.4.1 Mersenne Primes and Sequences 123
5.4.2 Cryptographic Primes of Form $((4u)^n - 1)/(4u - 1)$ . . 126
5.4.3 Prime Repunits and their Cryptographic Values 127
5.5 $n! \pm 1$ and $p\# \pm 1$ Primes and Sequences 127
5.6 Twin Primes and Sequences over $GF(2)$ 129
5.6.1 The Significance of Twins and their Sexes 130
5.6.2 Cryptographic Twins and the Sex Distribution 131
5.7 Twin Primes and Sequences over $GF(3)$ 133
5.8 Other Special Primes and Sequences 134
5.9 Prime Distributions and their Significance 134
5.10 Primes for Stream Ciphers and for RSA 135

6 Difference Sets and Cryptographic Functions 139
6.1 Rudiments of Difference Sets 139
6.2 Difference Sets and Autocorrelation Functions 142
6.3 Difference Sets and Nonlinearity 143
6.4 Difference Sets and Information Stability 145
6.5 Difference Sets and Linear Approximation 147
6.6 Almost Difference Sets 149
6.7 Almost Difference Sets and Autocorrelation Functions 153
6.8 Almost Difference Sets, Nonlinearity and Approximation 154
6.9 Summary 154

7 Difference Sets and Sequences 157
7.1 The NSG Realization of Sequences 157
7.2 Differential Analysis of Sequences 159
7.3 Linear Complexity of DSC (ADSC) Sequences 161
7.4 Barker Sequences 164

8 Binary Cyclotomic Generators 167
8.1 Cyclotomic Generator of Order 2k 167
8.2 Two-Prime Generator of Order 2 170
8.3 Two-Prime Generator of Order 4 182
8.4 Prime-Square Generator 183
8.5 Implementation and Performance 195
8.6 A Summary of Binary Cyclotomic Generators 196

9 Analysis of Cyclotomic Generators of Order 2 199
9.1 Crosscorrelation Property 200
9.2 Decimation Property 201
9.3 Linear Complexity 201
9.4 Security against a Decision Tree Attack 205
9.5 Sums of DSC Sequences 219

9.5.1 Linear Complexity Analysis 219
9.5.2 Balance Analysis 220
9.5.3 Correlation Analysis 220
9.5.4 Differential Analysis 220

10 Nonbinary Cyclotomic Generators 223
10.1 The rth-Order Cyclotomic Generator 223
10.2 Linear Complexity 224
10.3 Autocorrelation Property 226
10.4 Decimation Property 228
10.5 Ideas Behind the Cyclotomic Generators 228

11 Generators Based on Permutations 231
11.1 The Cryptographic Idea 231
11.2 Permutations on Finite Fields 233
11.3 A Generator Based on Inverse Permutations 234
11.4 Binary Generators and Permutations of $GF(2^n)$ 236
11.4.1 APN Permutations and their Properties 237
11.4.2 Quadratic Permutations with Controllable Nonlinearity 241
11.4.3 Permutations of Order 3 242
11.4.4 APN Permutations of Order $n-1$ 244
11.4.5 Permutations of Order $n-2$ 245
11.4.6 Permutations X^d with $d = 2^m - 1$ 246
11.4.7 APN Permutations via Crosscorrelation Function 246
11.4.8 Other Power Functions with Good Nonlinearity 251
11.4.9 Choosing the Linear Functions 251
11.5 Cyclic-Key Generators and their Problems 251
11.5.1 Cyclic-Key Generators 251
11.5.2 Several Specific Forms: An Overview 254
11.6 A Generator Based on Permutations of Z_m 256

12 Quadratic Partitions and Cryptography 265
12.1 Quadratic Partition and Cryptography 266
12.2 $p = x^2 + y^2$ and $p = x^2 + 4y^2$ 267
12.3 $p = x^2 + 2y^2$ and $p = x^2 + 3y^2$ 274
12.4 $p = x^2 + ny^2$ and Quadratic Reciprocity 275
12.5 $p = x^2 + 7y^2$ and Quadratic Forms 275
12.6 $p = x^2 + 15y^2$ and Genus Theory 279
12.7 $p = x^2 + ny^2$ and Class Field Theory 281
12.8 Other Cryptographic Quadratic Partitions 283

13 Group Characters and Cryptography 287
13.1 Group Characters . . . 287
13.2 Field Characters and Cryptography . . . 289
13.2.1 Field Multiplicative Characters: Most Used Ones . . . 291
13.2.2 Field Additive Characters: Most Used Ones . . . 293
13.3 The Nonlinearity of Characters . . . 299
13.3.1 The Nonlinearity of Multiplicative Characters . . . 299
13.3.2 The Nonlinearity of Additive Characters . . . 300
13.4 Ring Characters and Cryptography . . . 301
13.5 Group Characters and Cyclotomic Numbers . . . 302

14 P-Adic Numbers, Class Numbers and Sequences 307
14.1 The 2-Adic Value and 2-Adic Expansion . . . 307
14.2 A Fast Algorithm for the 2-Adic Expansion . . . 313
14.3 The Arithmetic of $Q_{[2]}$ and $Z_{[2]}$ . . . 313
14.4 Feedback Shift Registers with Carry . . . 318
14.5 Analysis and Synthesis of FCSRs . . . 320
14.6 The 2-Adic Span and 2-RA Algorithm . . . 326
14.7 Some Properties of FCSR Sequences . . . 335
14.8 Blum-Blum-Shub Sequences & Class Numbers . . . 339

15 Prime Ciphering Algorithms 347
15.1 Prime-32: A Description . . . 347
15.2 Theoretical Results about Prime-32 . . . 352
15.3 Security Arguments . . . 354
15.4 Performance of Prime-32 . . . 357
15.5 Prime-32 with a 192-Bit Key . . . 357
15.6 Prime-64 . . . 357

16 Cryptographic Problems and Philosophies 359
16.1 Nonlinearity and Linearity . . . 359
16.2 Stability and Instability . . . 362
16.2.1 Stability and Diffusion . . . 363
16.2.2 Stability of Local Nonlinearities and Differences . . . 365
16.2.3 Correlation Stability and Pattern Stability . . . 365
16.2.4 Mutual Information Stability . . . 366
16.3 Localness and Globalness . . . 367
16.4 Goodness and Badness . . . 369
16.5 About Good plus Good . . . 370
16.6 About Good plus Bad . . . 371
16.7 About Bad plus Good . . . 372
16.8 Hardware and Software Model Complexity . . . 373

Appendices **375**

A More About Cyclotomic Numbers **375**
A.1 Cyclotomic Numbers of Order 7 375
A.2 Cyclotomic Numbers of Orders 9, 18 377
A.3 Cyclotomic Numbers of Order Eleven 378
A.4 On Other Cyclotomic Numbers 378
A.5 Behind Cyclotomic Numbers 379

B Cyclotomic Formulae of Orders 6, 8 and 10 **383**

C Finding Practical Primes **389**

D List of Research Problems **391**

E Exercises **393**

F List of Mathematical Symbols **399**

Bibliography **401**

Index **429**