

Contents

- 1 Introduction to Stream Ciphers 1**
 - 1.1 History I: Antique Ciphers 1
 - 1.2 Lessons from History: The Classification of Ciphers 3
 - 1.3 History II: The Golden Age of Stream Ciphers 8
 - 1.4 Lessons from the Enigma 8
 - 1.5 History III: Towards Modern Cryptography 10
 - 1.6 When to Use Stream Ciphers? 11
 - 1.7 Outline of the Book 11
- Part I Shift Register-Based Stream Ciphers**
- 2 Linear Feedback Shift Registers 17**
 - 2.1 Basic Definitions 17
 - 2.2 Algebraic Description of LFSR Sequences 18
 - 2.2.1 Generating Functions 19
 - 2.2.2 Feedback Polynomials Without Multiple Roots 20
 - 2.2.3 Feedback Polynomials with Multiple Roots 21
 - 2.2.4 LFSR Sequences as Cyclic Linear Codes 23
 - 2.3 Properties of m-Sequences 24
 - 2.3.1 Golomb’s Axioms 24
 - 2.3.2 Sequences with Two Level Auto-Correlation 27
 - 2.3.3 Cross-Correlation of m-Sequences 29
 - 2.4 Linear Complexity 30
 - 2.4.1 Definition and Basic Properties 30
 - 2.4.2 The Berlekamp-Massey Algorithm 33
 - 2.4.3 Asymptotic Fast Computation of Linear Complexity 37
 - 2.4.4 Linear Complexity of Random Sequences 42
 - 2.5 The Linear Complexity Profile of Pseudo-random Sequences 44
 - 2.5.1 Basic Properties 44
 - 2.5.2 Continued Fractions 46

2.5.3	Classification of Sequences with a Perfect Linear Complexity Profile	48
2.6	Implementation of LFSRs	50
2.6.1	Hardware Realization of LFSRs	51
2.6.2	Software Realization of LFSRs	52
3	Non-linear Combinations of LFSRs	59
3.1	De Bruijn Sequences	59
3.2	A Simple Example of a Non-linear Combination of LFSRs	64
3.3	Different Attack Classes	65
3.3.1	Time-Memory Trade-off Attacks	65
3.3.2	Algebraic Attacks	65
3.3.3	Correlation Attacks	66
3.4	Non-linear Combinations of Several LFSR Sequences	66
3.4.1	The Product of Two LFSRs	67
3.4.2	General Combinations	70
3.5	Non-linear Filters	72
3.6	Correlation Immune Functions	75
3.6.1	Definition and Alternative Characterizations	75
3.6.2	Siegenthaler's Inequality	78
3.6.3	Asymptotic Enumeration of Correlation Immune Functions	80
4	Correlation Attacks	91
4.1	CJS-Attacks	91
4.1.1	The Basic Version	91
4.1.2	Using Relations of Different Size	94
4.1.3	How to Search Relations	96
4.1.4	Extended Relation Classes	98
4.1.5	Twice Step Decoding	101
4.1.6	Evaluation of the Relations	103
4.2	Attacks Based on Convolutional Codes	105
4.2.1	Introduction to Convolutional Codes	105
4.2.2	Decoding Convolutional Codes	107
4.2.3	Application to Cryptography	111
4.3	Attacking LFSRs with Sparse Feedback Polynomials	114
5	BDD-Based Attacks	117
5.1	Binary Decision Diagrams	117
5.1.1	Ordered BDDs	118
5.1.2	Free BDDs	124
5.2	An Example of a BDD-Based Attack	126
5.2.1	The Cipher E_0	126
5.2.2	Attacking E_0	127
6	Algebraic Attacks	131
6.1	Tools for Solving Non-linear Equations	131
6.1.1	Gröbner Bases	131

6.1.2	Linearization	143
6.2	Pre-processing Techniques for Algebraic Attacks	147
6.2.1	Reducing the Degree	147
6.2.2	Dealing with Combiners with Memory	149
6.3	Real World Examples	151
6.3.1	LILI-128	151
6.3.2	E_0	153
7	Irregular Clocked Shift Registers	155
7.1	The Stop-and-Go Generator and the Step-Once-Twice Generator	155
7.2	The Alternating Step Generator	157
7.3	The Shrinking Generator	158
7.3.1	Description of the Cipher	159
7.3.2	Linear Complexity of the Shrinking Generator	159
7.3.3	Correlation Attacks Against the Shrinking Generator	161
7.4	Side Channel Attacks	163
 Part II Some Special Ciphers		
8	The Security of Mobile Phones (GSM)	169
8.1	The GSM Protocol	169
8.2	A5/2	170
8.2.1	Description of A5/2	170
8.2.2	An Instance of a Ciphertext-Only Attack	172
8.2.3	Other Attacks Against A5/2	175
8.3	A5/1	176
8.3.1	Description of A5/1	176
8.3.2	Time-Memory Trade-off Attacks	176
8.3.3	Correlation Attacks	179
9	RC4 and Related Ciphers	183
9.1	Description of RC4	183
9.2	Application of RC4 in WLAN Security	184
9.2.1	The WEP Protocol	184
9.2.2	The WPA Protocol	185
9.2.3	A Weakness Common to Both Protocols	187
9.3	Analysis of the RC4 Key Scheduling	190
9.3.1	The Most Likely and Least Likely RC4 Permutation	191
9.3.2	Discarding the First RC4 Bytes	196
9.4	Chosen IV Attacks	199
9.4.1	Initialization Vector Precedes the Main Key	199
9.4.2	Variants of the Attack	200
9.4.3	Initialization Vector Follows the Main Key	202
9.5	Attacks Based on Golić's Correlation	202
9.5.1	Initialization Vector Follows the Main Key	204
9.5.2	Initialization Vector Precedes the Main Key	205
9.5.3	Attacking RC4 with the First n Bytes Discarded	207

9.5.4	A Ciphertext-Only Attack	209
9.6	State Recovering Attacks	209
9.7	Other Attacks on RC4	212
9.7.1	Digraph Probabilities	213
9.7.2	Fortuitous States	218
9.8	RC4 Variants	222
9.8.1	An RC4 Variant for 32-Bit Processors	222
9.8.2	RC4A	224
9.8.3	Modifications to Avoid Known Attacks	227
10	The eStream Project	229
10.1	Trivium	229
10.2	Rabbit	232
10.3	Mosquito and Moustique	235
11	The Blum-Blum-Shub Generator and Related Ciphers	241
11.1	Cryptographically Secure Pseudo-random Generators	241
11.2	The Blum-Blum-Shub Generator	244
11.3	Implementation Aspects	247
11.4	Extracting Several Bits per Step	251
11.5	The RSA Generator and the Power Generator	253
11.6	Generators Based on Other Hard Problems	254
11.7	Unconditionally Secure Pseudo-random Sequences	256
 Part III Mathematical Background		
12	Computational Aspects	261
12.1	Bit Tricks	261
12.1.1	Infinite 2-adic Expansions	261
12.1.2	Sideway Addition	262
12.1.3	Sideway Addition for Arrays	263
12.2	Binary Decision Diagrams, Implementation Aspects	264
12.2.1	Memory Management	264
12.2.2	Implementation of the Basic Operations	266
12.2.3	Implementation of Reordering Algorithms	267
12.2.4	Emulating a BDD Base	271
12.3	The O-Notation	272
12.4	The Complexity Classes \mathcal{P} and \mathcal{NP}	273
12.5	Fast Linear Algebra	278
12.5.1	Matrix Multiplication	278
12.5.2	Other Matrix Operations	289
12.5.3	Wiedmann's Algorithm and Black Box Linear Algebra	291
13	Number Theory	293
13.1	Basic Results	293
13.2	The Group $(\mathbb{Z}/n\mathbb{Z})^\times$	294
13.3	The Prime Number Theorem and Its Consequences	295

13.4	Zsigmondy's Theorem	297
13.5	Quadratic Residues	299
13.6	Lattice Reduction	301
14	Finite Fields	305
14.1	Basic Properties	305
14.2	Irreducible Polynomials	305
14.3	Primitive Polynomials	307
14.4	Trinomials	308
14.5	The Algebraic Normal Form	309
15	Statistics	311
15.1	Measure Theory	311
15.2	Simple Tests	312
15.2.1	The Variation Distance	312
15.2.2	The Test Problem	313
15.2.3	Optimal Tests	314
15.2.4	Bayesian Statistics	315
15.3	Sequential Tests	316
15.3.1	Introduction to Sequential Analysis	316
15.3.2	Martingales	316
15.3.3	Wald's Sequential Likelihood Ratio Test	319
15.3.4	Brownian Motion	322
15.3.5	The Functional Central Limit Theorem	326
16	Combinatorics	329
16.1	Asymptotic Calculations	329
16.2	Permutations	332
16.3	Trees	334
Part IV Exercises with Solutions		
17	Exercises	339
17.1	Proposals for Programming Projects	344
18	Solutions	347
Part V Programs		
19	An Overview of the Programs	365
20	Literate Programming	371
20.1	Introduction to Literate Programming	371
20.2	Pweb Design Goals	371
20.3	Pweb Manual	372
20.3.1	Structure of a WEB-Document	372
20.3.2	Text Sections	372
20.3.3	Code Sections and Modules	373
20.3.4	Macros	374

20.3.5	Special Variable Names	375
20.3.6	Include Files	375
20.3.7	Conditional Compilation	375
20.3.8	More pweb Commands	376
20.3.9	Compatibility Features	376
20.3.10	Common Errors	376
20.3.11	Editing pweb Documents	377
20.3.12	Extending pweb	377
Notations		379
References		381
Index		395

Stream Ciphers

Klein, A.

2013, XIX, 399 p. 71 illus., Softcover

ISBN: 978-1-4471-5078-7