

Contents

Foreword	vii
Preface	ix
Notation	xi
Chapter 1. Arithmetics of Finite Fields and Polynomials	1
1.1. Basic Algebra	1
1.2. Construction of finite fields	19
1.3. Polynomials over finite fields	28
Comments to Chapter 1	35
Chapter 2. Boolean Functions	37
2.1. Basic concepts and definitions	37
2.2. Numerical and metric characteristics	44
2.3. Autocorrelation and crosscorrelation	56
2.4. Group algebra of Boolean functions	61
2.5. Cryptographic properties of Boolean functions and mappings	65
2.6. Covering sequences of Boolean functions	74
Comments to Chapter 2	76
Chapter 3. Classifications of Boolean Functions	77
3.1. Group equivalence of mappings. Polya's theorem	77
3.2. Classification of Boolean functions of five variables	83
3.3. Classification of quadratic Boolean functions	91
3.4. Classification of homogeneous cubic forms of 8 variables	99
3.5. <i>RM</i> -equivalence of Boolean functions	101
Comments to Chapter 3	104
Chapter 4. Linear Codes over the Field \mathbb{F}_2	107
4.1. Basic properties of linear block codes	107
4.2. The decoding problem	116
4.3. Cyclic codes	120
4.4. Some classes of primitive cyclic codes	131
Comments to Chapter 4	136
Chapter 5. Reed–Muller Codes	139
5.1. General properties of the Reed–Muller codes	139
5.2. Reed's decoding algorithm	146
5.3. First order Reed–Muller codes and connections with other codes	150
5.4. Reed–Muller codes of second order and related codes	157

5.5. Classification of Boolean functions and Reed–Muller codes of the 3rd order	160
Comments to Chapter 5	163
Chapter 6. Nonlinearity	165
6.1. Nonlinearity as a measure of cryptographic quality	165
6.2. Maximum-nonlinear bent functions and their properties	166
6.3. Some classes of maximum-nonlinear bent functions	172
6.4. Partially maximum-nonlinear (partially bent) functions and their properties	177
6.5. Plateaued functions and partially defined mn-bent functions	179
6.6. Hyperbent functions	188
6.7. Biorthogonal bases	189
Comments to Chapter 6	192
Chapter 7. Correlation Immunity and Resiliency	195
7.1. Main definitions and properties	195
7.2. The inheritance of properties under restrictions of Boolean functions	208
7.3. General methods for constructing correlation-immune functions and resilient mappings	214
7.4. Nonlinearity of correlation-immune and resilient functions	218
7.5. Construction of resilient Boolean functions with good cryptographic properties	222
7.6. Covering sequences of correlation-immune and resilient functions	226
7.7. Quadratic resilient Boolean functions of maximum order	235
Comments to Chapter 7	237
Chapter 8. Codes, Boolean Mappings, and Their Cryptographic Properties	239
8.1. Almost perfect nonlinear and almost bent mappings	239
8.2. Coding-theoretic approach to the study of APN and AB mappings	249
8.3. Cyclic codes and Boolean mappings	255
8.4. Avalanche criteria and propagation criteria	261
8.5. Construction of Boolean functions satisfying the propagation criterion of degree k and order t	265
8.6. Global avalanche characteristics of Boolean functions	266
Comments to Chapter 8	269
Chapter 9. Basics of Cryptanalysis	271
9.1. The Berlekamp–Massey algorithm. Linear complexity	271
9.2. Principles of the statistical method for cryptanalysis of block ciphers	281
9.3. Principles of the correlation cryptanalysis method	287
9.4. Principles of the linear cryptanalysis method	295
9.5. Principles of the difference (differential) cryptanalysis method	300
Comments to Chapter 9	301
Bibliography	305
Index	329