

Contents

Preface	xi
CHAPTER 1 A bit of history	1
1.1 George Boole (1815–1864).....	1
1.2 Claude Elwood Shannon (1916–2001).....	3
CHAPTER 2 Fourier analysis of Boolean functions.....	5
2.1 Basic Definitions on Boolean Functions	5
2.2 Walsh Transform	7
2.3 Autocorrelation Function	8
2.4 Walsh Transform on Subspaces	9
2.5 Linear Transformations and the Sign Function	10
2.6 Parseval Equation	12
2.7 Asymptotic Results on Walsh Coefficients	13
2.8 Probability Distributions.....	14
2.9 Hadamard Matrices and Nonlinearity Bounds	16
2.10 Fast Walsh Transform.....	18
2.11 LFSRs and Linear Complexity.....	19
2.12 The Berlekamp–Massey Algorithm	21
2.13 De Bruijn Sequence	22
CHAPTER 3 Avalanche and propagation criteria	25
3.1 Introduction	25
3.2 Counting SAC Functions	26
3.3 Counting Balanced SAC Functions	28
3.4 Higher Order SAC.....	29
3.5 Propagation Criteria	38
3.6 Higher Order $PC(k)$	39
3.7 Construction of $SAC(k)$ and $PC(k)$ Functions.....	41
CHAPTER 4 Correlation immune and resilient Boolean functions	49
4.1 Introduction	49
4.2 Basic Properties of Correlation Immunity.....	50
4.3 LFSRs and Correlation Immunity.....	52

4.4	Counting Correlation Immune Functions	59
4.5	Resilient Functions	60
4.6	Tradeoff Between Correlation Immunity and Degree	61
4.7	Connections with Orthogonal Arrays	63
4.8	Constructing Correlation Immune Functions	65
4.9	Tradeoff Between Correlation Immunity and Nonlinearity	68
CHAPTER 5	Bent Boolean functions	73
5.1	Introduction	73
5.2	Definitions and Background	74
5.3	Characterizations of the Bent Property	76
5.4	Meier and Staffelbach's Approach	79
5.5	Degree of a Bent Function	80
5.6	New From Old Bent Functions	81
5.7	Rothaus's Construction	84
5.8	Maiorana and McFarland's Construction	85
5.9	Dillon's Construction	86
5.10	Dobbertin's Construction	89
5.11	Carlet's Construction	90
5.12	Extended Maiorana-McFarland Class	90
5.13	Normal and Nonnormal Bent Functions	96
5.14	Counting Bent Functions	97
5.15	Highly Nonlinear Balanced Functions	100
5.16	Partially Bent Functions	104
5.17	Semi-bent Functions	106
5.18	Symmetric Bent Functions	107
5.19	Rotation Symmetric Functions	108
5.20	Enumeration of Rotation Symmetric Functions	113
CHAPTER 6	Stream cipher design	119
6.1	Introduction	119
6.2	Boolean Functions in Pseudorandom Bit Generators	120
6.3	Nonlinear Combination Generators	124
6.4	Nonlinear Filter Generators	128
6.5	Multiplexer Generator	132
6.6	Irregularly Clocked LFSRs in Generators	140
6.7	Algebraic and Linearization Attacks	147
6.8	The eSTREAM Project	155
CHAPTER 7	Block ciphers	157
7.1	Some History	157
7.2	Introduction	158

7.3	Block Ciphers' Modes of Operation	159
7.3.1	Confidentiality modes	159
7.3.2	Authentication modes	162
7.4	Design Approaches	163
7.4.1	Feistel ciphers	163
7.4.2	Substitution permutation networks	164
7.5	Notable Symmetric Ciphers	165
7.5.1	Data Encryption Standard	166
7.5.2	Advanced Encryption Standard	173
7.6	Periods of Rijndael Transformations	180
7.7	Algebraic Representations of Rijndael/AES	181
7.8	Embedding AES in BES	185
7.9	Further Embeddings of AES	190
CHAPTER 8	Boolean Cayley graphs	193
8.1	Introduction	193
8.2	Spectra of Boolean Cayley Graphs	195
8.3	Few Spectral Coefficients of Boolean Functions	196
8.4	Bent Boolean Cayley Graphs	197
8.5	Coloring the Boolean Cayley Graph	200
8.6	Avalanche Features of the Cayley Graphs	201
8.7	Sensitivity of Hamming Weight of f to $\text{Spec}(\Gamma_f)$	204
8.8	Boolean Cayley Graphs Under Affine Transformations	205
References		209
Index		229