

Contents

1	Boolean Functions and Their Walsh Transforms	1
1.1	Logic Gates and Boolean Variables	1
1.2	Boolean Functions and Their Representations	2
1.2.1	Algebraic Normal Form	4
1.2.2	Truth Table Representation	5
1.2.3	Support Representation	5
1.2.4	Minterm Representation	6
1.2.5	Representation Conversions	7
1.2.6	Enumeration of Boolean Functions	9
1.3	Walsh Transforms and Walsh Spectrum of Boolean Functions	9
1.3.1	Walsh Functions and Walsh Transforms	10
1.3.2	Properties of Walsh Transforms	12
1.3.3	Hadamard Matrices	18
1.4	Basic Models of Stream Ciphers That Use Boolean Functions	20
1.4.1	Linear Feedback Shift Registers	22
1.4.2	Nonlinear Filtering Generators and Nonlinear Combiners	24
1.5	Cryptographic Properties of Boolean Functions	25
1.5.1	Algebraic Degree	25
1.5.2	Balance	26
1.5.3	Nonlinearity	27
1.5.4	Linear Structure	27
1.5.5	Propagation Criterion	27
1.5.6	Correlation Immunity	28
1.5.7	Algebraic Immunity	28
1.5.8	Remarks	29
	References	29

Independence of Boolean Functions of Their Variables	31
2.1 Introduction	31
2.2 The Algebraic Independence of Boolean Functions of Their Variables	31
2.3 The Degeneracy of Boolean Functions	37
2.4 Images of Boolean Functions on a Hyperplane	42
2.5 Derivatives of Boolean Functions	44
2.6 The Statistical Independence of Boolean Functions of Their Variables	48
2.7 The Statistical Independence of Two Individual Boolean Functions	53
2.7.1 Properties of the Statistical Independence of Boolean Functions	54
2.7.2 How to Judge When Two Boolean Functions Are Statistically Independent	56
2.7.3 Construction of Statistically Independent Boolean Functions	59
2.7.4 Enumeration of Statistically Independent Boolean Functions	63
2.7.5 On the Statistical Independence of a Group of Boolean Functions	65
References	71
Nonlinearity Measures of Boolean Functions	73
3.1 Introduction	73
3.2 Algebraic Degree and Nonlinearity of Boolean Functions	74
3.3 Walsh Spectrum Description of Nonlinearity	75
3.4 Nonlinearity of Some Basic Operations of Boolean Functions	77
3.5 Upper and Lower Bounds of Nonlinearity of Boolean Functions ...	84
3.6 Nonlinearity of Balanced Boolean Functions	86
3.7 Higher-Order Nonlinearity of Boolean Functions	87
3.8 Linear Structures of Boolean Functions	89
3.9 Remarks	94
References	95
Correlation Immunity of Boolean Functions	97
4.1 The Correlation Attack of Nonlinear Combiners	97
4.2 The Correlation Immunity and Correlation Attacks	101
4.3 Correlation Immunity of Boolean Functions	103
4.4 Correlation Immune Functions and Error-Correcting Codes	104
4.5 Construction of Correlation Immune Boolean Functions	106
4.5.1 Known Constructions of Correlation Immune Boolean Functions	107

4.5.2 Construction of Correlation Immune Boolean Functions Based on A Single Code	108
4.5.3 Preliminary Enumeration of Correlation Immune Boolean Functions	110
4.5.4 Construction of Correlation Immune Boolean Functions Using a Family of Error-Correcting Codes	110
4.6 Lower Bounds on Enumeration of the Correlation Immune Functions Constructible from the Error-Correcting Code Construction	113
4.7 Examples	114
4.8 Exhaustive Construction of Correlation Immune Boolean Functions	117
4.9 An Example of Exhaustive Construction of Correlation Immune Functions	119
4.10 Construction of High-Order Correlation Immune Boolean Functions	122
4.11 Construction of Correlation Immune Boolean Functions with Other Cryptographic Properties	124
4.11.1 Correlation Immune Functions with Good Balance	125
4.11.2 Correlation Immune Functions with High Algebraic Degree	126
4.11.3 Correlation Immune Functions with High Nonlinearity ...	127
4.11.4 Correlation Immune Functions with Propagation Criterion	130
4.11.5 Linear Structure Characteristics of Correlation Immune Functions	131
4.12 Construction of Algebraically Nondegenerate Correlation Immune Functions	133
4.12.1 On the Algebraic Degeneration of Correlation Immune Functions	134
4.12.2 Construction of Algebraically Nondegenerate Correlation Immune Functions	135
4.13 The ε -Correlation Immunity of Boolean Functions	139
4.14 Remarks	143
References	143
5 Algebraic Immunity of Boolean Functions	147
5.1 Algebraic Attacks on Stream Ciphers	147
5.2 A Small Example of Algebraic Attack	149
5.3 Annihilators and Algebraic Immunity of Boolean Functions	151
5.4 Construction of Annihilators of Boolean Functions	154
5.5 On the Upper and Lower Bounds of Algebraic Immunity of Boolean Functions	161

5.6	Computing the Annihilators of Boolean Functions	162
5.6.1	Computing the Annihilators of Boolean Functions: Approach I	163
5.6.2	Computing the Annihilators of Boolean Functions: Approach II	166
	References	175
6	The Symmetric Property of Boolean Functions	177
6.1	Basic Properties of Symmetric Boolean Functions	177
6.2	Computing the Walsh Transform of Symmetric Boolean Functions	180
6.2.1	Walsh Transforms on Symmetric Boolean Functions	180
6.2.2	Computational Complexity	184
6.3	Correlation Immunity of Symmetric Functions	187
6.3.1	When n Is Odd	189
6.3.2	When n Is Even	190
6.3.3	Higher-Order Correlation Immunity	191
6.4	On Symmetric Resilient Functions	192
6.4.1	Constructions of Symmetric Resilient Boolean Functions	193
6.4.2	Searching for More Solutions	194
6.4.3	The Exact Resiliency of Constructed Resilient Functions	196
6.5	Basic Properties of Majority Functions	198
6.6	The Walsh Spectrum of Majority Functions	203
6.6.1	When n Is Odd	203
6.6.2	When n Is Even	204
6.7	The Correlation Immunity of Majority Functions	206
6.8	The ε -Correlation Immunity of Majority Functions	209
6.8.1	When n Is Odd	209
6.8.2	When n Is Even	211
6.9	Remarks	213
	References	214
7	Boolean Function Representation of S-Boxes and Boolean Permutations	217
7.1	Vectorial Boolean Function Representation of S-Boxes	217
7.2	Boolean Function Representation of S-Boxes	218
7.2.1	On the Properties of (n, n) -Boolean Permutations	220
7.3	Properties of Boolean Permutations	223
7.4	Inverses of Boolean Permutations	225
7.5	Intractability Assumption and One-Way Trapdoor Boolean Permutations	229

7.6	Construction of Boolean Permutations	230
7.6.1	Some Primary Constructions	232
7.6.2	On the Flexibility of the New Construction Method for Boolean Permutations	236
7.6.3	Construction of Trapdoor Boolean Permutations with Limited Number of Terms	237
7.7	A Small Example of Boolean Permutations	238
7.7.1	Linearity and Nonlinearity of Boolean Permutations	239
	References	240
8	Cryptographic Applications of Boolean Functions	243
8.1	Applications of Degenerate Boolean Functions to Logic Circuit Representation	243
8.2	An Application of Boolean Permutations to Public Key Cryptosystem Design	245
8.2.1	Public Key Cryptosystem 1 (PKC1)	245
8.2.2	Public Key Cryptosystem 2 (PKC2)	246
8.2.3	Public Key Cryptosystem 3 (PKC3)	247
8.3	Application of Boolean Permutations to Digital Signatures	248
8.4	Application of Boolean Permutations to Shared Signatures	249
8.5	An Application of Boolean Permutations to Key Escrow Scheme	250
8.5.1	Setup	250
8.5.2	Escrowing Verification	251
8.5.3	Key Recovery	252
8.5.4	Properties	252
8.6	A Small Example of Key Escrow Scheme Based on Boolean Permutations	253
8.6.1	Selecting a Boolean Permutation of Order 6	253
8.6.2	Preparation	254
8.6.3	Verification	255
8.6.4	Key Recovery	255
8.7	Remarks	256
	References	256