## Contents

*Preface* ..... ix
*Acknowledgments* ..... x
*Notation* ..... xii

### 1 Introduction to cryptography, codes, Boolean, and vectorial functions

- 1.1 Cryptography ..... 1
- 1.2 Error-correcting codes ..... 4
- 1.3 Boolean functions ..... 17
- 1.4 Vectorial functions ..... 24

### 2 Generalities on Boolean and vectorial functions

- 2.1 A hierarchy of equivalence relations over Boolean and vectorial functions ..... 27
- 2.2 Representations of Boolean functions and vectorial functions ..... 30
- 2.3 The Fourier–Hadamard transform and the Walsh transform ..... 52
- 2.4 Fast computation of S-boxes ..... 74

### 3 Boolean functions, vectorial functions, and cryptography

- 3.1 Cryptographic criteria (and related parameters) for Boolean functions ..... 76
- 3.2 Cryptographic criteria for vectorial functions in stream and block ciphers ..... 112
- 3.3 Cryptographic criteria and parameters for vectorial functions in stream ciphers ..... 129
- 3.4 Cryptographic criteria and parameters for vectorial functions in block ciphers ..... 134
- 3.5 Search for functions achieving the desired features ..... 142
- 3.6 Boolean and vectorial functions for diffusion, secret sharing, and authentication ..... 145

### 4 Boolean functions, vectorial functions, and error-correcting codes

- 4.1 Reed–Muller codes ..... 151
- 4.2 Other codes related to Boolean functions ..... 159
## Contents

5 Functions with weights, Walsh spectra, and nonlinearities easier to study 164
  5.1 Affine functions and their combinations 164
  5.2 Quadratic functions and their combinations 170
  5.3 Cubic functions 180
  5.4 Indicators of flats 181
  5.5 Functions admitting (partial) covering sequences 182
  5.6 Functions with low univariate degree and related functions 187

6 Bent functions and plateaued functions 189
  6.1 Bent Boolean functions 190
  6.2 Partially-bent and plateaued Boolean functions 255
  6.3 Bent \(_4\) and partially-bent \(_4\) functions 266
  6.4 Bent vectorial functions 268
  6.5 Plateaued vectorial functions 274

7 Correlation immune and resilient functions 284
  7.1 Correlation immune and resilient Boolean functions 284
  7.2 Resilient vectorial Boolean functions 313

8 Functions satisfying SAC, PC, and EPC, or having good GAC 318
  8.1 \(PC(l)\) criterion 318
  8.2 \(PC(l)\) of order \(k\) and \(EPC(l)\) of order \(k\) criteria 319
  8.3 Absolute indicator 320

9 Algebraic immune functions 321
  9.1 Algebraic immune Boolean functions 321
  9.2 Algebraic immune vectorial functions 344

10 Particular classes of Boolean functions 352
  10.1 Symmetric functions 352
  10.2 Rotation symmetric, idempotent, and other similar functions 360
  10.3 Direct sums of monomials 362
  10.4 Monotone functions 363

11 Highly nonlinear vectorial functions with low differential uniformity 369
  11.1 The covering radius bound; bent/perfect nonlinear functions 370
  11.2 The Sidelnikov–Chabaud–Vaudenay bound 370
  11.3 Almost perfect nonlinear and almost bent functions 371
  11.4 The known infinite classes of AB functions 394
  11.5 The known infinite classes of APN functions 399
  11.6 Differentially uniform functions 412
## Contents

12 Recent uses of Boolean and vectorial functions and related problems  
12.1 Physical attacks and related problems on functions and codes  
12.2 Fully homomorphic encryption and related questions on Boolean functions  
12.3 Local pseudorandom generators and related criteria on Boolean functions  
12.4 The Gowers norm on pseudo-Boolean functions  
13 Open questions  
13.1 Questions of general cryptography dealing with functions  
13.2 General questions on Boolean functions and vectorial functions  
13.3 Bent functions and plateaued functions  
13.4 Correlation immune and resilient functions  
13.5 Algebraic immune functions  
13.6 Highly nonlinear vectorial functions with low differential uniformity  
13.7 Recent uses of Boolean and vectorial functions and related problems  
14 Appendix: finite fields  
14.1 Prime fields and fields with four, eight, and nine elements  
14.2 General finite fields: construction, primitive element  
14.3 Representation (additive and multiplicative); trace function  
14.4 Permutations on a finite field  
14.5 Equations over finite fields  

References  
Index