| | |
|---|---|
| 1. Record Nr. | UNINA9910797415103321 |
| Autore | Tokareva Natalia |
| Titolo | Bent functions : results and applications to cryptography / / by Natalia Tokareva, Sobolev Institute of Mathematics, Novosibirsk State University, Novosibirsk, Russia |
| Pubbl/distr/stampa | London, UK : , : Elsevier Science, , [2015]<br>©2015 |
| ISBN | 0-12-802555-7<br>0-12-802318-X |
| Descrizione fisica | 1 online resource (221 p.) |
| Disciplina | 511.324 |
| Soggetti | Computer security<br>Data encryption (Computer science)<br>Algebra, Boolean |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Description based upon print version of record |
| Nota di bibliografia | Includes bibliographical references and index. |
| Nota di contenuto | Front Cover; Bent Functions: Results and Applications to Cryptography; Copyright; Contents; Foreword; Preface; Notation; Chapter 1: Boolean Functions; Introduction; 1.1 Definitions; 1.2 Algebraic Normal Form; 1.3 Boolean Cube and Hamming Distance; 1.4 Extended Affinely Equivalent Functions; 1.5 Walsh-Hadamard Transform; 1.6 Finite Field and Boolean Functions; 1.7 Trace Function; 1.8 Polynomial Representation of a Boolean Function; 1.9 Trace Representation of a Boolean Function; 1.10 Monomial Boolean Functions; Chapter 2: Bent Functions: An Introduction; Introduction<br>2.1 Definition of a Nonlinearity2.2 Nonlinearity of a Random Boolean Function; 2.3 Definition of a Bent Function; 2.4 If n Is Odd?; 2.5 Open Problems; 2.6 Surveys; Chapter 3: History of Bent Functions; Introduction; 3.1 Oscar Rothaus; 3.2 V.A. Eliseev and O.P. Stepchenkov; 3.3 From the 1970s to the Present; Chapter 4: Applications of Bent Functions; Introduction; 4.1 Cryptography: Linear Cryptanalysis and Boolean Functions; 4.2 Cryptography: One Historical Example; 4.3 Cryptography: Bent Functions in CAST; 4.4 Cryptography: Bent Functions in Grain; 4.5 Cryptography: Bent Functions in HAVAL |

4.6 Hadamard Matrices and Graphs4.7 Links to Coding Theory; 4.8 Bent Sequences; 4.9 Mobile Networks, CDMA; 4.10 Remarks; Chapter 5: Properties of Bent Functions; Introduction; 5.1 Degree of a Bent Function; 5.2 Affine Transformations of Bent Functions; 5.3 Rank of a Bent Function; 5.4 Dual Bent Functions; 5.5 Other Properties; Chapter 6: Equivalent Representations of Bent Functions; Introduction; 6.1 Hadamard Matrices; 6.2 Difference Sets; 6.3 Designs; 6.4 Linear Spreads; 6.5 Sets of Subspaces; 6.6 Strongly Regular Graphs; 6.7 Bent Rectangles
Chapter 7: Bent Functions with a Small Number of VariablesIntroduction; 7.1 Two and Four Variables; 7.2 Six Variables; 7.3 Eight Variables; 7.4 Ten and More Variables; 7.5 Algorithms for Generation of Bent Functions; 7.6 Concluding Remarks; Chapter 8: Combinatorial Constructions of Bent Functions; Introduction; 8.1 Rothaus's Iterative Construction; 8.2 Maiorana-McFarland Class; 8.3 Partial Spreads: PS+, PS-; 8.4 Dillon's Bent Functions: PSap; 8.5 Dobbertin's Construction; 8.6 More Iterative Constructions; 8.7 Minterm Iterative Constructions; 8.8 Bent Iterative Functions: BI
8.9 Other ConstructionsChapter 9: Algebraic Constructions of Bent Functions; Introduction; 9.1 An Algebraic Approach; 9.2 Bent Exponents: General Properties; 9.3 Gold Bent Functions; 9.4 Dillon Exponent; 9.5 Kasami Bent Functions; 9.6 Canteaut-Leander Bent Functions (MF-1); 9.7 Canteaut-Charpin-Kuyreghyan Bent Functions (MF-2); 9.8 Niho Exponents; 9.9 General Algebraic Approach; 9.10 Other Constructions; Chapter 10: Bent Functions and Other Cryptographic Properties; Introduction; 10.1 Cryptographic Criteria; 10.2 High Degree and Balancedness; 10.3 Correlation Immunity and Resiliency
10.4 Algebraic Immunity

Sommario/riassunto

Bent Functions: Results and Applications to Cryptography offers a unique survey of the objects of discrete mathematics known as Boolean bent functions. As these maximal, nonlinear Boolean functions and their generalizations have many theoretical and practical applications in combinatorics, coding theory, and cryptography, the text provides a detailed survey of their main results, presenting a systematic overview of their generalizations and applications, and considering open problems in classification and systematization of bent functions.    The text is appropriate for novices and advanced