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] ©2015
	ISBN	0-12-802555-7 0-12-802318-X
	Descrizione fisica	1 online resource (221 p.)
	Disciplina	511.324
	Soggetti	Computer security Data encryption (Computer science) 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 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

| 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 |

2.	Record Nr.	UNINA9910788886703321
	Autore	DeVore Ronald A.
	Titolo	Maximal functions measuring smoothness / / Ronald A. DeVore and Robert C. Sharpley
	Pubbl/distr/stampa	Providence, R.I., USA : , : American Mathematical Society, , [1984] ©1984
	ISBN	1-4704-0703-5
	Descrizione fisica	1 online resource (125 p.)
	Collana	Memoirs of the American Mathematical Society, , 0065-9266 ; ; number 293
	Disciplina	510 s
515.8/4
	Soggetti	Functions of several real variables
Smoothness of functions
Maximal functions
Sobolev spaces
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	"January 1984, volume 47, number 293 (fifth of six numbers)."
	Nota di bibliografia	Bibliography: pages 114-115.
	Nota di contenuto	""Table of Contents""; ""Glossary""; ""Section 1. Introduction""; ""Section 2. Maximal Functions""; ""Section 3. Inequalities For Polynomials""; ""Section 4. Additional Estimates""; ""Section 5. The Calderon Maximal Operator And Peano Derivatives""; ""Section 6. Smoothness Spaces""; ""Section 7. Comparisons With Besov Spaces""; ""Section 8. Interpolation""; ""Section 9. Embeddings""; ""Section 10. Extension Theorem""; ""Section 11. Extensions For Domains With Minimally Smooth Boundary""; ""Section 12. The Case $0 < p < 1$""; ""References""