1.	Record Nr.	UNINA9910483086803321
	Titolo	Applied Algebra, Algebraic Algorithms and Error-Correcting Codes : 17th International Symposium, AAECC-17, Bangalore, India, December 16-20, 2007, Proceedings / / edited by Serdar Boztas, Hsiao-feng Lu
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
	ISBN	3-540-77224-3
	Edizione	[1st ed. 2007.]
	Descrizione fisica	1 online resource (XII, 368 p.)
	Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 4851
	Disciplina	005.72
	Soggetti	Data structures (Computer science) Information theory Coding theory Cryptography Data encryption (Computer science) Computer science - Mathematics Discrete mathematics Algorithms Data Structures and Information Theory Coding and Information Theory Cryptology Discrete Mathematics in Computer Science Symbolic and Algebraic Manipulation
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	Invited Contributions -- List Decoding and Pseudorandom Constructions -- A Survey of Recent Attacks on the Filter Generator -- Iterative List Decoding of LDPC Codes -- Inverted Edwards Coordinates -- Spectra of Boolean Functions, Subspaces of Matrices, and Going Up Versus Going Down -- Efficient List Decoding of Explicit Codes with Optimal Redundancy -- Algebraic Structure Theory of Tail-Biting Trellises -- Nice Codes from Nice Curves -- Regular Contributions -- Generalized Sudan’s List Decoding for Order Domain Codes -- Bent

Functions and Codes with Low Peak-to-Average Power Ratio for Multi-Code CDMA -- Determining the Nonlinearity of a New Family of APN Functions -- An Improvement of Tardos’s Collusion-Secure Fingerprinting Codes with Very Short Lengths -- Space-Time Codes from Crossed Product Algebras of Degree 4 -- On Non-randomness of the Permutation After RC4 Key Scheduling -- Correctable Errors of Weight Half the Minimum Distance Plus One for the First-Order Reed-Muller Codes -- Fault-Tolerant Finite Field Computation in the Public Key Cryptosystems -- A Note on a Class of Quadratic Permutations over -- Constructions of Orthonormal Lattices and Quaternion Division Algebras for Totally Real Number Fields -- Quaternary Plotkin Constructions and Quaternary Reed-Muller Codes -- Joint Source-Cryptographic-Channel Coding Based on Linear Block Codes -- On the Key-Privacy Issue of McEliece Public-Key Encryption -- Lattices for Distributed Source Coding: Jointly Gaussian Sources and Reconstruction of a Linear Function -- Linear Complexity and Autocorrelation of Prime Cube Sequences -- The “Art of Trellis Decoding” Is NP-Hard -- On the Structure of Inversive Pseudorandom Number Generators -- Subcodes of Reed-Solomon Codes Suitable for Soft Decoding -- Normalized Minimum DeterminantCalculation for Multi-block and Asymmetric Space-Time Codes -- On the Computation of Non-uniform Input for List Decoding on Bezerra-Garcia Tower -- Dense MIMO Matrix Lattices — A Meeting Point for Class Field Theory and Invariant Theory -- Secure Cross-Realm Client-to-Client Password-Based Authenticated Key Exchange Against Undetectable On-Line Dictionary Attacks -- Links Between Discriminating and Identifying Codes in the Binary Hamming Space -- Construction of Rotation Symmetric Boolean Functions on Odd Number of Variables with Maximum Algebraic Immunity -- A Path to Hadamard Matrices -- The Tangent FFT -- Novel Algebraic Structure for Cyclic Codes -- Distribution of Trace Values and Two-Weight, Self-orthogonal Codes over GF(p,2) -- Generalized Rotation Symmetric and Dihedral Symmetric Boolean Functions ? 9 Variable Boolean Functions with Nonlinearity 242 -- On Quasi-cyclic Codes over Integer Residue Rings -- Extended Norm-Trace Codes with Optimized Correction Capability -- On Generalized Hamming Weights and the Covering Radius of Linear Codes -- Homomorphic Encryptions of Sums of Groups.

Sommario/riassunto

This book constitutes the refereed proceedings of the 17th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-17, held in Bangalore, India, in December 2007. The 33 revised full papers presented together with 8 invited papers were carefully reviewed and selected from 61 submissions. Among the subjects addressed are block codes, including list-decoding algorithms; algebra and codes: rings, fields, algebraic geometry codes; algebra: rings and fields, polynomials, permutations, lattices; cryptography: cryptanalysis and complexity; computational algebra: algebraic algorithms and transforms; sequences and boolean functions.