1. Record Nr. UNISA996466118503316

Titolo	Applied Algebra, Algebraic Algorithms and Error-Correcting Codes [[electronic resource]] : 16th International Symposium, AAECC-16, Las Vegas, NV, USA, February 20-24, 2006, Proceedings / / edited by Marc Fossorier, Hideki Imai, Shu Lin, Alain Poli
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-31424-5
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XII, 344 p.)
Collana	Theoretical Computer Science and General Issues, , 2512-2029 ; ; 3857
Disciplina	005.72
Soggetti	Coding theory Information theory Cryptography Data encryption (Computer science) Computer science—Mathematics Discrete mathematics Algorithms 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	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	On Bent and Highly Nonlinear Balanced/Resilient Functions and Their Algebraic Immunities -- On Generalized Parity Checks -- Cryptography Based on Bilinear Maps -- The Merit Factor Problem for Binary Sequences -- Quantum Period Reconstruction of Binary Sequences -- The Vector Key Equation and Multisequence Shift Register Synthesis -- A General Framework for Applying FGLM Techniques to Linear Codes -- A Theory of Highly Nonlinear Functions -- The Solutions of the Third Power Sum Equation for Niho Type Decimations -- On Constructing AG Codes Without Basis Functions for Riemann-Roch Spaces -- Computing Gröbner Bases for Vanishing Ideals of Finite Sets of Points -- A Class of

Fermat Curves for which Weil-Serre's Bound Can Be Improved -- Nonbinary Quantum Codes from Hermitian Curves -- A Genetic Algorithm for Cocyclic Hadamard Matrices -- Unconditionally Secure Chaffing-and-Winnowing: A Relationship Between Encryption and Authentication -- A Fast Calculus for the Linearizing Attack and Its Application to an Attack on KASUMI -- On Achieving Chosen Ciphertext Security with Decryption Errors -- Applying Fujisaki-Okamoto to Identity-Based Encryption -- A Short Random Fingerprinting Code Against a Small Number of Pirates -- A General Formulation of Algebraic and Fast Correlation Attacks Based on Dedicated Sample Decimation -- Traitor Tracing Against Powerful Attacks Using Combinatorial Designs -- New Bounds on the Capacity of Multi-dimensional RLL-Constrained Systems -- LDPC Codes for Fading Channels: Two Strategies -- Low-Floor Tanner Codes Via Hamming-Node or RSCC-Node Doping -- Algebraic Constructions of Quasi-cyclic LDPC Codes – Part I: For AWGN and Binary Random Erasure Channels -- Algebraic Construction of Quasi-cyclic LDPC Codes – Part II: For AWGN and Binary Random and Burst Erasure Channels -- New Constructions of Quasi-cyclic LDPC Codes Based on Two Classes of Balanced Incomplete Block Designs: For AWGN and Binary Erasure Channels -- Long Extended BCH Codes Are Spanned by Minimum Weight Words -- On the Feng-Rao Bound for Generalized Hamming Weights -- Nested Codes for Constrained Memory and for Dirty Paper -- Complementary Sets and Reed-Muller Codes for Peak-to-Average Power Ratio Reduction in OFDM -- Hadamard Codes of Length 2 t s (s Odd). Rank and Kernel.