1.	Record Nr.	UNINA9910144030303321
	Titolo	Applied Algebra, Algebraic Algorithms and Error-Correcting Codes : 15th International Symposium, AAECC-15, Toulouse, France, May 12-16, 2003, Proceedings / / edited by Marc Fossorier, Tom Hoeholdt, Alain Poli
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003
	ISBN	3-540-44828-4
	Edizione	[1st ed. 2003.]
	Descrizione fisica	1 online resource (X, 270 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2643
	Disciplina	005.7/2
	Soggetti	Algebra Coding theory Information theory Data encryption (Computer science) Algorithms Computer science—Mathematics Coding and Information Theory Cryptology Algorithm Analysis and Problem Complexity 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	Cryptography and the Methodology of Provable Security -- Dynamical Systems Generated by Rational Functions -- Homotopy Methods for Equations over Finite Fields -- Three Constructions of Authentication/Secrecy Codes -- The Jacobi Model of an Elliptic Curve and Side-Channel Analysis -- Fast Point Multiplication on Elliptic Curves through Isogenies -- Interpolation of the Elliptic Curve Diffie-Hellman Mapping -- An Optimized Algebraic Method for Higher Order Differential Attack -- Fighting Two Pirates -- Copyright Control and Separating Systems -- Unconditionally Secure Homomorphic Pre-distributed Commitments -- A Class of Low-Density Parity-Check

Codes Constructed Based on Reed-Solomon Codes with Two Information Symbols -- Relative Duality in MacWilliams Identity -- Good Expander Graphs and Expander Codes: Parameters and Decoding -- On the Covering Radius of Certain Cyclic Codes -- Unitary Error Bases: Constructions, Equivalence, and Applications -- Differentially 2-Uniform Cocycles — The Binary Case -- The Second and Third Generalized Hamming Weights of Algebraic Geometry Codes -- Error Correcting Codes over Algebraic Surfaces -- A Geometric View of Decoding AG Codes -- Performance Analysis of M-PSK Signal Constellations in Riemannian Varieties -- Improvements to Evaluation Codes and New Characterizations of Arf Semigroups -- Optimal 2-Dimensional 3-Dispersion Lattices -- On g-th MDS Codes and Matroids -- On the Minimum Distance of Some Families of ?2 k-Linear Codes -- Quasicyclic Codes of Index ? over F q Viewed as F q[x]-Submodules of F q ?[x]/?x m?1? -- Fast Decomposition of Polynomials with Known Galois Group.

Sommario/riassunto

This book constitutes the refereed proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-15, held in Toulouse, France, in May 2003.The 25 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 40 submissions. Among the subjects addressed are block codes; algebra and codes: rings, fields, and AG codes; cryptography; sequences; decoding algorithms; and algebra: constructions in algebra, Galois groups, differential algebra, and polynomials.