

- | | |
|-------------------------|--|
| 1. Record Nr. | UNINA990006424920403321 |
| Titolo | Dix-huitième siècle : revue annuelle / publiée par la Société française d'étude du 18. siècle avec le concours du C.N.R.S. |
| Pubbl/distr/stampa | Paris : Garnier Frères, 1969 |
| Descrizione fisica | v. ; 22 cm |
| Disciplina | 944.005 |
| Locazione | DFD |
| Collocazione | XI C AAVV 125
XI C AAVV 126 |
| Lingua di pubblicazione | Francese |
| Formato | Materiale a stampa |
| Livello bibliografico | Periodico |
-
- | | |
|------------------------|---|
| 2. Record Nr. | UNINA9910484968703321 |
| Titolo | Applied Algebra, Algebraic Algorithms and Error-Correcting Codes : 18th International Symposium, AAecc-18, Tarragona, Sapin, June 8-12, 2009, Proceedings // edited by Maria Bras-Amorós, Tom Høholdt |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009 |
| ISBN | 3-642-02181-6 |
| Edizione | [1st ed. 2009.] |
| Descrizione fisica | 1 online resource (IX, 243 p.) |
| Collana | Theoretical Computer Science and General Issues, , 2512-2029 ; ; 5527 |
| Classificazione | DAT 465f
DAT 584f
DAT 702f
MAT 110f
SS 4800 |
| Altri autori (Persone) | Bras-AmarosMaria
HøholdtTom |
| Disciplina | 005.72 |
| Soggetti | Coding theory
Information theory
Cryptography
Data encryption (Computer science)
Computer science - Mathematics
Discrete mathematics
Data structures (Computer science) |

Algorithms
Coding and Information Theory
Cryptology
Discrete Mathematics in Computer Science
Symbolic and Algebraic Manipulation
Data Structures and Information Theory

Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	<p>Codes -- The Order Bound for Toric Codes -- An Extension of the Order Bound for AG Codes -- Sparse Numerical Semigroups -- From the Euclidean Algorithm for Solving a Key Equation for Dual Reed–Solomon Codes to the Berlekamp–Massey Algorithm -- Rank for Some Families of Quaternary Reed-Muller Codes -- Optimal Bipartite Ramanujan Graphs from Balanced Incomplete Block Designs: Their Characterizations and Applications to Expander/LDPC Codes -- Simulation of the Sum-Product Algorithm Using Stratified Sampling -- A Systems Theory Approach to Periodically Time-Varying Convolutional Codes by Means of Their Invariant Equivalent -- On Elliptic Convolutional Goppa Codes -- The Minimum Hamming Distance of Cyclic Codes of Length $2p^s$ -- There Are Not Non-obvious Cyclic Affine-invariant Codes -- On Self-dual Codes over \mathbb{Z}_{16} -- Cryptography -- A Non-abelian Group Based on Block Upper Triangular Matrices with Cryptographic Applications -- Word Oriented Cascade Jump ??LFSR -- On Some Sequences of the Secret Pseudo-random Index j in RC4 Key Scheduling -- Very-Efficient Anonymous Password-Authenticated Key Exchange and Its Extensions -- Efficient Constructions of Deterministic Encryption from Hybrid Encryption and Code-Based PKE -- Algebra -- Noisy Interpolation of Multivariate Sparse Polynomials in Finite Fields -- New Commutative Semifields and Their Nuclei -- Spreads in Projective Hjelmslev Geometries -- On the Distribution of Nonlinear Congruential Pseudorandom Numbers of Higher Orders in Residue Rings -- Rooted Trees Searching for Cocyclic Hadamard Matrices over \mathbb{D}_{4t} -- Extended Abstracts -- Interesting Examples on Maximal Irreducible Goppa Codes -- Repeated Root Cyclic and Negacyclic Codes over Galois Rings -- Construction of Additive Reed-Muller Codes -- Gröbner Representations of Binary Matroids -- A Generalization of the Zig-Zag Graph Product by Means of the Sandwich Product -- Novel Efficient Certificateless Aggregate Signatures -- Bounds on the Number of Users for Random 2-Secure Codes.</p>
Sommario/riassunto	<p>This book constitutes the refereed proceedings of the 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAEECC-18, held in Tarragona, Spain, in June 2009. The 22 revised full papers presented together with 7 extended abstracts were carefully reviewed and selected from 50 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.</p>

