1.	Record Nr.	UNINA9910143614503321
	Titolo	Cryptography and coding : 7th ima conference, cirencester, uk, december 20-22, 1999 : proceedings / / edited by Michael, Jr. Walker
	Pubbl/distr/stampa	Berlin, Germany : , : Springer, , [1999] Â©1999
	ISBN	3-540-46665-7
	Edizione	[1st ed. 1999.]
	Descrizione fisica	1 online resource (X, 352 p.)
	Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1746
	Disciplina	003.54
	Soggetti	Coding theory
	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	Applications of Exponential Sums in Communications Theory -- Some Applications of Bounds for Designs to the Cryptography -- Further Results on the Relation Between Nonlinearity and Resiliency for Boolean Functions -- Combinatorial Structure of Finite Fields with Two Dimensional Modulo Metrics? -- A New Method for Generating Sets of Orthogonal Sequences for a Synchronous CDMA System -- New Self-Dual Codes over GF(5) -- Designs, Intersecting Families, and Weight of Boolean Functions -- Coding Applications in Satellite Communication Systems [Invited Paper] -- A Unified Code -- Enhanced Image Coding for Noisy Channels -- Perfectly Secure Authorization and Passive Identification for an Error Tolerant Biometric System -- An Encoding Scheme for Dual Level Access to Broadcasting Networks -- Photograph Signatures for the Protection of Identification Documents -- An Overview of the Isoperimetric Method in Coding Theory (Extended Abstract) [Invited Paper] -- Rectangular Basis of a Linear Code -- Graph Decoding of Array Error-Correcting Codes -- Catastrophicity Test for Time-Varying Convolutional Encoders -- Low Complexity Soft-Decision Sequential Decoding Using Hybrid Permutation for Reed-Solomon Codes -- On Efficient Decoding of Alternant Codes over a Commutative Ring? -- Reduced Complexity Sliding Window BCJR Decoding Algorithms for Turbo Codes -- Advanced Encryption Standard (AES) - An Update [Invited Paper] -- The Piling-Up Lemma and Dependent Random Variables -- A Cryptographic Application of Weil Descent --

Edit Probability Correlation Attack on the Bilateral Stop/Go Generator -- Look-Up Table Based Large Finite Field Multiplication in Memory Constrained Cryptosystems (Extended Abstract) -- On the Combined Fermat/Lucas Probable Prime Test? -- On the Cryptanalysis of Nonlinear Sequences [Invited Paper] -- Securing Aeronautical Telecommunications [Invited Paper] -- Tensor-Based Trapdoors for CVP and Their Application to Public Key Cryptography (Extended Abstract) -- Delegated Decryption -- Fast and Space-Efficient Adaptive Arithmetic Coding? -- Robust Protocol for Generating Shared RSA Parameters -- Some Soft-Decision Decoding Algorithms for Reed-Solomon Codes -- Weaknesses in Shared RSA Key Generation Protocols -- Digital Signature with Message Recovery and Authenticated Encryption (Signcryption) - A Comparison.