1.	Record Nr.	UNISA996465845203316
	Titolo	Coding and Cryptology [[electronic resource]] : Second International Workshop, IWCC 2009 / / edited by Yeow Meng Chee, Chao Li, San Ling, Huaxiong Wang, Chaoping Xing
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
	ISBN	3-642-01877-7
	Edizione	[1st ed. 2009.]
	Descrizione fisica	1 online resource (VIII, 275 p.)
	Collana	Security and Cryptology ; ; 5557
	Classificazione	DAT 465f DAT 580f SS 4800
	Disciplina	005.82
	Soggetti	Data encryption (Computer science) Coding theory Information theory Computer science—Mathematics Computer communication systems Cryptology Coding and Information Theory Discrete Mathematics in Computer Science Computer Communication Networks Kongress. Zhangjiajie (2009)
	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	An Infinite Class of Balanced Vectorial Boolean Functions with Optimum Algebraic Immunity and Good Nonlinearity -- Separation and Witnesses -- Binary Covering Arrays and Existentially Closed Graphs -- A Class of Three-Weight and Four-Weight Codes -- Equal-Weight Fingerprinting Codes -- Problems on Two-Dimensional Synchronization Patterns -- A New Client-to-Client Password-Authenticated Key Agreement Protocol -- Elliptic Twin Prime Conjecture -- Hunting for Curves with Many Points -- List Decoding of Binary Codes–A Brief Survey of Some Recent

Results -- Recent Developments in Low-Density Parity-Check Codes -- On the Applicability of Combinatorial Designs to Key Predistribution for Wireless Sensor Networks -- On Weierstrass Semigroups of Some Triples on Norm-Trace Curves -- ERINDALE: A Polynomial Based Hashing Algorithm -- A Survey of Algebraic Unitary Codes -- New Family of Non-Cartesian Perfect Authentication Codes -- On the Impossibility of Strong Encryption Over -- Minimum Distance between Bent and Resilient Boolean Functions -- Unconditionally Secure Approximate Message Authentication -- Multiplexing Realizations of the Decimation-Hadamard Transform of Two-Level Autocorrelation Sequences -- On Cayley Graphs, Surface Codes, and the Limits of Homological Coding for Quantum Error Correction.

Sommario/riassunto

This book constitutes the refereed proceedings of the Second International Workshop on Coding and Cryptology, IWCC 2009, held in Zhangjiajie, China, in June 2009. The 21 revised full technical papers, except one, are contributed by the invited speakers of the workshop. The papers were carefully selected during two rounds of reviewing and improvement for inclusion in the volume and address all aspects of coding theory, cryptology and related areas - such as combinatorics - theoretical or applied. Topics addressed are coding theory, secure codes, hash functions, combinatorics, boolean functions, authentication, cryptography, protocols, sequences, and secure communications.