1.	Record Nr.	UNINA9910484972303321
	Titolo	Coding and Cryptography : International Workshop, WCC 2005, Bergen, Norway, March 14-18, 2005, Revised Selected Papers / / edited by Øyvind Ytrehus
	Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
	ISBN	3-540-35482-4
	Edizione	[1st ed. 2006.]
	Descrizione fisica	1 online resource (XII, 444 p.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 3969
	Altri autori (Persone)	Ytrehusyvind
	Disciplina	005.8
	Soggetti	Coding theory Information theory Cryptography Data encryption (Computer science) Computer science - Mathematics Discrete mathematics Computer networks Coding and Information Theory Cryptology Discrete Mathematics in Computer Science Computer Communication Networks
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	"International Workshop on Coding and Cryptography (WCC 2005) held in Bergen, Norway, March 14-18, 2005"--Pref.
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Second Support Weights for Binary Self-dual Codes -- On Codes Correcting Symmetric Rank Errors -- Error and Erasure Correction of Interleaved Reed–Solomon Codes -- A Welch–Berlekamp Like Algorithm for Decoding Gabidulin Codes -- On the Weights of Binary Irreducible Cyclic Codes -- 3-Designs from Z 4-Goethals-Like Codes and Variants of Cyclotomic Polynomials -- Space-Time Code Designs Based on the Generalized Binary Rank Criterion with Applications to Cooperative Diversity -- Geometric Conditions for the Extendability of Ternary Linear Codes -- On the Design of Codes for DNA Computing -- Open Problems Related to Algebraic Attacks on Stream Ciphers -- On the

Non-linearity and Sparsity of Boolean Functions Related to the Discrete Logarithm in Finite Fields of Characteristic Two -- Interpolation of Functions Related to the Integer Factoring Problem -- On Degrees of Polynomial Interpolations Related to Elliptic Curve Cryptography -- Finding Good Differential Patterns for Attacks on SHA-1 -- Extending Gibson’s Attacks on the GPT Cryptosystem -- Reduction of Conjugacy Problem in Braid Groups, Using Two Garside Structures -- A New Key Assignment Scheme for Access Control in a Complete Tree Hierarchy -- Multi-Dimensional Hash Chains and Application to Micropayment Schemes -- On the Affine Transformations of HFE-Cryptosystems and Systems with Branches -- Dimension of the Linearization Equations of the Matsumoto-Imai Cryptosystems -- RSA-Based Secret Handshakes -- On a Relation Between Verifiable Secret Sharing Schemes and a Class of Error-Correcting Codes -- ID-Based Series-Parallel Multisignature Schemes for Multi-Messages from Bilinear Maps -- A New Public-Key Cryptosystem Based on the Problem of Reconstructing p–Polynomials -- On the Wagner–Magyarik Cryptosystem -- Constructions ofComplementary Sequences for Power-Controlled OFDM Transmission -- A Novel Method for Constructing Almost Perfect Polyphase Sequences -- Linear Filtering of Nonlinear Shift-Register Sequences -- Realizations from Decimation Hadamard Transform for Special Classes of Binary Sequences with Two-Level Autocorrelation -- Frequency/Time Hopping Sequences with Large Linear Complexities -- One and Two-Variable Interlace Polynomials: A Spectral Interpretation -- Improved Bounds on Weil Sums over Galois Rings and Homogeneous Weights -- Locally Invertible Multivariate Polynomial Matrices.

Sommario/riassunto

Thisvolumecontainsrefereedpapersdevotedtocodingandcryptography. These papers arethe full versionsof a selectionof the best extended abstractsaccepted for presentation at the International Workshop on Coding and Cryptography (WCC 2005) held in Bergen, Norway, March 14–18, 2005. Each of the 118 - tended abstracts originallysubmitted to the workshop were reviewed by at least two members of the Program Committee. As a result of this screening process, 58 papers were selected for presentation, of which 52 were eventually presented at the workshop together with four invited talks. The authors of the presented papers were in turn invited to submit full v- sions of their papers to the full proceedings. Each of the full-version submissions were once again thoroughly examined and commented upon by at least two reviewers. This volume is the end result of this long process. I am grateful to the reviewers who contributed to guaranteeing the high standards of this volume, and who are named on the next pages. It was a pl- sure for me to work with my program co-chair Pascale Charpin, whose expe- enced advice I havefurther bene?ted greatly from during the preparationof this ´ volume. Discussions with Tor Helleseth and Angela Barbero were also useful in putting the volume together. Finally, I would like to thank all the authors and all the other participants of the WCC 2005 for making it in every sense a highly enjoyable event.