<<   >>

<<   >>

13   ISBN   9783540354819

10   ISBN   3540354816

2006-12

Ytrehus, Xyvind; Ytrehus, Cyvind; Ytrehus, Yvind

441

PDF

This book constitutes the thoroughly refereed post-proceedings of the International Workshop on Coding and Cryptography, WCC 2005, held in Bergen, Norway, in March 2005. The 33 revised full papers were carefully reviewed and selected during two rounds of reviewing and improvement from 118 submissions. The papers address all aspects of coding theory, cryptography and related areas, theoretical or applied. Topics covered are: coding theory, i.e., error-correcting codes, decoding algorithms, and related combinatorial problems; cryptology, i.e., block and stream ciphers, hash functions, public key cryptography, secret sharing, authentication, and intellectual property protection; and discrete mathematics and algorithmic tools arising from these two areas, such as boolean functions, sequences, finite fields, algebraic systems and related polynomial properties.

Second Support Weights for Binary Self-dual CodesOn Codes Correcting Symmetric Rank ErrorsError and Erasure Correction of Interleaved Reed-Solomon CodesA Welch Berlekamp Like Algorithm for Decoding Gabidulin CodesOn the Weights of Binary Irreducible Cyclic Codes3-Designs from Z4-Goethals-Like Codes and Variants of Cyclotomic PolynomialsSpace-Time Code Designs Based on the Generalized Binary RankCriterion with Applications to Cooperative DiversityGeometric Conditions for the Extendability of Ternary Linear CodesOn the Design of Codes for DNA ComputingOpen Problems Related to Algebraic Attacks on Stream CiphersOn the Non-linearity and Sparsity of Boolean Functions Related to the Discrete Logarithm in Finite Fields of Characteristic TwoInterpolation of Functions Related to the Integer Factoring ProblemOn Degrees of Polynomial Interpolations Related to Elliptic Curve CryptographyFinding Good Differential Patterns for Attacks on SHA-1Extending Gibson's Attacks on the GPT CryptosystemReduction of Conjugacy Problem in Braid Groups, Using Two GarsideStructuresA New Key Assignment Scheme for Access Control in a Complete Tree HierarchyMulti-Dimensional Hash Chains and Application to Micropayment SchemesOn the Affine Transformations of HFE-Cryptosystems and Systems with BranchesDimension of the Linearization Equations of the Matsumoto-Imai CryptosystemsRSA-Based Secret HandshakesOn a Relation Between Verifiable Secret Sharing Schemes and a Class of Error-Correcting CodesID-Based Series-Parallel Multisignature Schemes for Multi-Messages from Bilinear MapsA New Public-Key Cryptosystem Based on the Problem of Reconstructing o-PolynomialsOn the Wagner Magyarik Cryptosystem……Author Index

<<   >>

PDF