

<<编码与密码术>>

图书基本信息

书名：<<编码与密码术>>

13位ISBN编号：9783540354819

10位ISBN编号：3540354816

出版时间：2006-12

出版时间：湖北辞书出版社

作者：Ytrehus, Xyvind; Ytrehus, Cyvind; Ytrehus, Yvind

页数：441

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

内容概要

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.

书籍目录

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 o -Polynomials
On the Wagner Magyarik Cryptosystem.....
Author Index

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>