1. Record Nr. UNISA996465914303316

Titolo	Cryptography and Coding [[electronic resource]] : 12th IMA International Conference, IMACC 2009, Cirencester, UK, December 15-17, 2009, Proceedings / / edited by Matthew G. Parker
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-10868-7
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XI, 495 p.)
Collana	Security and Cryptology ; ; 5921
Classificazione	DAT 465f DAT 580f SS 4800
Disciplina	512
Soggetti	Data encryption (Computer science) Coding theory Information theory Computer science—Mathematics Data structures (Computer science) Computer security Cryptology Coding and Information Theory Symbolic and Algebraic Manipulation Data Structures and Information Theory Systems and Data Security Discrete Mathematics in Computer Science Cirencester (2009) Kongress.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	International conference proceedings.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Coding Theory -- Subspace Codes -- On Linear Programming Decoding on a Quantized Additive White Gaussian Noise Channel -- Codes as Modules over Skew Polynomial Rings -- On Higher Weights and Code Existence -- Mass Formula for Even Codes over -- On the Classification of Self-dual -Codes -- On Linear Codes from Maximal

Curves -- Symmetric Cryptography -- On Linear Cryptanalysis with Many Linear Approximations -- Bivium as a Mixed-Integer Linear Programming Problem -- Security of Cyclic Double Block Length Hash Functions -- Another Glance at Double-Length Hashing -- Geometric Ideas for Cryptographic Equation Solving in Even Characteristic -- Security Protocols -- Provably Secure Code-Based Threshold Ring Signatures -- A New Protocol for the Nearby Friend Problem -- Distributing the Key Distribution Centre in Sakai–Kasahara Based Systems -- Key Predistribution Schemes and One-Time Broadcast Encryption Schemes from Algebraic Geometry Codes -- Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes -- Certificate-Free Attribute Authentication -- Asymmetric Cryptography -- Comparing with RSA -- Double-Exponentiation in Factor-4 Groups and Its Applications -- Oracle-Assisted Static Diffie-Hellman Is Easier Than Discrete Logarithms -- An Improvement to the Gaudry-Schost Algorithm for Multidimensional Discrete Logarithm Problems -- Boolean Functions -- On Designs and Multiplier Groups Constructed from Almost Perfect Nonlinear Functions -- A New Family of Hyper-Bent Boolean Functions in Polynomial Form -- The Rayleigh Quotient of Bent Functions -- Side Channels and Implementations -- Cache Timing Analysis of LFSR-Based Stream Ciphers -- Optimal Recovery of Secret Keys from Weak Side Channel Traces -- Practical Zero-Knowledge Proofs for Circuit Evaluation.

Sommario/riassunto

This book constitutes the refereed proceedings of the 12th IMA International Conference on Cryptography and Coding, held in Cirencester, UK in December 2009. The 26 revised full papers presented together with 3 invited contributions were carefully reviewed and selected from 53 submissions. The papers are organized in topical sections on coding theory, symmetric cryptography, security protocols, asymmetric cryptography, Boolean functions and side channels and implementations.