1. Record Nr. UNISA996465794603316

| | |
|---|---|
| Titolo | Cryptography and Coding [[electronic resource] ] : 9th IMA International Conference, Cirencester, UK, December 16-18, 2003, Proceedings / / edited by Kenneth G. Paterson |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003 |
| ISBN | 3-540-40974-2 |
| Edizione | [1st ed. 2003.] |
| Descrizione fisica | 1 online resource (X, 390 p.) |
| Collana | Lecture Notes in Computer Science, , 0302-9743 ; ; 2898 |
| Disciplina | 005.8/2 |
| Soggetti | Data encryption (Computer science)<br>Coding theory<br>Information theory<br>Computer science<br>Computer communication systems<br>Computer science—Mathematics<br>Cryptology<br>Coding and Information Theory<br>Computer Science, general<br>Computer Communication Networks<br>Discrete Mathematics in Computer Science |
| 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 at the end of each chapters and index. |
| Nota di contenuto | Coding and Applications -- Recent Developments in Array Error-Control Codes -- High Rate Convolutional Codes with Optimal Cycle Weights -- A Multifunctional Turbo-Based Receiver Using Partial Unit Memory Codes -- Commitment Capacity of Discrete Memoryless Channels -- Separating and Intersecting Properties of BCH and Kasami Codes -- Applications of Coding in Cryptography -- Analysis and Design of Modern Stream Ciphers -- Improved Fast Correlation Attack Using Low Rate Codes -- On the Covering Radius of Second Order Binary Reed-Muller Code in the Set of Resilient Boolean Functions -- Degree Optimized Resilient Boolean Functions from Maiorana- |

McFarland Class -- Differential Uniformity for Arrays -- Cryptography -- Uses and Abuses of Cryptography -- A Designer's Guide to KEMs -- A General Construction of IND-CCA2 Secure Public Key Encryption -- Efficient Key Updating Signature Schemes Based on IBS -- Periodic Sequences with Maximal Linear Complexity and Almost Maximal k-Error Linear Complexity -- Cryptanalysis -- Estimates for Discrete Logarithm Computations in Finite Fields of Small Characteristic -- Resolving Large Prime(s) Variants for Discrete Logarithm Computation -- Computing the M = UU t Integer Matrix Decomposition -- Cryptanalysis of the Public Key Cryptosystem Based on the Word Problem on the Grigorchuk Groups -- More Detail for a Combined Timing and Power Attack against Implementations of RSA -- Predicting the Inversive Generator -- A Stochastical Model and Its Analysis for a Physical Random Number Generator Presented At CHES 2002 -- Analysis of Double Block Length Hash Functions -- Network Security and Protocols -- Cryptography in Wireless Standards -- On the Correctness of Security Proofs for the 3GPP Confidentiality and Integrity Algorithms -- A General Attack Model on Hash-Based Client Puzzles -- Tripartite Authenticated Key Agreement Protocols from Pairings -- Remote User Authentication Using Public Information -- Mental Poker Revisited.

Sommario/riassunto

The ninth in the series of IMA Conferences on Cryptography and Coding was held (as ever) at the Royal Agricultural College, Cirencester, from 16–18 Dec- ber 2003. The conference's varied programme of 4 invited and 25 contributed papers is represented in this volume. The contributed papers were selected from the 49 submissions using a - reful refereeing process. The contributed and invited papers are grouped into 5 topics: coding and applications; applications of coding in cryptography; cryptography; cryptanalysis; and network security and protocols. These topic headings represent the breadth of activity in the areas of coding, cryptography and communications, and the rich interplay between these areas.
Assemblingtheconferenceprogrammeandthisproceedingsrequiredthehel p of many individuals. I would like to record my appreciation of them here. Firstly, I would like to thank the programme committee who aided me immensely by evaluating the submissions, providing detailed written feedback for the authors of many of the papers, and advising me at many critical points - ring the process. Their help and cooperation was essential, especially in view of the short amount of time available to conduct the reviewing task. The committee this year consisted of Mike Darnell, Mick Ganley, Bahram Honary, Chris Mitchell, Matthew Parker, Nigel Smart and Mike Walker.