1. Record Nr. UNINA9910483738203321

Titolo	Cryptography and Coding : 10th IMA International Conference, Cirencester, UK, December 19-21, 2005, Proceedings / / edited by Nigel Smart
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XII, 468 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 3796
Altri autori (Persone)	SmartNigel P <1967-> (Nigel Paul)
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Computer science Coding theory Information theory Computer science - Mathematics Discrete mathematics Computer networks Cryptology Theory of Computation Coding and Information Theory Discrete Mathematics in Computer Science Computer Communication Networks
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 and index.
Nota di contenuto	Invited Papers -- Abstract Models of Computation in Cryptography -- Pairing-Based Cryptography at High Security Levels -- Improved Decoding of Interleaved AG Codes -- Coding Theory -- Performance Improvement of Turbo Code Based on the Extrinsic Information Transition Characteristics -- A Trellis-Based Bound on (2,1)-Separating Codes -- Tessellation Based Multiple Description Coding -- Exploiting Coding Theory for Collision Attacks on SHA-1 -- Signatures and Signcryption -- Hash Based Digital Signature Schemes -- A General

Construction for Simultaneous Signing and Encrypting -- Non-interactive Designated Verifier Proofs and Undeniable Signatures -- Symmetric Cryptography -- Partial Key Recovery Attacks on XCBC, TMAC and OMAC -- Domain Expansion of MACs: Alternative Uses of the FIL-MAC -- Normality of Vectorial Functions -- Related-Key Differential Attacks on Cobra-H64 and Cobra-H128 -- Side Channels -- The Physically Observable Security of Signature Schemes -- On the Automatic Construction of Indistinguishable Operations -- Efficient Countermeasures for Thwarting the SCA Attacks on the Frobenius Based Methods -- Algebraic Cryptanalysis -- Complexity Estimates for the F 4 Attack on the Perturbed Matsumoto-Imai Cryptosystem -- An Algebraic Framework for Cipher Embeddings -- Probabilistic Algebraic Attacks -- Information Theoretic Applications -- Unconditionally Secure Information Authentication in Presence of Erasures -- Generalized Strong Extractors and Deterministic Privacy Amplification -- On Threshold Self-healing Key Distribution Schemes -- Number Theoretic Foundations -- Concrete Security of the Blum-Blum-Shub Pseudorandom Generator -- The Equivalence Between the DHP and DLP for Elliptic Curves Used in Practical Applications, Revisited -- Pairings on Elliptic Curves over Finite Commutative Rings -- Public Key and ID-Based Encryption Schemes -- A Key Encapsulation Mechanism for NTRU -- Efficient Identity-Based Key Encapsulation to Multiple Parties -- Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme.

Sommario/riassunto

The10thintheseriesofIMAConferencesonCryptographyandCodingwashel d at the RoyalAgricultural College, Cirencester, during 19-21 December 2005. As usual, the venue provided a relaxed and informal atmosphere for attendees to discuss work and listen to the collection of talks. The program consisted of four invited talks and 26 contributed talks. The invitedtalkswheregivenbyTuviEtzion,UeliMaurer,AlfredMenezesandAmin Shokrollahi, and three of these invited talks appear as papers in this volume. Special thanks must go to these four speakers as they helped to set the tone, by coveringall the areasthe meeting aimed to cover, from cryptographythrough to coding. In addition the best speakers are often the hardest to persuade to come to a meeting, as they are usually the most busy. We therefore feel privileged to have had a meeting with four such distinguished speakers. The contributed talks were selected from 94 submissions. This is nearly twice thenumberofsubmissionsforthepreviousmeetingin2003. Thisisanindication of the strength of the subject and the interest in the IMA series of meetings as a venue to present new work. The contributed talks ranged over a wide number of areas, including information theory, coding theory, number theory and as- metric and symmetric cryptography. Subtopics included a number of current "hot topics," such as algebraic cryptanalysis and cryptographic systems based on bilinear pairings. Assembling the conference program and these proceedings required the help of a large number of individuals. I would like to thank them all here.