1. Record Nr. UNISA996465293103316

Titolo	Cryptography and Coding [[electronic resource]] : 8th IMA International Conference Cirencester, UK, December 17-19, 2001 Proceedings / / edited by Bahram Honary
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2001
ISBN	3-540-45325-3
Edizione	[1st ed. 2001.]
Descrizione fisica	1 online resource (IX, 419 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2260
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Computers Coding theory Information theory Computer science—Mathematics Computer communication systems Management information systems Computer science Cryptology Theory of Computation Coding and Information Theory Discrete Mathematics in Computer Science Computer Communication Networks Management of Computing and Information Systems
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	A Statistical Decoding Algorithm for General Linear Block Codes -- On the Undetected Error Probability for Shortened Hamming Codes on Channels with Memory -- The Complete Weight Enumerator for Codes over M nxs(F q) -- Further Improvement of Kumar-Rajagopalan-Sahai Coding Constructions for Blacklisting Problem -- A Simple Soft-Input/Soft-Output Decoder for Hamming Codes -- A Technique with an

Information-Theoretic Basis for Protecting Secret Data from Differential Power Attacks -- Key Recovery Attacks on MACs Based on Properties of Cryptographic APIs -- The Exact Security of ECIES in the Generic Group Model -- A New Ultrafast Stream Cipher Design: COS Ciphers -- On Rabin-Type Signatures -- Strong Adaptive Chosen-Ciphertext Attacks with Memory Dump (or: The Importance of the Order of Decryption and Validation) -- Majority-Logic-Decodable Cyclic Arithmetic-Modular AN-Codes in 1, 2, and L Steps -- Almost-Certainly Runlength-Limiting Codes -- Weight vs. Magnetization Enumerator for Gallager Codes -- Graph Configurations and Decoding Performance -- A Line Code Construction for the Adder Channel with Rates Higher than Time-Sharing -- The Synthesis of TD-Sequences and Their Application to Multi-functional Communication Systems -- Improvement of the Delsarte Bound for ?-Designs in Finite Polynomial Metric Spaces -- Statistical Properties of Digital Piecewise Linear Chaotic Maps and Their Roles in Cryptography and Pseudo-Random Coding -- The Wide Trail Design Strategy -- Undetachable Threshold Signatures -- Improving Divide and Conquer Attacks against Cryptosystems by Better Error Detection / Correction Strategies -- Key Recovery Scheme Interoperability - A Protocol for Mechanism Negotiation -- Unconditionally Secure Key Agreement Protocol -- An Efficient Stream Cipher Alpha1 for Mobile and Wireless Devices -- Investigation of Linear Codes Possessing Some Extra Properties -- Statistical Physics of Low Density Parity Check Error Correcting Codes -- Generating Large Instances of the Gong-Harn Cryptosystem -- Lattice Attacks on RSA-Encrypted IP and TCP -- Spectrally Bounded Sequences, Codes, and States: Graph Constructions and Entanglement -- Attacking the Affine Parts of SFLASH -- An Identity Based Encryption Scheme Based on Quadratic Residues -- Another Way of Doing RSA Cryptography in Hardware -- Distinguishing TEA from a Random Permutation: Reduced Round Versions of TEA Do Not Have the SAC or Do Not Generate Random Numbers -- A New Search Pattern in Multiple Residue Method (MRM) and Its Importance in the Cryptanalysis of the RSA -- A New Undeniable Signature Scheme Using Smart Cards -- Non-binary Block Inseparable Errors Control Codes -- Cryptanalysis of Nonlinear Filter Generators with (0, 1)-Metric Viterbi Decoding.

Sommario/riassunto

The mathematical theory and practice of cryptography and coding underpins the provision of effective security and reliability for data communication, processing, and storage. Theoretical and implementational advances in the fields of cryptography and coding are therefore a key factor in facilitating the growth of data communications and data networks of various types. Thus, this Eight International Conference in an established and successful IMA series on the theme of “Cryptography and Coding” was both timely and relevant. The theme of this conference was the future of coding and cryptography, which was touched upon in presentations by a number of invited speakers and researchers. The papers that appear in this book include recent research and development in error control coding and cryptography. These start with mathematical bounds, statistical decoding schemes for error correcting codes, and undetected error probabilities and continue with the theoretical aspects of error correction coding such as graph and trellis decoding, multifunctional and multiple access communication systems, low density parity check codes, and iterative decoding. These are followed by some papers on key recovery attack, authentication, stream cipher design, and analysis of ECIES algorithms, and lattice attacks on IP based protocols.