1. Record Nr. UNINA9910144901503321

Titolo	Cryptography and Coding [[electronic resource]] : 6th IMA International Conference, Cirencester, UK, December 17-19, 1997, Proceedings / / edited by Michael Darnell
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1997
ISBN	3-540-69668-7
Edizione	[1st ed. 1997.]
Descrizione fisica	1 online resource (XI, 345 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1355
Disciplina	003/.54
Soggetti	Computer security Data encryption (Computer science) Computers Coding theory Information theory Computer science—Mathematics Computer communication systems Systems and Data Security 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 contenuto	The theory and application of reciprocal pairs of periodic sequences -- Zero-error codes for correlated information sources -- Trellis decoding techniques and their performance in the adder channel for synchronous and asynchronous CCMA codes -- Key agreement protocols and their security analysis -- Low density parity check codes based on sparse matrices with no small cycles -- On the SAFER cryptosystem -- An adaptive approach to T of N user multi-access communications channel using an orthogonal coded multiplexer -- The breaking of the Lorenz

Cipher: An introduction to the theory behind the operational role of “Colossus” at BP -- Split knowledge generation of RSA parameters -- Analysis of error control in digital trunked radio systems -- Reconstruction of convolutional encoders over GF(q) -- HCC: A hash function using error correcting codes -- Public-key cryptosystems based on elliptic curves -- Novel application of turbo decoding for radio channels -- Finding small roots of univariate modular equations revisited -- Robust Reed Solomon coded MPSK modulation -- RSA-type signatures in the presence of transient faults -- A digital signature scheme based on random error-correcting codes -- Variable rate adaptive trellis coded QAM for high bandwidth efficiency applications under Rayleigh fading channel -- Variable rate adaptive channel coding for coherent and non-coherent rayleigh fading channel -- Labyrinth: A new ultra high speed stream cipher -- Resisting the Bergen-Hogan attack on adaptive arithmetic coding -- Novel decoding technique for the synchronous and quasi-synchronous multiple access adder channel -- Increasing efficiency of International key escrow in mutually mistrusting domains -- Multi dimensional compartment schemes -- Evaluation of standard approximation to log-likelihood ratio addition in the MAP algorithm, and Its application in block code (‘Turbo’) Iterative decoding algorithms -- Multiuser coding based on detecting matrices for Synchronous-CDMA systems -- Enumeration of convolutional codes and minimal encoders -- On using Carmichael numbers for public key encryption systems -- Hash functions and MAC algorithms based on block ciphers -- Witness hiding restrictive blind signature scheme -- A note on the construction and upper bounds of correlation-immune functions -- On generalised concatenated codes -- Error performance analysis of different interleaving strategies applied to eight track digital tape systems -- Efficient error-propagating block chaining.

Sommario/riassunto

This book constitutes the refereed proceedings of the 6th International Conference on Cryptography and Coding held at the Institute of Mathematics and its Applications (IMA) in Cirencester, UK, in December 1997. The 35 revised full papers presented emphasize the links and commonality between the underlying mathematical bases and algorithmic foundations of cryptography, error control coding and digital signal processing devices available today. Besides classical crypto topics, other issues concerning information transmission and processing are addressed, such as multiple-access coding, image processing, synchronization and sequence design.