1. Record Nr. UNISA996465583303316

Titolo	Cryptography and Coding [[electronic resource]] : Fifth IMA Conference; Cirencester, UK, December 1995. Proceedings / / edited by Colin Boyd
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1995
ISBN	3-540-49280-1
Edizione	[1st ed. 1995.]
Descrizione fisica	1 online resource (XI, 297 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1025
Disciplina	003/.54
Soggetti	Computers Data encryption (Computer science) Coding theory Information theory Combinatorics Computer communication systems Information technology Business—Data processing Theory of Computation Cryptology Coding and Information Theory Computer Communication Networks IT in Business
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Design choices and security implications in implementing Diffie-Hellman key agreement -- A broadcast key distribution scheme based on block designs -- Minimal supports in linear codes -- Sequential decoding for a subcode of Reed Solomon Codes -- Linear Span analysis of a set of periodic sequence generators -- Minimal weight k-SR representations -- The main conjecture for MDS codes -- Some decoding applications of minimal realization -- The synthesis of perfect sequences -- Computation of low-weight parity checks for

correlation attacks on stream ciphers -- A storage complexity based analogue of Maurer key establishment using public channels -- Soft decision decoding of Reed Solomon codes using the Dorsch algorithm -- Good codes based on very sparse matrices -- Quantum cryptography: Protecting our future networks with quantum mechanics -- Prepaid electronic cheques using public-key certificates -- How traveling salespersons prove their identity -- An elliptic curve analogue of McCurley's key agreement scheme -- Multi-dimensional ring TCM codes for fading channels -- Authentication codes: An area where coding and cryptology meet -- Efficient generation of binary words of given weight -- Distribution of recurrent sequences modulo prime powers -- On-line secret sharing -- Church-Rosser codes -- A new algorithm for finding minimum-weight words in large linear codes -- Coding and cryptography for speech and vision -- Some constructions of generalised concatenated codes based on unit memory codes -- A note on the hash function of Tillich and Zémor -- Cryptanalysis of Harari's identification scheme -- Analysis of sequence segment keying as a method of CDMA transmission -- Constructions for variable-length error-correcting codes.

Sommario/riassunto

This book constitutes the refereed proceedings of the 5th IMA Conference on Cryptography and Coding, held in Cirencester, UK in December 1995. The volume presents 22 full revised papers selected from 48 submissions together with five invited full papers and three abstracts on the mathematical theory and practice of cryptography and coding; continuing advances in these strongly related areas are crucial for the security and reliability of data communication, processing, and storage. Among the topics addressed are linear codes, error-correcting codes, decoding, key distribution, authentication, hash functions, block ciphers, cryptanalysis, and electronic cash.