1. Record Nr. UNINA9910143457803321

Titolo	Fast Software Encryption : 4th International Workshop, FSE'97, Haifa, Israel, January 20-22, 1997, Proceedings / / edited by Eli Biham
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1997
ISBN	3-540-69243-6
Edizione	[1st ed. 1997.]
Descrizione fisica	1 online resource (IX, 299 p.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 1267
Disciplina	005.8/2
Soggetti	Cryptography Data encryption (Computer science) Data protection Computer science Algorithms Coding theory Information theory Computer science - Mathematics Discrete mathematics Cryptology Data and Information Security Theory of Computation Coding and Information Theory 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 and index.
Nota di contenuto	?2 cryptanalysis of the SEAL encryption algorithm -- Partitioning cryptanalysis -- The interpolation attack on block ciphers -- Best differential characteristic search of FEAL -- New block encryption algorithm MISTY -- The design of the ICE encryption algorithm -- Advanced Encryption Standard -- TWOPRIME: A fast stream ciphering algorithm -- On nonlinear filter generators -- Chameleon — A new kind of stream cipher -- Improving linear cryptanalysis of LOKI91 by probabilistic counting method -- Cryptanalysis of Ladder-DES -- A

family of trapdoor ciphers -- The block cipher Square -- XMX: A firmware-oriented block cipher based on modular multiplications -- MMH: Software message authentication in the Gbit/second rates -- Fast message authentication using efficient polynomial evaluation -- Reinventing the travois: Encryption/MAC in 30 ROM bytes -- All-or-nothing encryption and the package transform -- On the security of remotely keyed encryption -- Sliding encryption: A cryptographic tool for mobile agents -- Fast software encryption: Designing encryption algorithms for optimal software speed on the Intel Pentium processor -- A fast new DES implementation in software -- Optimizing a fast stream cipher for VLIW, SIMD, and superscalar processors.

Sommario/riassunto

This volume constitutes the strictly refereed post-workshop proceedings of the Fourth International Workshop on Fast Software Encryption, FSE'97, held in Haifa, Israel, in January 1997. The 23 full papers presented were carefully selected from 44 submissions and revised for inclusion in the book. Also contained is a summary of a panel discussion. The papers are organized in sections on cryptanalysis, blockciphers, stream ciphers, message authentication codes, modes of operation, and fast software encryption. Particular emphasis is placed on applicability and implementation issues of fast cryptography.