1. Record Nr. UNISA996466247103316

Titolo	Fast Software Encryption [[electronic resource]] : Cambridge Security Workshop, Cambridge, U.K., December 9 - 11, 1993. Proceedings / / edited by Ross Anderson
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1994
ISBN	3-540-48456-6
Edizione	[1st ed. 1994.]
Descrizione fisica	1 online resource (CCXL, 230 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 809
Disciplina	005.8/2
Soggetti	Computers Data encryption (Computer science) Software engineering Algorithms Combinatorics Theory of Computation Cryptology Software Engineering/Programming and Operating Systems Algorithm Analysis and Problem Complexity
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	SAFER K-64: A byte-oriented block-ciphering algorithm -- A new approach to block cipher design -- Fast block cipher proposal -- Fish: A fast software stream cipher -- The Shrinking Generator: some practical considerations -- A modern rotor machine -- Two stream ciphers -- A software-optimized encryption algorithm -- Encrypting network traffic -- Design principles for dedicated hash functions -- Performance of symmetric ciphers and one-way hash functions -- On the security of shift register based keystream generators -- The differential cryptanalysis and design of natural stream ciphers -- On modes of operation -- Cryptanalysis of clock controlled shift registers -- A bulk data encryption algorithm -- On finite automaton one-key cryptosystems -- Parallel FFT-hashing -- Attacks on double block length hash functions -- On quadratic m-sequences -- 2-Adic shift

registers -- New bent mappings suitable for fast implementation -- Cryptographic pseudo-random numbers in simulation -- Description of a new variable-length key, 64-bit block cipher (Blowfish) -- VINO: A block cipher including variable permutations -- Practically secure Feistel ciphers.

Sommario/riassunto

This volume contains the refereed papers presented at the International Workshop on Software Encryption Algorithms, held at Cambridge University, U.K. in December 1993. The collection of papers by representatives of all relevant research centers gives a thorough state-of-the-art report on all theoretical aspects of encryption algorithms and takes into account the new demands from new applications, as for example from the data-intensive multimedia applications. The 26 papers are organized in sections on block ciphers, stream ciphers, software performance, cryptanalysis, hash functions and hybrid ciphers, and randomness and nonlinearity.