1. Record Nr. UNISA996465767003316

Titolo	Fast Software Encryption [[electronic resource]] : Second International Workshop, Leuven, Belgium, December 14-16, 1994. Proceedings / / edited by Bart Preneel
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 1995
ISBN	3-540-47809-4
Edizione	[1st ed. 1995.]
Descrizione fisica	1 online resource (IX, 375 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1008
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Algorithms Coding theory Information theory Combinatorics Cryptology Algorithm Analysis and Problem Complexity Coding and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Clock-controlled pseudorandom generators on finite groups -- On random mappings and random permutations -- Binary cyclotomic generators -- Construction of bent functions and balanced Boolean functions with high nonlinearity -- Additive and linear structures of cryptographic functions -- The RC5 encryption algorithm -- The MacGuffin block cipher algorithm -- S-boxes and round functions with controllable linearity and differential uniformity -- Properties of linear approximation tables -- Searching for the optimum correlation attack -- A known plaintext attack on the PKZIP stream cipher -- Linear cryptanalysis of stream ciphers -- Feedback with carry shift registers over finite fields -- A free energy minimization framework for inference problems in modulo 2 arithmetic -- Truncated and higher order differentials -- SAFER K-64: One year later -- Improved characteristics for differential cryptanalysis of hash functions based on block ciphers

-- Linear cryptanalysis using multiple approximations and FEAL -- Problems with the linear cryptanalysis of DES using more than one active S-box per round -- Correlation matrices -- On the need for multipermutations: Cryptanalysis of MD4 and SAFER -- How to exploit the intractability of exact TSP for cryptography -- How to reverse engineer an EES device -- A fast homophonic coding algorithm based on arithmetic coding -- On Fibonacci keystream generators -- Cryptanalysis of McGuffin -- Performance of block ciphers and hash functions — One year later -- TEA, a tiny encryption algorithm.

Sommario/riassunto

This book contains a set of revised refereed papers selected from the presentations at the Second International Workshop on Fast Software Encryption held in Leuven, Belgium, in December 1994. The 28 papers presented significantly advance the state of the art of software algorithms for two cryptographic primitives requiring very high speeds, namely encryption algorithms and hash functions: this volume contains six proposals for new ciphers as well as new results on the security of the new proposals. In addition, there is an introductory overview by the volume editor. The papers are organized in several sections on stream ciphers and block ciphers; other papers deal with new algorithms and protocols or other recent results.