1. Record Nr. UNINA9910484780703321

Titolo	Fast Software Encryption : 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers / / edited by Henri Gilbert, Helena Handschuh
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XI, 443 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 3557
Altri autori (Persone)	GilbertHenri HandschuhHelena
Disciplina	005.8/2
Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Algorithms Computer science - Mathematics Discrete mathematics Cryptology Coding and Information Theory Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"The Fast Software Encryption 2005 Workshop was the twelfth in a series of annual workshops ... sponsored for the fourth year by the International Association for Cryptologic Research"--Pref.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	New Designs -- A New MAC Construction ALRED and a Specific Instance ALPHA-MAC -- New Applications of T-Functions in Block Ciphers and Hash Functions -- The Poly1305-AES Message-Authentication Code -- Stream Ciphers I -- Narrow T-Functions -- A New Class of Single Cycle T-Functions -- F-FCSR: Design of a New Class of Stream Ciphers -- Boolean Functions -- Cryptographically Significant Boolean Functions: Construction and Analysis in Terms of Algebraic Immunity -- The ANF of the Composition of Addition and Multiplication mod 2 n with a Boolean Function -- Block Ciphers I --

New Combined Attacks on Block Ciphers -- Small Scale Variants of the AES -- Stream Ciphers II -- Unbiased Random Sequences from Quasigroup String Transformations -- A New Distinguisher for Clock Controlled Stream Ciphers -- Analysis of the Bit-Search Generator and Sequence Compression Techniques -- Some Attacks on the Bit-Search Generator -- Hash Functions -- SMASH – A Cryptographic Hash Function -- Security Analysis of a 2/3-Rate Double Length Compression Function in the Black-Box Model -- Preimage and Collision Attacks on MD2 -- Modes of Operation -- How to Enhance the Security of the 3GPP Confidentiality and Integrity Algorithms -- Two-Pass Authenticated Encryption Faster Than Generic Composition -- Padding Oracle Attacks on CBC-Mode Encryption with Secret and Random IVs -- Stream Ciphers III -- Analysis of the Non-linear Part of Mugi -- Two Attacks Against the HBB Stream Cipher -- Two Linear Distinguishing Attacks on VMPC and RC4A and Weakness of RC4 Family of Stream Ciphers -- Impossible Fault Analysis of RC4 and Differential Fault Analysis of RC4 -- Block Ciphers II -- Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192 -- New Attacks Against Reduced-Round Versions of IDEA -- Implementations -- How toMaximize Software Performance of Symmetric Primitives on Pentium III and 4 Processors -- A Side-Channel Analysis Resistant Description of the AES S-Box -- DPA Attacks and S-Boxes.

Sommario/riassunto

The Fast Software Encryption 2005 Workshop was the twelfth in a series of annual workshops on symmetric cryptography, sponsored for the fourth year by the International Association for Cryptologic Research (IACR). The workshop concentratedonallaspectsoffastprimitivesforsymmetriccryptology, including thedesign, cryptanalysisandimplementationofblockandstreamciphersaswell as hash functions and message authentication codes. The ?rst FSE workshop was held in Cambridge in 1993, followed by Leuven in 1994, Cambridge in 1996, Haifain1997,Parisin1998,Romein1999, NewYorkin2000,Yokohamain2001, Leuven in 2002, Lund in 2003, and New Delhi in 2004. This year, a total of 96 submissions were received. After an extensive review by the Program Committee, 30 submissions were accepted. Two of these s- missions were merged into a single paper, yielding a total of 29 papers accepted for presentation at the workshop. Also, we were very fortunate to have in the programan invited talk byXuejia Laion "Attacks andProtection ofHash Fu- tions" and a very entertaining rump session that Bart Preneel kindly accepted to chair. These proceedings contain the revised versions of the accepted papers; the revised versions were not subsequently checked for correctness.