1. Record Nr. UNISA996466087903316

Titolo	Fast Software Encryption [[electronic resource]] : 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers / / edited by Matt Robshaw
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-36598-2
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XI, 434 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 4047
Disciplina	005.8
Soggetti	Data encryption (Computer science) Algorithms Coding theory Information theory Computer science—Mathematics Cryptology Algorithm Analysis and Problem Complexity Coding and Information Theory Discrete Mathematics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"International Association for Cryptologic Research"--Cover.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Stream Ciphers I -- Cryptanalysis of Achterbahn -- Cryptanalysis of Grain -- Cryptanalysis of the Stream Cipher DECIM -- Block Ciphers -- On Feistel Structures Using a Diffusion Switching Mechanism -- Pseudorandom Permutation Families over Abelian Groups -- A Zero-Dimensional Gröbner Basis for AES-128 -- Hash Functions I -- Cryptanalysis of the Full HAVAL with 4 and 5 Passes -- Collisions and Near-Collisions for Reduced-Round Tiger -- Analysis of Step-Reduced SHA-256 -- Analysis -- Improved Linear Distinguishers for SNOW 2.0 -- Reducing the Space Complexity of BDD-Based Attacks on Keystream Generators -- Breaking the ICE – Finding Multicollisions in Iterated Concatenated and Expanded (ICE) Hash Functions -- Proposals -- A New Dedicated 256-Bit Hash Function: FORK-256 -- Some Plausible Constructions of Double-Block-Length Hash Functions -- Provably

Secure MACs from Differentially-Uniform Permutations and AES-Based Implementations -- Hash Functions II -- Searching for Differential Paths in MD4 -- A Study of the MD5 Attacks: Insights and Improvements -- The Impact of Carries on the Complexity of Collision Attacks on SHA-1 -- Modes and Models -- A New Mode of Encryption Providing a Tweakable Strong Pseudo-random Permutation -- New Blockcipher Modes of Operation with Beyond the Birthday Bound Security -- The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function -- Implementation and Bounds -- How Far Can We Go on the x64 Processors? -- Computing the Algebraic Immunity Efficiently -- Upper Bounds on Algebraic Immunity of Boolean Power Functions -- Stream Ciphers II -- Chosen-Ciphertext Attacks Against MOSQUITO -- Distinguishing Attacks on the Stream Cipher Py -- Resynchronization Attacks on WG and LEX.

Sommario/riassunto

Fast Software Encryption (FSE) 2006 is the 13th in a series of workshops on symmetric cryptography. It has been sponsored for the last ?ve years by the International Association for Cryptologic Research (IACR), and previous FSE workshops have been held around the world: 1993 Cambridge, UK 1994 Leuven, Belgium 1996 Cambridge, UK 1997 Haifa, Israel 1998 Paris, France 1999 Rome, Italy 2000 New York, USA 2001 Yokohama, Japan 2002 Leuven, Belgium 2003 Lund, Sweden 2004 New Delhi, India 2005 Paris, France The FSE workshop is devoted to research on fast and secure primitives for symmetric cryptography, including the design and analysis of block ciphers, stream ciphers, encryption schemes, analysis and evaluation tools, hash fu- tions, and message authentication codes. This year more than 100 papers were submitted to FSE for the ?rst time. After an extensive review by the ProgramCommittee, 27 papers were presented at the workshop. Of course, the programwould not have been complete without the invited speaker, and the presentation by Eli Biham on the early history of di? erential cryptanalysis was particularly appreciated by workshop attendees.