1. Record Nr. UNINA9910483441103321

Titolo	Fast Software Encryption : 16th International Workshop, FSE 2009 Leuven, Belgium, February 22-25, 2009 Revised Selected Papers / / edited by Orr Dunkelman
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	1-282-33190-6 9786612331909 3-642-03317-2
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (425 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 5665
Classificazione	DAT 465f SS 4800
Disciplina	005.82
Soggetti	Cryptography Data encryption (Computer science) Computer programming Data structures (Computer science) Information theory Coding theory Algorithms Computer science - Mathematics Cryptology Programming Techniques Data Structures and Information Theory Coding and Information Theory Mathematical Applications in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Stream Ciphers -- Cube Testers and Key Recovery Attacks on Reduced-Round MD6 and Trivium -- An Efficient State Recovery Attack on X-FCSR-256 -- Key Collisions of the RC4 Stream Cipher -- Invited Talk -- Intel’s New AES Instructions for Enhanced Performance and Security -- Theory of Hash Functions -- Blockcipher-Based Hashing Revisited --

On the Security of Tandem-DM -- Indifferentiability of Permutation-Based Compression Functions and Tree-Based Modes of Operation, with Applications to MD6 -- Hash Functions Analysis I -- Cryptanalysis of RadioGatún -- Preimage Attacks on Reduced Tiger and SHA-2 -- Cryptanalysis of the LAKE Hash Family -- Block Ciphers Analysis -- New Cryptanalysis of Block Ciphers with Low Algebraic Degree -- Algebraic Techniques in Differential Cryptanalysis -- Multidimensional Extension of Matsui's Algorithm 2 -- Hash Functions Analysis II -- Meet-in-the-Middle Attacks on SHA-3 Candidates -- Practical Collisions for EnRUPT -- The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl -- Block Ciphers -- Revisiting the IDEA Philosophy -- Cryptanalysis of the ISDB Scrambling Algorithm (MULTI2) -- Beyond-Birthday-Bound Security Based on Tweakable Block Cipher -- Theory of Symmetric Key -- Enhanced Target Collision Resistant Hash Functions Revisited -- Message Authentication Codes -- MAC Reforgeability -- New Distinguishing Attack on MAC Using Secret-Prefix Method -- Fast and Secure CBC-Type MAC Algorithms -- HBS: A Single-Key Mode of Operation for Deterministic Authenticated Encryption.

Sommario/riassunto

This book constitutes the thoroughly refereed proceedings of the 16th International Workshop on Fast Software Encryption, FSE 2009 held in Leuven, Belgium in February 2009. The 24 revised full papers were carefully reviewed and selected from 76 submissions. The papers are organized in topical sections on stream ciphers, theory of hash functions, block ciphers analysis, block ciphers, theory of symmetric key, and message authentication codes.