1. Record Nr. UNINA9910483346803321

Titolo	Fast Software Encryption : 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers / / edited by Alex Biryukov
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2007
ISBN	3-540-74619-6
Edizione	[1st ed. 2007.]
Descrizione fisica	1 online resource (XI, 470 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 4593
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Algorithms Coding theory Information theory 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	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Hash Function Cryptanalysis and Design (I) -- Producing Collisions for Panama, Instantaneously -- Cryptanalysis of FORK-256 -- The Grindahl Hash Functions -- Stream Ciphers Cryptanalysis (I) -- Overtaking VEST -- Cryptanalysis of Achterbahn-128/80 -- Differential-Linear Attacks Against the Stream Cipher Phelix -- Theory -- How to Enrich the Message Space of a Cipher -- Security Analysis of Constructions Combining FIL Random Oracles -- Bad and Good Ways of Post-processing Biased Physical Random Numbers -- Fast Talks: Block Cipher Cryptanalysis -- Improved Slide Attacks -- A New Class of Weak Keys for Blowfish -- Fast Talks: Block Cipher Design -- The 128-Bit Blockcipher CLEFIA (Extended Abstract) -- New Lightweight DES Variants -- Block Cipher Cryptanalysis -- A New Attack on 6-Round

IDEA -- Related-Key Rectangle Attacks on Reduced AES-192 and AES-256 -- An Analysis of XSL Applied to BES -- Stream Cipher Cryptanalysis (II) -- On the Security of IV Dependent Stream Ciphers -- Two General Attacks on Pomaranch-Like Keystream Generators -- Analysis of QUAD -- Cryptanalysis of Hash Functions (II) -- Message Freedom in MD4 and MD5 Collisions: Application to APOP -- New Message Difference for MD4 -- Algebraic Cryptanalysis of 58-Round SHA-1 -- Theory of Stream Ciphers -- Algebraic Immunity of S-Boxes and Augmented Functions -- Generalized Correlation Analysis of Vectorial Boolean Functions -- Side Channel Attacks -- An Analytical Model for Time-Driven Cache Attacks -- MACs and Small Block Ciphers -- Improving the Security of MACs Via Randomized Message Preprocessing -- New Bounds for PMAC, TMAC, and XCBC -- Perfect Block Ciphers with Small Blocks.

Sommario/riassunto

This book contains the thoroughly refereed post-proceedings of the 14th International Workshop on Fast Software Encryption, FSE 2007, held in Luxembourg, Luxembourg, March 2007. It addresses all current aspects of fast and secure primitives for symmetric cryptology, covering hash function cryptanalysis and design, stream ciphers cryptanalysis, theory, block cipher cryptanalysis, block cipher design, theory of stream ciphers, side channel attacks, and macs and small block ciphers.