1. Record Nr. UNISA996465849303316

Titolo	Fast Software Encryption [[electronic resource]] : 17th International Workshop, FSE 2010, Seoul, Korea, February 7-10, 2010 Revised Selected Papers / / edited by Seokhie Hong, Tetsu Iwata
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-38745-9 9786613565372 3-642-13858-6
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (XI, 385 p. 71 illus.)
Collana	Security and Cryptology ; ; 6147
Disciplina	005.8/2
Soggetti	Data encryption (Computer science) Computer communication systems User interfaces (Computer systems) Algorithms Management information systems Computer science Computer security Cryptology Computer Communication Networks User Interfaces and Human Computer Interaction Algorithm Analysis and Problem Complexity Management of Computing and Information Systems Systems and Data Security
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	Stream Ciphers and Block Ciphers -- Cryptanalysis of the DECT Standard Cipher -- Improving the Generalized Feistel -- Nonlinear Equivalence of Stream Ciphers -- RFID and Implementations -- Lightweight Privacy Preserving Authentication for RFID Using a Stream Cipher -- Fast Software AES Encryption -- Hash Functions I -- Attacking the Knudsen-Preneel Compression Functions -- Finding

Preimages of Tiger Up to 23 Steps -- Cryptanalysis of ESSENCE -- Theory -- Domain Extension for Enhanced Target Collision-Resistant Hash Functions -- Security Analysis of the Mode of JH Hash Function -- Enhanced Security Notions for Dedicated-Key Hash Functions: Definitions and Relationships -- Message Authentication Codes -- A Unified Method for Improving PRF Bounds for a Class of Blockcipher Based MACs -- How to Thwart Birthday Attacks against MACs via Small Randomness -- Constructing Rate-1 MACs from Related-Key Unpredictable Block Ciphers: PGV Model Revisited -- Hash Functions II -- Higher Order Differential Attack on Step-Reduced Variants of Luffa v1 -- Rebound Attack on Reduced-Round Versions of JH -- Hash Functions III (Short Presentation) -- Pseudo-cryptanalysis of the Original Blue Midnight Wish -- Differential and Invertibility Properties of BLAKE -- Cryptanalysis -- Rotational Cryptanalysis of ARX -- Another Look at Complementation Properties -- Super-Sbox Cryptanalysis: Improved Attacks for AES-Like Permutations.