1. Record Nr. UNINA9910143901303321

Titolo	Fast Software Encryption : 9th International Workshop, FSE 2002, Leuven, Belgium, February 4-6, 2002. Revised Papers / / edited by Joan Daemen, Vincent Rijmen
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2002
ISBN	3-540-45661-9
Edizione	[1st ed. 2002.]
Descrizione fisica	1 online resource (XII, 284 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2365
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 Math Applications 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 at the end of each chapters and index.
Nota di contenuto	Block Cipher Cryptanalysis -- New Results on Boomerang and Rectangle Attacks -- Multiplicative Differentials -- Differential and Linear Cryptanalysis of a Reduced-Round SC2000 -- Impossible Differential Cryptanalysis of Reduced Round XTEA and TEA -- Improved Cryptanalysis of MISTY1 -- Multiple Linear Cryptanalysis of a Reduced Round RC6 -- Integral Cryptanalysis -- On the Security of CAMELLIA against the Square Attack -- Saturation Attacks on Reduced Round Skipjack -- Integral Cryptanalysis -- Block Cipher Theory -- Improved Upper Bounds of Differential and Linear Characteristic Probability for Camellia -- The Round Functions of RIJNDAEL Generate the Alternating Group -- Non-cryptographic Primitive for Pseudorandom Permutation -- Stream Cipher Design -- BeepBeep: Embedded Real-Time Encryption

-- A New Keystream Generator MUGI -- Scream: A Software-Efficient Stream Cipher -- Stream Cipher Cryptanalysis -- Distinguishing Attacks on SOBER-t16 and t32 -- Linearity Properties of the SOBER-t32 Key Loading -- A Time-Memory Tradeoff Attack Against LILI-128 -- Odds and Ends -- On the Security of Randomized CBC-MAC Beyond the Birthday Paradox Limit A New Construction -- Cryptanalysis of the Modified Version of the Hash Function Proposed at PKC'98 -- Compression and Information Leakage of Plaintext.