1. Record Nr. UNISA996465822403316

Titolo	Advanced Encryption Standard - AES [[electronic resource]] : 4th International Conference, AES 2004, Bonn, Germany, May 10-12, 2004, Revised Selected and Invited Papers / / edited by Hans Dobbertin, Vincent Rijmen, Aleksandra Sowa
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (X, 190 p.)
Collana	Security and Cryptology ; ; 3373
Disciplina	005.8
Soggetti	Data encryption (Computer science) Algorithms Computer science—Mathematics Cryptology Algorithm Analysis and Problem Complexity Symbolic and Algebraic Manipulation 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	Cryptanalytic Attacks and Related Results -- The Cryptanalysis of the AES – A Brief Survey -- The Boomerang Attack on 5 and 6-Round Reduced AES -- A Three Rounds Property of the AES -- DFA on AES -- Refined Analysis of Bounds Related to Linear and Differential Cryptanalysis for the AES -- Algebraic Attacks and Related Results -- Some Algebraic Aspects of the Advanced Encryption Standard -- General Principles of Algebraic Attacks and New Design Criteria for Cipher Components -- An Algebraic Interpretation of 128 -- Hardware Implementations -- Efficient AES Implementations on ASICs and FPGAs -- Small Size, Low Power, Side Channel-Immune AES Coprocessor: Design and Synthesis Results -- Other Topics -- Complementation-Like and Cyclic Properties of AES Round Functions -- More Dual Rijndaels -- Representations and Rijndael Descriptions -- Linearity of the AES Key Schedule -- The Inverse S-Box, Non-linear Polynomial