

1. Record Nr.	UNISA996465788403316
Titolo	Fast Software Encryption [[electronic resource]] : 10th International Workshop, FSE 2003, LUND, Sweden, February 24-26, 2003, Revised Papers / / edited by Thomas Johansson
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003
ISBN	3-540-39887-2
Edizione	[1st ed. 2003.]
Descrizione fisica	1 online resource (X, 402 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2887
Disciplina	005.82
Soggetti	Data encryption (Computer science) Coding theory Information theory Algorithms Computer science—Mathematics Computer software Cryptology Coding and Information Theory Algorithm Analysis and Problem Complexity Symbolic and Algebraic Manipulation Mathematical Software
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	Block Cipher Cryptanalysis -- Cryptanalysis of IDEA-X/2 -- Differential-Linear Cryptanalysis of Serpent -- Rectangle Attacks on 49-Round SHACAL-1 -- Cryptanalysis of Block Ciphers Based on SHA-1 and MD5 -- Analysis of Involutional Ciphers: Khazad and Anubis -- Boolean Functions and S-Boxes -- On Plateaued Functions and Their Constructions -- Linear Redundancy in S-Boxes -- Stream Cipher Cryptanalysis -- Loosening the KNOT -- On the Resynchronization Attack -- Cryptanalysis of Sober-t32 -- MACs -- OMAC: One-Key CBC MAC -- A Concrete Security Analysis for 3GPP-MAC -- New Attacks against Standardized MACs -- Analysis of RMAC -- Side Channel Attacks -- A Generic Protection against High-Order Differential Power

Analysis -- A New Class of Collision Attacks and Its Application to DES
 -- Block Cipher Theory -- Further Observations on the Structure of the
 AES Algorithm -- Optimal Key Ranking Procedures in a Statistical
 Cryptanalysis -- Improving the Upper Bound on the Maximum
 Differential and the Maximum Linear Hull Probability for SPN Structures
 and AES -- Linear Approximations of Addition Modulo 2ⁿ -- Block
 Ciphers and Systems of Quadratic Equations -- New Designs -- Turing:
 A Fast Stream Cipher -- Rabbit: A New High-Performance Stream
 Cipher -- Helix: Fast Encryption and Authentication in a Single
 Cryptographic Primitive -- PARSHA-256 -- A New Parallelizable Hash
 Function and a Multithreaded Implementation -- Modes of Operation
 -- Practical Symmetric On-Line Encryption -- The Security of "One-
 Block-to-Many" Modes of Operation.

2. Record Nr.	UNINA9910797979003321
Autore	Barr Colin
Titolo	Religion and Greater Ireland : Christianity and Irish global networks, 1750-1950 // edited by Colin Barr and Hilary M. Carey
Pubbl/distr/stampa	Montreal, [Quebec] : , : McGill-Queen's University Press, , 2015 ©2015
ISBN	0-7735-9735-2 0-7735-9734-4
Descrizione fisica	1 online resource (471 pages)
Collana	McGill-Queen's Studies in the History of Religion. Series Two ; ; 73
Disciplina	200.93615
Soggetti	Immigrants - Religious life Ireland Religion Ireland Ethnic identity
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Part one : Irish global networks -- Part two : Atlantic world -- Part three : Asia and Africa -- Part four : Southern world.
Sommario/riassunto	Stimulating essays that break new ground on religion and Irish identity in modern world history.

