Johansson

Fast Software Encryption

10th International Workshop, FSE 2003, LUND, Sweden, February 24-26, 2003, Revised Papers

This book constitutes the thoroughly refereed postproceedings of the 10th International Workshop on Fast Software Encryption, FSE 2003, held in Lund, Sweden in February 2003. The 27 revised full papers presented were carefully reviewed, improved, and selected from 71 submissions. The papers are organized in topical sections on block cipher cryptanalysis, Boolean functions and S-boxes, stream cipher cryptanalysis, MACs, block cipher theory, side channel attacks, new designs, and modes of operation.

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 2 n .- 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.



53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540204497
Medium: Buch
ISBN: 978-3-540-20449-7
Verlag: Springer
Erscheinungstermin: 16.10.2003
Sprache(n): Englisch
Auflage: 1. Auflage 2003
Serie: Lecture Notes in Computer Science
Produktform: Kartoniert
Gewicht: 622 g
Seiten: 402
Format (B x H): 155 x 235 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)