

<<快速软件加密 Fast software encryption>>

图书基本信息

书名：<<快速软件加密 Fast software encryption>>

13位ISBN编号：9783540438694

10位ISBN编号：3540438696

出版时间：2002-12

出版时间：湖南文艺出版社

作者：Matsui, Mitsuru; Matsui, Mitsuru;

页数：350

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<快速软件加密 Fast softwar>>

内容概要

This book constitutes the thoroughly refereed post-proceedings of the 8th International Workshop on Fast Software Encryption, FSE 2001, held in Yokohama, Japan in April 2001. The 27 revised full papers presented together with one invited paper were carefully reviewed and selected from 46 submissions. The papers are organized in topical sections on cryptanalysis of block ciphers, hash functions and Boolean functions, modes of operation, cryptanalysis of stream ciphers, pseudo-randomness, and design and evaluation.

书籍目录

Cryptanalysis of Block Ciphers I The Saturation Attack-A Bait for Twofish Linear Cryptanalysis of Reduced Round Serpent Cryptanalysis of the Mercy Block Cipher Hash Functions and Boolean Functions Producing Collisions for PANAMA The RIPEMDn and RIPEMDR Improved Variants of MD4 Are Not Collision Free New Constructions of Resilient Boolean Functions with Maximal Nonlinearity Modes of Operations Optimized Self-Synchronizing Mode of Operation Fast Encryption and Authentication: XCBC Encryption and XECB Authentication Modes IncrementM Unforgeable Encryption Cryptanalysis of Stream Ciphers I ZIP Attacks with Reduced Known Plaintext Cryptanalysis of the SEAL 3.0 Pseudorandom Function Family Cryptanalysis of SBLH A Practical Attack on Broadcast RC4 Cryptanalysis of Block Ciphers II Improved SQUARE Attacks against Reduced-Round HIEROCRYPT Differential Cryptanalysis of Q Differential Cryptanalysis of Nimbus Cryptanalysis of Stream Ciphers II Fast Correlation Attack Algorithm with List Decoding and an Application Bias in the LEVIATHAN Stream Cipher Analysis of SSC2Pseudo-Randomness Round Security and Super-Pseudorandomness of MISTY Type Structure New Results on the Pseudorandomness of Some Blockcipher Constructions FSE 2001 Special Talk NESSIE: A European Approach to Evaluate Cryptographic Algorithms Cryptanalysis of Block Ciphers III Related Key Attacks on Reduced Round KASUMI..... Design and Evaluation Author Index

#### 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>