

<<快速软件加密Fast software>>

图书基本信息

书名：<<快速软件加密Fast software encryption>>

13位ISBN编号：9783540417286

10位ISBN编号：3540417281

出版时间：2001-12

出版时间：1 (2001年3月1日)

作者：Bruce Schneier

页数：313

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 software>>

内容概要

This book constitutes the thoroughly refereed post-proceedings of the 7th International Workshop on Fast Software Encryption, FSE 2000, held in New York City, USA in April 2000. The 21 revised full papers presented were carefully reviewed and selected from a total of 53 submissions. The volume presents topical sections on stream-cipher cryptanalysis, new ciphers, AES cryptanalysis, block-cipher cryptanalysis, and theoretical work.

书籍目录

Specific Stream-Cipher Cryptanalysis Real Time Cryptanalysis of A5/1 on a PC Statistical Analysis of the Alleged RC4 Keystream Generator New Ciphers The Software-Oriented Stream Cipher SSC2 Mercy: A Fast Large Block Cipher for Disk Sector Encryption AES Cryptanalysis 1 A Statistical Attack on RC6 Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent Correlations in RC6 with a Reduced Number of Rounds Block-Cipher Cryptanalysis 1 On the Interpolation Attacks on Block Ciphers Stochastic Cryptanalysis of Crypton Power Analysis Bitslice Ciphers and Power Analysis Attacks Securing the AES Finalists Against Power Analysis Attacks General Stream-Cipher Cryptanalysis Ciphertext Only Reconstruction of Stream Ciphers based on Combination Generators A Simple Algorithm for Fast Correlation Attacks on Stream Ciphers A Low-Complexity and High-Performance Algorithm for the Fast Correlation Attack AES Cryptanalysis 2 Improved Cryptanalysis of Rijndael On the Pseudorandomness of the AES Finalists -- RC6 and Serpent Block-Cipher Cryptanalysis 2 Linear Cryptanalysis of Reduced-Round Versions of the SAFER Block Cipher Fam A Chosen-Plaintext Linear Attack on DES Theoretical Work Provable Security against Differential and Linear Cryptanalysis for the SPN Structure Unforgeable Encryption and Chosen Ciphertext Secure Modes of Operation Efficient Methods for Generating MARS-Like S-Boxes 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>