Page 1

<<　　　　　　　　　Fast software encryption>>

13　ISBN　　　9783540417286

10　ISBN　　　3540417281

　　　　2001-12

　　　　1 (2001　3　1　)

　Bruce Schneier

　313

　　　　　　　　PDF

　　　　　http://www.tushu007.com

<< Fast software>>

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.

Specific Stream-Cipher Cryptanalysis Real Time Cryptanalysis of A5/1 on a PC Statistical Analysis of the Alleged RC4 Keystream GeneratorNew Ciphers The Software-Oriented Stream Cipher SSC2 Mercy: A Fast Large Block Cipher for Disk Sector EncryptionAES Cryptanalysis 1 A Statistical Attack on RC6 Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent Correlations in RC6 with a Reduced Number of RoundsBlock-Cipher Cryptanalysis 1 On the Interpolation Attacks on Block Ciphers Stochastic Cryptanalysis of CryptonPower Analysis Bitslice Ciphers and Power Analysis Attacks Securing the AES Finalists Against Power Analysis AttacksGeneral 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 AttackAES Cryptanalysis 2 Improved Cryptanalysis of Rijndael On the Pseudorandomness of the AES Finalists -- RC6 and SerpentBlock-Cipher Cryptanalysis 2 Linear Cryptanalysis of Reduced-Round Versions of the SAFER Block Cipher Fam A Chosen-Plaintext Linear Attack on DESTheoretical 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-BoxesAuthor Index

<< Fast software>>

PDF

:http://www.tushu007.com