<<快速软件加密术 Fast softw>>

图书基本信息

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

13位ISBN编号：9783540440093

10位ISBN编号：3540440097

出版时间：2002-12

出版时间：1 (2002年9月1日)

作者：Joan Daemen

页数：276

<<快速软件加密术 Fast softw>>

内容概要

This book constitutes the thoroughly refereed post-proceedings of the 9th International Workshop on Fast Software Encryption, FSE 2002, held in Leuven, Belgium in February 2002. The 21 revised full papers presented were carefully reviewed and selected from 70 submissions. The papers are organized in topical sections on blook cipher cryptoanalysis, integral cryptoanalysis, block cipher theory, stream cipher design, stream cipher cryptanalysis, and odds and ends.

<<快速软件加密术 Fast softw>>

书籍目录

Block Cipher Cryptanalysis　New Results on Boomerang and Rectangle Attacks　Multiplicative Differentials　Differential and Linear Cryptanalysis of a Reduced-Rouna SC2000　Impossible Differential Cryptanalysis of Reduced Round　XTEA and TEA　Improved Cryptanalysis of MISTY1　Multiple Linear Cryptanalysis of a Reduced Round RC6Integral Cryptanalysis　On the Security of CAMELLIA against the Square Attack　Saturation Attacks on Reduced-Round Skipjack　Integral CryptanalysisBlock Cipher Theory　Improved Upper Bounds of Differential and Linear Characteristic　Probability for Camellia　The Round Functions of RIJNDAEL Generate the Alternating Group　Non-cryptographic Primitive for Pseudorandom PermutationStream Cipher Design　BeepBeep: Embedded Real-Time Encryption　A New Keystream Generator MUGI　Scream: A Software-Efficient Stream CipherStream Cipher Cryptanalysis　Distinguishing Attacks on SOBER-t16 and t32　Linearity Properties of the SOBER-t32 Key Loading　A Time-Memory Tradeoff Attack against LILI-128Odds and Ends　On the Security of Randomized CBC-MAC beyond the Birthday　Paradox Limit: A New Construction　Cryptanalysis of the Modified Version of the Hash Function　Proposed at PKC'98 ……Author Index

<<快速软件加密术 Fast softw>>

版权说明