

<<快速软件加密法/Fast softw>>

图书基本信息

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

13位ISBN编号：9783540365976

10位ISBN编号：3540365974

出版时间：2006-12

出版时间：湖北辞书出版社

作者：Robshaw, Matt 编

页数：432

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>

## 内容概要

This book constitutes the thoroughly refereed post-proceedings of the 13th International Workshop on Fast Software Encryption, FSE 2006, held in Graz, Austria in March 2006. The 27 revised full papers presented were carefully reviewed and selected from more than 100 submissions. The papers address all current aspects of fast and secure primitives for symmetric cryptology and they are organized in topical sections on stream ciphers, block ciphers, hash functions, analysis, proposals, modes and models, as well as implementation and bounds.

书籍目录

Stream Ciphers I Cryptanalysis of Achterbahn Cryptanalysis of Grain Cryptanalysis of the Stream Cipher  
DECIMBlock Ciphers On Feistel Structures Using a Diffusion Switching Mechanism Pseudorandom  
Permutation Families over Abelian Groups A Zero-Dimensional GrSbner Basis for AES-128Hash Functions I  
Cryptanalysis of the Full HAVAL with 4 and 5 Passes Collisions and Near-Collisions for Reduced-Round Tiger  
Analysis of Step-Reduced SHA-256Analysis Improved Linear Distinguishers for SNOW 2.0 Reducing the Space  
Complexity of BDD-Based Attacks on Keystream Generators Breaking the ICE - Finding Multicollisions in  
Iterated Concatenated and Expanded (ICE) Hash FhncionsProposals A New Dedicated 256-Bit Hash Function:  
FORK-256 Some Plausible Constructions of Double-Block-Length Hash Functions Provably Secure MACs from  
Differentially-Uniform Permutations and AES-Based ImplementationsHash Functions II Searching for  
Differential Paths in MD4 A Study of the MD5 Attacks: Insights and Improvements The Impact of Carries on the  
Complexity of Collision Attacks on SHA-1Modes and Models A New Mode of Encryption Providing a  
Tweakable Strong Pseudo-random Permutation New Blockcipher Modes of Operation with Beyond the Birthday  
Bound Security The Ideal-Cipher Model,Revisited:An Uninstantiable Blockcipher-Besed Hash  
FunctionInmplementation and BoundsStream CiphersIIAuthor 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>