

## <<Progress in Cryptology>>

### 图书基本信息

书名：<<Progress in Cryptology Mycrypt 2005密码术进展 - Mycrypt 2005/会议录>>

13位ISBN编号：9783540289388

10位ISBN编号：3540289380

出版时间：2005-10

出版时间：1 (2005年10月26日)

作者：Ed Dawson

页数：327

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>

## <<Progress in Cryptolo>>

### 内容概要

This book constitutes the refereed proceedings of the First International Conference on Cryptology hosted in Malaysia, held in Kuala Lumpur, Malaysia in September 2005, in conjunction with the e-Secure Malaysia 2005 convention. The 19 revised full papers presented together with 3 invited papers were carefully reviewed and selected from a total of 90 submissions. The papers are organized in topical sections on stream ciphers analysis, cryptography based on combinatorics, cryptographic protocols, implementation issues, unconventional cryptography, block cipher cryptanalysis, and homomorphic encryption.

## <<Progress in Cryptology>>

### 书籍目录

Invited Talk Trends and Challenges for Securer Cryptography in Practice  
 Stream Ciphers Analysis Distinguishing Attacks on T-Functions  
 Introducing a New Variant of Fast Algebraic Attacks and Minimizing  
 Their Successive Data Complexity Cryptography Based on Combinatorics  
 Equivalent Keys in HFE,  $C^*$ , and Variations A New Structural Attack for GPT and Variants  
 A Family of Fast Syndrome Based Cryptographic Hash Functions  
 Cryptographic Protocols Optimization of Electronic First-Bid Sealed-Bid Auction Based on  
 Homomorphic Secret Sharing Identity Based Delegation Network  
 On Session Key Construction in Provably-Secure Key Establishment Protocols  
 On the Security of Probabilistic Multisignature Schemes and Their Optimality  
 Invited Talk Efficient Secure Group Signatures with Dynamic Joins and Keeping Anonymity Against  
 Group Managers Implementation Issues An Analysis of Double Base Number Systems and a Sublinear Scalar  
 Multiplication Algorithm Power Analysis by Exploiting Chosen Message and Internal Collisions - Vulnerability of  
 Checking Mechanism for RSA-Decryption Optimization of the MOVA Undeniable Signature  
 Scheme Unconventional Cryptography Questionable Encryption and Its Applications Twin RSA  
 Invited Talk Security of Two-Party Identity-Based Key Agreement Block Cipher Cryptanalysis  
 Related-Key Differential Attacks on Cobra-S128, Cobra-F64a, and Cobra-F64b ..... Homomorphic Encryption  
 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>