

<<Progress in Cryptology>>

图书基本信息

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

13位ISBN编号：9783540308058

10位ISBN编号：3540308059

出版时间：2006-01-09

出版时间：Springer

作者：Subhamoy Maitra

页数：416

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 6th International Conference on Cryptology in India, INDOCRYPT 2005, held in Bangalore, India in December 2005. The 31 revised full papers presented together with 1 invited paper were carefully reviewed and selected from 148 submissions. The papers are organized in topical sections on sequences, boolean function and S-box, hash functions, design principles, cryptanalysis, time memory trade-off, new constructions, pairings, signatures, applications, e-cash, and implementations.

## &lt;&lt;Progress in Cryptolo&gt;&gt;

## 书籍目录

Invited Talk Abelian Varieties and Cryptography Sequences Proof of a Conjecture on the Joint Linear Complexity Profile of Multisequences Period of Streamcipher Edon80 Boolean Function and S-Box On the Algebraic Immunity of Symmetric Boolean Functions On Highly Nonlinear S-Boxes and Their Inability to Thwart DPA Attacks Hash Functions How to Construct Universal One-Way Hash Functions of Order  $r$  Towards Optimal Double-Length Hash Functions Design Principles Near Optimal Algorithms for Solving Differential Equations of Addition with Batch Queries Design Principles for Combiners with Memory Cryptanalysis Cryptanalysis of the Quadratic Generator Attack the Dragon Two Algebraic Attacks Against the F-FCSRs Using the IV Mode Cryptanalysis of Keystream Generator by Decimated Sample Based Algebraic and Fast Correlation Attacks Time Memory Trade-Off TMD-Tradeoff and State Entropy Loss Considerations of Streamcipher MICKEY Time-Memory Trade-Offs: False Alarm Detection Using Checkpoints Cryptanalysis Cryptanalysis of Barni et al. Watermarking Scheme Completion Attacks and Weak Keys of Oleshchuk's Public Key Cryptosystem New Constructions An Optimal Subset Cover for Broadcast Encryption MaTRU: A New NTRU-Based Cryptosystem Anonymous Password-Based Authenticated Key Exchange Pairings Signatures Applications E-Cash Implementations Author Index

## <<Progress in Cryptolo>>

### 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>