

<<Advances in Cryptology>>

图书基本信息

书名：<<Advances in Cryptology ASIACRYPT 2005密码术进展 - ASIACRYPT 2005/会议录>>

13位ISBN编号：9783540306849

10位ISBN编号：3540306846

出版时间：2006-1

出版时间：湖北辞书出版社

作者：Roy, Bimal

页数：701

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>

## <<Advances in Cryptolo>>

### 内容概要

This book constitutes the refereed proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2005, held in Chennai, India in December 2005. The 37 revised full papers presented were carefully reviewed and selected from 237 submissions. The papers are organized in topical sections on algebra and number theory, multiparty computation, zero knowledge and secret sharing, information and quantum theory, privacy and anonymity, cryptanalytic techniques, stream cipher cryptanalysis, block ciphers and hash functions, bilinear maps, key agreement, provable security, and digital signatures.

<<Advances in Cryptology>>

书籍目录

Algebra and Number Theory Discrete-Log-Based Signatures May Not Be Equivalent to Discrete Log Do AR  
 Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log? Adaptive Density Attacks on  
 Low-Weight Knapsacks Efficient and Secure Elliptic Curve Point Multiplication Using Double Base  
 Chains Multiparty Computation Upper Bounds on the Communication Complexity of Optimally Resilient  
 Cryptographic Multiparty Computation Graph Decomposition Based Frameworks for Subset Cover Broadcast  
 Encryption and Efficient Instantiations Revealing Additional Information in Two Party Computations Zero  
 Knowledge and Secret Sharing Gate Evaluation Secret Sharing and Secure One-Round Two Party Computation  
 Parallel Multi-party Computation from Linear Multi-secret Sharing Schemes Updatable Zero-Knowledge  
 Databases Information and Quantum Theory Simple and Tight Bounds for Information Reconciliation and  
 Privacy Amplification Quantum Fully Anonymous Anonymous Privacy and Anonymity Privacy Preserving  
 Graph Algorithms in the Semi-honest Model Spreading Alerts Quietly and the Subgroup Escape Problem A  
 Sender Verifiable Mix-Net and a New Proof of a Shuffle Universally Anonymizable Public-Key  
 Encryption Cryptanalytic Techniques Fast Computation of Large Distributions and Its Cryptographic  
 Applications An Analysis of the XSL Algorithm Stream Cipher Cryptanalysis New Applications of Time  
 Memory Data Structures Block Ciphers and Hash Functions Bilinear Maps Key Agreement Provable  
 Security Signatures Author Index

## <<Advances 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>