第一图书网, tushu007.com

<<Advances in Cryptolo>>

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

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.

书籍目录

Algebra and Number Theory　Discrete-Lo-Based Signatules May Not Be Equivalent to Discrete Log　Do AR Elliptic Curves of the Same Order lIare the Samc Dimculty of Discrete Log?　Adaptizlg Density Attacks m Low-Weight Knapsacks　Egzclcnt and Secure Elliptic Curve Point Mu]tiplication Using Double Base ChainsMultiparty Coinput ation　Uppm Bounds on the Communication Complexity of Optimally　Resilient Cryptographic Multiparty Computation　Graph Decomposition Based Frameworks fiar Subset Cover Broadcast　Encryption and Bfllcient installtiations　Revealing Additional Information in Two Party ComputatkmsZero Knowledge and Secret Sharing　Gate Evaluation Secret Sharing and Secure One-Round Two Party Computation　Parallel Multi-party Computatiol from Linear Multi-secret Shaling Schemes　Updatable Zero-Knowledge DatabasesInformation and Quantum Theory　Shnple and Tight Bounds for Information ReconciliaLion and Privacy Amplification　QUfalltlll]ft Anoltymous 1"l'ansmisslonsPrivacy and Anonylnity　Prlvacy Preserving Groph Algorithms in the Semi honest Model　Spieading Alerts Quietly and the Subgloup Escape Problem　A Sender Verifiable Mix-Net and a New Proof of a Shuffle　Universol]y Anonymizable Public-Key EncryptionCryptanalytic Techniques　Fast Conlputation of Large Distributions and Its Cryptographlc Applications　An Analysis of the XSL Algorithm　Stream Cipher Cryptanalysis　New Applications of Time Memory Data 'IYa& offs……Block Ciphers and Hash FunctionsBilinear MapsKey AreementProvable SecuritySignaturesAuthor 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