<<密码法进展>>

图书基本信息

书名：<<密码法进展>>

13位ISBN编号：9783540497677

10位ISBN编号：3540497676

出版时间：2006-12

出版时间：湖南文艺出版社

作者：Barua, Rana; Lange, Tanja;

页数：454

内容概要

This book constitutes the refereed proceedings of the 7th International Conference on Cryptology in India, INDOCRYPT 2006, held in Kolkata, India in December 2006. The 29 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 186 submissions. The papers are organized in topical sections on symmetric cryptography: attacks, hash functions, provable security: key agreement, provable security: public key cryptograpy, symmetric cryptography: design, modes of operation and message authentication codes, fast implementation of public key cryptography, id-based cryptography, as well as embedded systems and side channel attacks.

书籍目录

Invited Talk Whither Cryptography?Symmetric Cryptography: Attacks   Non-randomness in eSTREAM Candidates Salsa20 and TSC-4   Differential and Rectangle Attacks on Reduced-Round SHACAL-1   Algebraic Attacks on Clock-Controlled Cascade Ciphers   An Algorithm for Solving the LPN Problem and Its Application   to Security Evaluation of the HB Protocols for RFID AuthenticationHash Functions   Update on Tiger   RC4-Hash: A New Hash Function Based on RC4   Security of VSH in the Real WorldProvable Security:Key Agreement   Cryptanalysis of Two Provably Secure Cross-Realm   C2C-PAKE Protocols   Efficient and Provably Secure Generic Construction of Three-Party   Password-Based Authenticated Key Exchange Protocols   On the Importance of Public-Key Validation in the MQV and HMQV   Key Agreement ProtocolsInvited Talk   Another Look at "Provable Security". IIProvable Security: Public Key Cryptography   Efficient CCA-Secure Public-Key Encryption Schemes from   RSA-Related Assumptions   General Conversion for Obtaining Strongly Existentially Unforgeable   Signatures   Conditionally Verifiable Signature   Constant Phase Bit Optimal Protocols fox Perfectly Reliable and   Secure Message TransmissionSymmetric Cryptography: Design   Using Wiedemann's Algorithm to Compute the Immunity Against   Algebraic and Fast Algebraic Attacks······Modes of Operation and Message Authentication CodesFast Implementation of Public Key CryptogyaphyID-Based CryptographyEmbedded System and Side Channel AttacksAuthor Index

版权说明