第一图书网, tushu007.com

<<密码学进展Advances in cr>>

图书基本信息

书名：<<密码学进展Advances in cryptology>>

13位ISBN编号：9783540494751

10位ISBN编号：3540494758

出版时间：2006-12

出版时间：湖南文艺出版社

作者：Xuejia Lai 著

页数：468

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 12th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT 2005, held in Shanghai, China in December 2006.　The 30 revised full papers presented were carefully reviewed and selected from 314 submissions. The papers are organized in topical sections on attacks on hash functions, stream ciphers and boolean functions, biometrics and ECC computation, id-based schemes, public-key schemes, RSA and factorization, construction of hash function, protocols, block ciphers, and signatures.

书籍目录

Attacks on Hash Functions　Finding SHA-1 Characteristics: General Results and Applications　Improved Collision Search for SHA-0　Forgery and Partial Key-Recovery Attacks on HMAC and NMAC Using Hash CollisionsStream Ciphers and Boolean Functions　New Guess-and-Determine Attack on the Self-Shrinking Generator　On the (In)security of Stream Ciphers Based on Arrays and Modular Addition　Construction and Analysis of Boolean Functions of 2t + 1 Variables with Maximum Algebraic ImmunityBiometrics and ECC Computation　Secure Sketch for Biometric Templates　The 2-Adic CM Method for Genus 2 Curves with Application to Cryptography　Extending Scalar Multiplication Using Double BasesID-Based Schemes　HIBE With Short Public Parameters Without Random Oracle　Forward-Secure and Searchable Broadcast Encryption with Short Ciphertexts and Private Keys　On the Generic Construction of Identity-Based Signatures with Additional PropertiesPublic-Key Schemes　On the Provable Security of an Efficient RSA-Based Pseudorandom Generator　On the Security of OAEP　Relationship Between Standard Model Plaintext Awareness and Message HidingRSA and Factorization　On the Equivalence of RSA and Factoring Regarding Generic Ring Algorithms　Trading One-Wayness Against Chosen-Cipherte~t Security in Factoring-Based Encryption　A Strategy for Finding Roots of Multivariate Polynomials with New Applications in Attacking RSA VariantsConstruction of Hash Function　Indifferentiable Security Analysis of Popular Hash Functions with Prefix-Free Padding……ProtocolsBlock CiphersSignaturesAuthor 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