

<<Advances in Cryptology>>

图书基本信息

书名：<<Advances in Cryptology - EUROCRYPT 2005密码术进展>>

13位ISBN编号：9783540259107

10位ISBN编号：3540259104

出版时间：2005-8

出版时间：北京燕山出版社

作者：Cramer, Ronald; Cramer, Roland;

页数：576

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 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2005, held in Aarhus, Denmark in May 2005. The 33 revised full papers presented were carefully reviewed and selected from 190 submissions. The papers are organized in topical sections on cryptanalysis, theory, encryption, signatures and authentication, algebra and number theory, quantum cryptography, secure protocols, and broadcast encryption and traitor tracing.

<<Advances in Cryptology>>

书籍目录

Cryptanalysis Cryptanalysis of the Hash Functions MD4 and RIPEMD How to Break MD5 and Other Hash Functions Collisions of SHA-0 and Reduced SHA-1 Theory Reducing Complexity Assumptions for Statistically-Hiding Commitment Smooth Projective Hashing and Two-Message Oblivious Transfer On Robust Combiners for Oblivious Transfer and Other Primitives Encryption Efficient Identity-Based Encryption Without Random Oracles Tag-KEM/DEM: A New Framework for Hybrid Encryption and a New Analysis of Kurosawa-Desmedt KEM Signatures and Authentication Secure Remote Authentication Using Biometric Data Stronger Security Bounds for Wegman-Carter-Shoup Authenticators 3-Move Undeniable Signature Scheme Group Signatures with Efficient Concurrent Join Algebra and Number Theory Floating-Point LLL Revisited Practical Cryptography in High Dimensional Tori A Tool Kit for Finding Small Roots of Bivariate Polynomials over the Integers Quantum Cryptography Computational Indistinguishability Between Quantum States and Its Cryptographic Application Approximate Quantum Error-Correcting Codes and Secret Sharing Schemes Secure Protocols Compact E-Cash.....Algebra and Number Theory Theory Encryption Cryptanalysis Broadcast Encryption and Traitor Tracing 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>