

<<Progress in Cryptology>>

图书基本信息

书名：<<Progress in Cryptology - INDOCRYPT 2004密码学进展>>

13位ISBN编号：9783540241300

10位ISBN编号：3540241302

出版时间：2005-02-14

出版时间：Springer

作者：Canteaut, Anne; Viswanathan, Kapaleeswaran;

页数：429

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>

<<Progress in Cryptolo>>

内容概要

This book constitutes the refereed proceedings of the 5th International Conference on Cryptology in India, INDOCRYPT 2004, held in Chennai, India in December 2004. The 30 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 181 submissions. The papers are organized in topical sections on cryptographic protocols, applications, stream ciphers, cryptographic Boolean functions, foundations, block ciphers, public key encryption, efficient representations, public key cryptanalysis, modes of operation, signatures, and traitor tracing and visual cryptography.

<<Progress in Cryptolo>>

书籍目录

Invited Talks Design of Secure Key Establishment Protocols: Successes, Failures and Prospects Secure Protocols for Complex Tasks in Complex Environments Cryptographic Protocols Tripartite Key Exchange in the Canetti-Krawczyk Proof Model The Marriage Proposals Problem: Fair and Efficient Solution for Two-Party Computations Applications On the Security of a Certified E-Mail Scheme Multiplicative Homomorphic E-Voting Stream Ciphers Chosen Ciphertext Attack on a New Class of Self-Synchronizing Stream Ciphers Algebraic Attacks Over $GF(q)$ Cryptographic Boolean Functions Results on Algebraic Immunity for Cryptographically Significant Boolean Functions Generalized Boolean Bent Functions On Boolean Functions with Generalized Cryptographic Properties Foundations Information Theory and the Security of Binary Data Perturbation Symmetric Authentication Codes with Secrecy and Unconditionally Secure Authenticated Encryption Block Ciphers Faster Variants of the MESH Block Ciphers Related-Key Attacks on Reduced Rounds of SHACAL-2 Related-Key Attacks on DDP Based Ciphers: CIKS-128 and CIKS-128H Cryptanalysis of Ake98 Public Key Encryption Designing an Efficient and Secure Public-Key Cryptosystem Based on Reducible Rank Codes..... Efficient Representations Public Key Cryptanalysis Modes of Operation Traitor Tracing and Visual Cryptography Author Index

<<Progress 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>