

图书基本信息

书名：《Topics in Cryptology - CT-RSA 2001: The Cryptographer's Track at RSA Conference 2001 San Francisco, CA, USA, April 8-12, 2001 Proceedings (平装)》

13位ISBN编号：9783540418986

10位ISBN编号：3540418989

出版时间：2001-12

出版社：1 edition (2001年5月1日)

作者：David Naccache

页数：470

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《Topics in Cryptology》

内容概要

在线阅读本书

This book constitutes the refereed proceedings of the Cryptographers' Track at RSA Conference 2001, CT-RSA 2001, in San Francisco, CA, USA in April 2001. The 33 revised full papers presented were carefully reviewed and selected from 65 submissions. The papers are organized in topical sections on new cryptosystems; RSA; symmetric cryptography; gambling and lotteries; reductions, constructions, and security proofs; flaws and attacks; implementation; multivariate cryptography; number theoretic problems; passwords and credentials; and protocols.

《Topics in Cryptology》

书籍目录

New Cryptosystems Faster Generation of NICE-Schnorr-Type Signatures New Key Agreement Protocols in Braid Group Cryptography RSA Improving SSL Handshake Performance via Batching From Fixed-Length Messages to Arbitrary-Length Messages Practical RSA Signature Padding Schemes An Advantage of Low-Exponent RSA with Modulus Primes Sharing Least Significant Bits Symmetric Cryptography On the Strength of Simply-Iterated Feistel Ciphers with Whitening Keys Analysis of SHA-1 in Encryption Mode Fast Implementation and Fair Comparison of the Final Candidates for Advanced Encryption Standard Using Field Programmable Gate Arrays Gambling and Lotteries Fair e-Lotteries and e-Casinos Secure Mobile Gambling Reductions, Constructions and Security Proofs Formal Security Proofs for a Signature Scheme with Partial Message Recovery The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform Flaws and Attacks Security Weaknesses in Bluetooth Distinguishing Exponent Digits by Observing Modular Subtractions On the Power of Misbehaving Adversaries and Security Analysis of the Original EPOC Implementation Modular Exponentiation on Fine-Grained FPGA..... Multivariate Cryptography Number Theoretic Problems Protocols I Protocols I Author 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:www.tushu000.com