

<<Cryptography and Cod>>

图书基本信息

书名：<<Cryptography and Coding密码术与编码/会议录>>

13位ISBN编号：9783540302766

10位ISBN编号：354030276X

出版时间：2006-6

出版时间：Springer-Verlag New York Inc

作者：Smart, Nigel (EDT)

页数：458

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>

## <<Cryptography and Cod>>

### 内容概要

This book constitutes the refereed proceedings of the 10th IMA International Conference on Cryptography and Coding, held in Cirencester, UK, in December 2005. The 26 revised full papers presented together with 4 invited contributions were carefully reviewed and selected from 94 submissions. The papers are organized in topical sections on coding theory, signatures and signcryption, symmetric cryptography, side channels, algebraic cryptanalysis, information theoretic applications, number theoretic foundations, and public key and ID-based encryption schemes.

<<Cryptography and Cod>>

书籍目录

Invited Papers Abstract Models of Computation in Cryptography Pairing-Based Cryptography at High Security Levels Improved Decoding of Interleaved AG Codes Coding Theory Performance Improvement of Turbo Code Based on the Extrinsic Information Transition Characteristics A Trellis-Based Bound on (2, 1)-Separating Codes Tessellation Based Multiple Description Coding Exploiting Coding Theory for Collision Attacks on SHA-1 Signatures and Signcryption Hash Based Digital Signature Schemes A General Construction for Simultaneous Signing and Encrypting Non-interactive Designated Verifier Proofs and Undeniable Signatures Symmetric Cryptography Partial Key Recovery Attacks on XCBC, TMAC and OMAC Domain Expansion of MACs: Alternative Uses of the FIL-MAC Normality of Vectorial Functions Related-Key Differential Attacks on Cobra-H64 and Cobra-H128 Side Channels The Physically Observable Security of Signature Schemes On the Automatic Construction of Indistinguishable Operations Efficient Countermeasures for Thwarting the SCA Attacks on the Frobenius Based Methods Algebraic Cryptanalysis Complexity Estimates for the F4 Attack on the Perturbed Matsumoto-Imai Cryptosystem An Algebraic Framework for Cipher Embeddings Probabilistic Algebraic Attacks Information Theoretic Applications Number Theoretic Foundations Public Key and ID-Based Encryption Schemes Author Index

<<Cryptography and Cod>>

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>