1. Record Nr. UNINA9910144204303321

| | |
|---|---|
| Titolo | Information Security and Cryptology - ICISC 2003 : 6th International Conference, Seoul, Korea, November 27-28, 2003, Revised Papers / / edited by Jong In Lim, Dong Hoon Lee |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004 |
| ISBN | 1-280-30725-0<br>9786610307258<br>3-540-24691-6 |
| Edizione | [1st ed. 2004.] |
| Descrizione fisica | 1 online resource (XII, 464 p.) |
| Collana | Lecture Notes in Computer Science, , 0302-9743 ; ; 2971 |
| Disciplina | 005.8 |
| Soggetti | Data encryption (Computer science)<br>Computer communication systems<br>Operating systems (Computers)<br>Algorithms<br>Computer science—Mathematics<br>Management information systems<br>Computer science<br>Cryptology<br>Computer Communication Networks<br>Operating Systems<br>Algorithm Analysis and Problem Complexity<br>Discrete Mathematics in Computer Science<br>Management of Computing and Information Systems |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Note generali | Bibliographic Level Mode of Issuance: Monograph |
| Nota di bibliografia | Includes bibliographical references at the end of each chapters and index. |
| Nota di contenuto | Invited Talk -- Binary Tree Encryption: Constructions and Applications -- Digital Signatures I -- A Separable Threshold Ring Signature Scheme -- On the Security of a Group Signature Scheme with Forward Security -- An Efficient Strong Designated Verifier Signature Scheme -- Primitives -- Sound Computational Interpretation of Formal Encryption |

with Composed Keys -- On the Security of a New Variant of OMAC -- New Methods to Construct Cheating Immune Functions -- Yet Another Definition of Weak Collision Resistance and Its Analysis -- Fast Implementations -- Implementation of Tate Pairing on Hyperelliptic Curves of Genus 2 -- A General Expansion Method Using Efficient Endomorphisms -- Design of Bit Parallel Multiplier with Lower Time Complexity -- Architecture for an Elliptic Curve Scalar Multiplication Resistant to Some Side-Channel Attacks -- Efficient Scalar Multiplication in Hyperelliptic Curves Using A New Frobenius Expansion -- Computer Security/Mobile Security -- Adaptive Protocol for Entity Authentication and Key Agreement in Mobile Networks -- Extended Role Based Access Control and Procedural Restrictions -- Layer-Based Access Control Model in the Manufacturing Infrastructure and Design Automation System -- Voting/Auction Protocols -- Secure Double Auction Protocols with Full Privacy Protection -- Sealed-Bid Auctions with Efficient Bids -- Providing Receipt-Freeness in Mixnet-Based Voting Protocols -- Receipt-Free Electronic Auction Schemes Using Homomorphic Encryption -- Watermarking -- Software Watermarking Through Register Allocation: Implementation, Analysis, and Attacks -- Analysis of the Bounds for Linear Block Codes in Watermark Channel -- Digital Signatures II -- Security Analysis of Some Proxy Signatures -- A More Secure and Efficacious TTS Signature Scheme -- An Efficient Revocation Algorithm in Group Signatures -- Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity -- Authentication/Threshold Protocols -- Group Oriented Cryptosystems Based on Linear Access Structures -- A New Algorithm for Searching a Consistent Set of Shares in a Threshold Scheme with Cheaters -- Non-interactive Deniable Ring Authentication -- Block/Stream Ciphers -- Differential Cryptanalysis of TEA and XTEA -- A Complete Divide and Conquer Attack on the Alpha1 Stream Cipher -- New Block Cipher: ARIA -- Truncated Differential Attacks on 8-Round CRYPTON.

Sommario/riassunto

This book constitutes the thoroughly refereed post-proceedings of the 6th International Conference on Information Security and Cryptology, ICISC 2003, held in Seoul, Korea, in November 2003. The 32 revised full papers presented together with an invited paper were carefully selected from 163 submissions during two rounds of reviewing and improvement. The papers are organized in topical sections on digital signatures, primitives, fast implementations, computer security and mobile security, voting and auction protocols, watermarking, authentication and threshold protocols, and block ciphers and stream ciphers.