1. Record Nr. UNISA996465784903316

Titolo	Information and Communications Security [[electronic resource]] : 5th International Conference, ICICS 2003, Huhehaote, China, October 10-13, 2003, Proceedings / / edited by Petra Perner, Dieter Gollmann, Jianying Zhou
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003
ISBN	3-540-39927-5
Edizione	[1st ed. 2003.]
Descrizione fisica	1 online resource (X, 418 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2836
Disciplina	005.8
Soggetti	Computer security Data encryption (Computer science) Computer communication systems Operating systems (Computers) Algorithms Computer science—Mathematics Systems and Data Security Cryptology Computer Communication Networks Operating Systems Algorithm Analysis and Problem Complexity Discrete Mathematics in Computer Science
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 and index.
Nota di contenuto	A Fast Square Root Computation Using the Frobenius Mapping -- A Forward-Secure Blind Signature Scheme Based on the Strong RSA Assumption -- Secure Route Structures for the Fast Dispatch of Large-Scale Mobile Agents -- On the RS-Code Construction of Ring Signature Schemes and a Threshold Setting of RST -- A Policy Based Framework for Access Control -- Trading-Off Type-Inference Memory Complexity against Communication -- Security Remarks on a Group Signature Scheme with Member Deletion -- An Efficient Known Plaintext Attack

on FEA-M -- An Efficient Public-Key Framework -- ROCEM: Robust Certified E-mail System Based on Server-Supported Signature -- Practical Service Charge for P2P Content Distribution -- ICMP Traceback with Cumulative Path, an Efficient Solution for IP Traceback -- A Lattice Based General Blind Watermark Scheme -- Role-Based Access Control and the Access Control Matrix -- Broadcast Encryption Schemes Based on the Sectioned Key Tree -- Research on the Collusion Estimation -- Multiple Description Coding for Image Data Hiding Jointly in the Spatial and DCT Domains -- Protocols for Malicious Host Revocation -- A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code -- A Novel Two-Level Trust Model for Grid -- Practical t-out-n Oblivious Transfer and Its Applications -- Adaptive Collusion Attack to a Block Oriented Watermarking Scheme -- ID-Based Distributed “Magic Ink” Signature from Pairings -- A Simple Anonymous Fingerprinting Scheme Based on Blind Signature -- Compact Conversion Schemes for the Probabilistic OW-PCA Primitives -- A Security Verification Method for Information Flow Security Policies Implemented in Operating Systems -- A Novel Efficient Group Signature Scheme with Forward Security -- Variations of Diffie-Hellman Problem -- A Study on the Covert Channel Detection of TCP/IP Header Using Support Vector Machine -- A Research on Intrusion Detection Based on Unsupervised Clustering and Support Vector Machine -- UC-RBAC: A Usage Constrained Role-Based Access Control Model -- (Virtually) Free Randomization Techniques for Elliptic Curve Cryptography -- An Optimized Multi-bits Blind Watermarking Scheme -- A Compound Intrusion Detection Model -- An Efficient Convertible Authenticated Encryption Scheme and Its Variant -- Space-Economical Reassembly for Intrusion Detection System -- A Functional Decomposition of Virus and Worm Programs.

Sommario/riassunto

ICICS 2003, the Fifth International Conference on Information and Communication Security, was held in Huhehaote city, Inner Mongolia, China, 10–13 October 2003. Among the preceding conferences, ICICS’ 97 was held in B- jing, China, ICICS’99 in Sydney, Australia, ICICS 2001 in Xi’an, China, and ICICS 2002,in Singapore. TheproceedingswerereleasedasVolumes1334,1726, 2229, and 2513 of the LNCS series of Springer-Verlag, respectively. ICICS 2003 was sponsored by the Chinese Academy of Sciences (CAS), the National Natural Science Foundation of China, and the China Computer Federation. The conference was organized by the Engineering Research Center for Information Security Technology of the Chinese Academy of Sciences (ERCIST, CAS) in co-operation with the International Communications and Information Security Association (ICISA). The aim of the ICICS conferences has been to offer the attendees the opportunity to discuss the state-of-the-art technology in theoretical and practical aspects of information and communications security. The response to the Call for Papers was surprising. When we were preparing the conference between April and May, China, including the conference venue, Huhehaote City, was fighting against SARS. Despite this 176 papers were submitted to the conference from 22 countries and regions, and after a competitive selection process, 37 papers from 14 countries and regions were accepted to appear in the proceedings and be presented at ICICS 2003. We would like to take this opportunity to thank all those who submitted papers to ICICS 2003 for their valued contribution to the conference.