1. Record Nr. UNISA996465548203316

Titolo	Information and Communications Security [[electronic resource]] : 7th International Conference, ICICS 2005, Beijing, China, December 10-13, 2005, Proceedings / / edited by Wenbo Mao, Guilin Wang
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XIV, 498 p.)
Collana	Security and Cryptology ; ; 3783
Disciplina	005.82
Soggetti	Data encryption (Computer science) Operating systems (Computers) Management information systems Computer science Computers and civilization Computer communication systems Algorithms Cryptology Operating Systems Management of Computing and Information Systems Computers and Society Computer Communication Networks Algorithm Analysis and Problem Complexity
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	Fair Exchange -- An Evenhanded Certified Email System for Contract Signing -- Efficient ID-Based Optimistic Fair Exchange with Provable Security -- On the Quest for Impartiality: Design and Analysis of a Fair Non-repudiation Protocol -- Generic, Optimistic, and Efficient Schemes for Fair Certified Email Delivery -- Digital Signatures I -- Cryptanalysis of a Forward Secure Blind Signature Scheme with Provable Security -- On Delegatability of Four Designated Verifier Signatures -- PIATS: A Partially Sanitizable Signature Scheme -- Cryptographic Protocols --

Ciphertext Comparison, a New Solution to the Millionaire Problem -- Private Itemset Support Counting -- Visual Cryptographic Protocols Using the Trusted Initializer -- Admissible Interference by Typing for Cryptographic Protocols -- Cryptanalysis -- On the Security Bounds of CMC, EME, EME?+? and EME* Modes of Operation -- On the Security of Encryption Modes of MD4, MD5 and HAVAL -- Cryptanalysis of PASS II and MiniPass -- Simple Power Analysis on Fast Modular Reduction with NIST Recommended Elliptic Curves -- Digital Signatures II -- Asymmetric Concurrent Signatures -- Generic Construction of (Identity-Based) Perfect Concurrent Signatures -- Sequential Aggregate Signatures Working over Independent Homomorphic Trapdoor One-Way Permutation Domains -- Network Security -- Session Table Architecture for Defending SYN Flood Attack -- A Behavior-Based Ingress Rate-Limiting Mechanism Against DoS/DDoS Attacks -- Port Scan Behavior Diagnosis by Clustering -- Network Vulnerability Analysis Through Vulnerability Take-Grant Model (VTG) -- Applied Cryptography -- Multiplex Encryption: A Practical Approach to Encrypting Multi-recipient Emails -- Secure Multicast Using Proxy Encryption -- Efficient and Non-interactive Timed-Release Encryption -- Key Management -- Security Properties of Two Authenticated Conference Key Agreement Protocols -- Cryptanalysis of Two User Identification Schemes with Key Distribution Preserving Anonymity -- Enhanced ID-Based Authenticated Key Agreement Protocols for a Multiple Independent PKG Environment -- Access Control -- Enforce Mandatory Access Control Policy on XML Documents -- Network Access Control for Mobile Ad-Hoc Networks -- Remotely Keyed Cryptographics Secure Remote Display Access Using (Mostly) Untrusted Hardware -- Applications -- Authenticating Query Results in Data Publishing -- Multi-Source Stream Authentication Framework in Case of Composite MPEG-4 Stream -- Batching SSL/TLS Handshake Improved -- Achieving Efficient Conjunctive Keyword Searches over Encrypted Data -- Watermarking -- Total Disclosure of the Embedding and Detection Algorithms for a Secure Digital Watermarking Scheme for Audio -- Reversible Watermark with Large Capacity Using the Predictive Coding -- System Security -- PCAV: Internet Attack Visualization on Parallel Coordinates -- Implementation of Packet Filter Configurations Anomaly Detection System with SIERRA -- D_DIPS: An Intrusion Prevention System for Database Security.

Sommario/riassunto

The Seventh International Conference on Information and Communications - curity,ICICS2005,washeldinBeijing,China,10-13December2005. TheICICS conference series is an established forum for exchanging new research ideas and development results in the areas of information security and applied crypt- raphy. The ?rst event began here in Beijing in 1997. Since then the conference series has been interleaving its venues in China and the rest of the world: ICICS 1997 in Beijing, China; ICICS 1999 in Sydney, Australia; ICICS 2001 in Xi'an, China; ICICS 2002 in Singapore; ICICS 2003 in Hohhot City, China; and ICICS 2004 in Malaga, Spain. The conference proceedings of the past events have - ways been published by Springer in the Lecture Notes in Computer Science series, with volume numbers, respectively: LNCS 1334,LNCS 1726,LNCS 2229, LNCS 2513, LNCS 2836, and LNCS 3269. ICICS 2005 was sponsored by the Chinese Academy of Sciences (CAS); the Beijing Natural Science Foundation of China under Grant No. 4052016; the National Natural Science Foundation of China under Grants No. 60083007 and No. 60573042;the NationalGrandFundamentalResearch973ProgramofChina under Grant No. G1999035802, and Hewlett-Packard Laboratories, China. The conference was organized and hosted 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 conference series has been to o?er the attendees the opportunity to discuss the latest developments in theoretical and practical - pects of information and communications security.