1. Record Nr. UNINA9910144344703321

Titolo	Information and Communications Security : 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29, 2004. Proceedings / / edited by Javier López, Eiji Okamoto
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004
ISBN	3-540-30191-7 3-540-23563-9
Edizione	[1st ed. 2004.]
Descrizione fisica	1 online resource (XII, 572 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 3269
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer science—Mathematics Operating systems (Computers) Management information systems Computer science Algorithms Computer communication systems Cryptology Discrete Mathematics in Computer Science Operating Systems Management of Computing and Information Systems Algorithm Analysis and Problem Complexity Computer Communication Networks
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	On the Minimal Assumptions of Group Signature Schemes -- Perfect Concurrent Signature Schemes -- New Identity-Based Ring Signature Schemes -- On the Security of a Multi-party Certified Email Protocol -- Robust Metering Schemes for General Access Structures -- PayFlux – Secure Electronic Payment in Mobile Ad Hoc Networks -- Flexible Verification of MPEG-4 Stream in Peer-to-Peer CDN -- Provably Secure Authenticated Tree Based Group Key Agreement -- Taxonomic

Consideration to OAEP Variants and Their Security -- Factorization-Based Fail-Stop Signatures Revisited -- A Qualitative Evaluation of Security Patterns -- Type Inferability and Decidability of the Security Problem Against Inference Attacks on Object-Oriented Databases -- Volatile Memory Computer Forensics to Detect Kernel Level Compromise -- A Secure Workflow Model Based on Distributed Constrained Role and Task Assignment for the Internet -- Hydan: Hiding Information in Program Binaries -- A Semi-fragile Steganographic Digital Signature for Images -- Identification of Traitors Using a Trellis -- Decentralized Publish-Subscribe System to Prevent Coordinated Attacks via Alert Correlation -- Reflector Attack Traceback System with Pushback Based iTrace Mechanism -- Automatic Covert Channel Analysis of a Multilevel Secure Component -- Sound Approximations to Diffie-Hellman Using Rewrite Rules -- On Randomized Addition-Subtraction Chains to Counteract Differential Power Attacks -- New Power Analysis on the Ha-Moon Algorithm and the MIST Algorithm -- Modified Power-Analysis Attacks on XTR and an Efficient Countermeasure -- Modelling Dependencies Between Classifiers in Mobile Masquerader Detection -- Threat Analysis on NEtwork MObility (NEMO) -- Macro-level Attention to Mobile Agent Security: Introducing the Mobile Agent Secure Hub Infrastructure Concept -- Securing the Destination-Sequenced Distance Vector Routing Protocol (S-DSDV) -- Secret-Public Storage Trade-Off for Broadcast Encryption Key Management -- Security Analysis of the Generalized Self-shrinking Generator -- On Asymptotic Security Estimates in XL and Gröbner Bases-Related Algebraic Cryptanalysis -- On Some Weak Extensions of AES and BES -- Clock Control Sequence Reconstruction in the Ciphertext Only Attack Scenario -- Transient Fault Induction Attacks on XTR -- Adaptive-CCA on OpenPGP Revisited -- A New Key-Insulated Signature Scheme -- Secure Hierarchical Identity Based Signature and Its Application -- Multi-designated Verifiers Signatures -- Dynamic Access Control for Multi-privileged Group Communications -- An Efficient Authentication Scheme Using Recovery Information in Signature -- Time-Scoped Searching of Encrypted Audit Logs -- Rights-Carrying and Self-enforcing Information Objects for Information Distribution Systems.