1. Record Nr. UNISA996466220103316

Titolo	Information security : 5th International Conference, ISC 2002, Sao Paulo, Brazil, September 30-October 2, 2002 : proceedings / / Agnes Hui Chan, Virgil Gligor (eds.)
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [2002] Â©2002
ISBN	3-540-45811-5
Edizione	[1st ed. 2002.]
Descrizione fisica	1 online resource (511 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2433
Disciplina	005.8
Soggetti	Computers - Access control Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intrusion Detection and Tamper Resistance -- Real-Time Intruder Tracing through Self-Replication -- On the Difficulty of Protecting Private Keys in Software -- Intrusion Detection with Support Vector Machines and Generative Models -- Cryptographic Algorithm and Attack Implementation -- Small and High-Speed Hardware Architectures for the 3GPP Standard Cipher KASUMI -- Fast Software Implementations of SC2000 -- Comparative Analysis of the Hardware Implementations of Hash Functions SHA-1 and SHA-512 -- Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG -- Access Control and Trust Management (I) -- Role-Based Access Control for E-commerce Sea-of-Data Applications -- An Access Control Model for Tree Data Structures -- A New Design of Privilege Management Infrastructure for Organizations Using Outsourced PKI -- Authentication and Privacy -- Password Authenticated Key Exchange Based on RSA for Imbalanced Wireless Networks -- Quantifying Privacy Leakage through Answering Database Queries -- A New Offiine Privacy Protecting E-cash System with Revokable Anonymity -- E-commerce Protocols (I) -- Receipt-Free Sealed-Bid Auction -- Exclusion-Freeness in Multi-party Exchange Protocols -- A Realistic Protocol for Multi-party Certified Electronic Mail -- Signature Schemes -- A Nyberg-Rueppel Signature for Multiple Messages and Its Batch Verification --

Comments to the UNCITRAL Model Law on Electronic Signatures -- An Anonymous Loan System Based on Group Signature Scheme -- Traceability Schemes for Signed Documents* -- Cryptography (I) -- Proofs of Knowledge for Non-monotone Discrete-Log Formulae and Applications -- Inversion/Division Systolic Architecture for Public-Key Cryptosystems in GF(2m) -- Efficient Bit Serial Multiplication Using Optimal Normal Bases of Type II in GF(2m) -- Access Control and Trust Management (II) -- Conditional Cryptographic Delegation for P2P Data Sharing -- Certification of Public Keys within an Identity Based System -- A New Public Key Cryptosystem for Constrained Hardware -- Key Management -- A Distributed and Computationally Secure Key Distribution Scheme* -- On Optimal Hash Tree Traversal for Interval Time-Stamping -- An Efficient Dynamic and Distributed Cryptographic Accumulator* -- Security Analysis -- A Second-Order DPA Attack Breaks a Window-Method Based Countermeasure against Side Channel Attacks -- Parallelizable Elliptic Curve Point Multiplication Method with Resistance against Side-Channel Attacks -- Automated Analysis of Some Security Mechanisms of SCEP* -- An Attack on a Protocol for Certified Delivery -- E-commerce Protocols (II) -- Oblivious Counter and Majority Protocol -- Efficient Mental Card Shuffling via Optimised Arbitrary-Sized Benes Permutation Network -- Fingerprinting Concatenated Codes with Efficient Identification -- Cryptography (II) -- A Provably Secure Additive and Multiplicative Privacy Homomorphism* -- Algorithms for Efficient Simultaneous Elliptic Scalar Multiplication with Reduced Joint Hamming Weight Representation of Scalars.

Sommario/riassunto

As distinct from other security and cryptography conferences, the Information Security Conference (ISC) 2002 brought together individuals involved in a wide variety of different disciplines of information security to foster the exchange of ideas. The conference is an outgrowth of the Information Security Workshop, first held in Ishikawa, Japan 1997. ISC 2002 was held in Sao Paulo, Brazil, on September 30– October 2, 2002. The Program Committee considered 81 submissions of which 38 papers were accepted for presentation. These proceedings contain revised versions of the accepted papers. The papers provide a representative sample of both the variety and the truly international scope of information security research conducted currently. The topics addressed range from e-commerce protocols to access control and trust management, and to cryptography and cryptographic algorithms. Many people deserve our gratitude for their contribution to the success of the conference. We would like to thank the General Chair, Routo Terada, for overseeing the local arrangements, including registration and maintaining the conference website, and for the smooth running of the conference. We are grateful to Robbie Ye for his expert help in processing the electronic submissions, reviews and acceptance notifications. Robbie’s enthusiasm and energy greatly simplified the Program Committee’s task of conducting the on-line evaluation of the submitted papers under tight time constraints.