1. Record Nr.	UNINA9910143895903321
Titolo	Information and Communications Security : 4th International Conference, ICICS 2002, Singapore, December 9-12, 2002, Proceedings / / edited by Robert H. Deng, Feng Bao, Jianying Zhou
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2002
ISBN	3-540-36159-6
Edizione	[1st ed. 2002.]
Descrizione fisica	1 online resource (XII, 500 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 2513
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer communication systems Operating systems (Computers) Computer science—Mathematics Management information systems Computer science Cryptology Computer Communication Networks Operating Systems Discrete Mathematics in Computer Science 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	System Security I -- Defenses against the Truncation of Computation Results of Free-Roaming Agents -- A Distributed Dynamic ?Firewall Architecture with Mobile Agents and KeyNote Trust Management System -- Encoding Function Pointers and Memory Arrangement Checking against Buffer Overflow Attack -- An Evaluation of Different IP Traceback Approaches -- Security against Inference Attacks on Negative Information in Object-Oriented Databases -- Cryptosystem I -- Robust Key-Evolving Public Key Encryption Schemes -- A Group Signature Scheme Committing the Group -- Unconditionally Secure Key Insulated Cryptosystems: Models, Bounds and Constructions --

Anonymous Fingerprinting as Secure as the Bilinear Diffie-Hellman Assumption -- Reducing the Memory Complexity of Type-Inference Algorithms -- Security Protocol I -- The Risks of Compromising Secret Information -- Password-Authenticated Key Exchange between Clients with Different Passwords -- Robust, Privacy Protecting and Publicly Verifiable Sealed-Bid Auction -- Attacking Predictable IPsec ESP Initialization Vectors -- Fingerprinting & Watermarking -- An ID Coding Scheme for Fingerprinting, Randomized c-Secure CRT Code -- A Robust Block Oriented Watermarking Scheme in Spatial Domain -- A Flexibly Revocable Key-Distribution Scheme for Efficient Black-Box Tracing -- Efficient Implementation of Algorithms -- Low Complexity Bit Serial Systolic Multipliers over GF(2m) for Three Classes of Finite Fields -- Fast Elliptic Curve Multiplications with SIMD Operations -- Further Results on Multiples of Primitive Polynomials and Their Products over GF(2) -- System Security II -- A Secure Object Sharing Scheme for Java Card -- IDS Interoperability and Correlation Using IDMEF and Commodity Systems -- A Synthetic Fraud Data Generation Methodology -- User Interaction Design for Secure Systems -- Using Independent Auditors as Intrusion Detection Systems -- Cryptosystem II -- Cellular Automata Based Cryptosystem (CAC) -- New Weak-Key Classes of IDEA -- Risks with Raw-Key Masking — The Security Evaluation of 2-Key XCBC -- A New Statistical Testing for Symmetric Ciphers and Hash Functions -- Message Authentication Codes with Error Correcting Capabilities -- Access Control -- The Consistency of an Access Control List -- Knowledge-Based Modeling and Simulation of Network Access Control Mechanisms Representing Security Policies -- A Specification Language for Distributed Policy Control -- Access Control Infrastructure for Digital Objects -- Security Protocol II -- Distributed Key Generation as a Component of an Integrated Protocol -- A Secure Agent-Mediated Payment Protocol -- Cryptanalysis & Cryptographic Techniques -- Tensor Transform of Boolean Functions and Related Algebraic and Probabilistic Properties -- Related-Cipher Attacks -- A Chosen Plaintext Linear Attack on Block Cipher CIKS-1 -- Ideal Threshold Schemes from Orthogonal Arrays -- Cryptanalysis of the Reduced-Round RC6.

Sommario/riassunto

This volume contains the proceedings of the 4th International Conference on information and Communications Security (ICICS2002). The three previous conferences were held in Beijing(ICICS97), Sydney (ICICS99) and Xian(ICICS01), where we had an enthusiastic and well-attended event. ICICS2002 is sponsored and organized by the Laboratories for Information Technology, Singapore, in co-operation with the Engineering Research Center for Information Security Technology of the Chinese Academy of Sciences and the International Communications and Information Security Association (ICISA). During the past five years the conference has placed equal emphasis on the theoretical and practical aspects of information and communications security and has established itself as a forum at which academic and industrial people meet and discuss emerging security challenges and solutions. We hope to uphold this tradition by offering you yet another successful meeting with a rich and interesting program. The response to the Call For Papers was overwhelming, 161 paper submissions were received. Therefore, the paper selection process was very competitive and difficult–only 41 papers were accepted and many good papers had to be rejected. The success of the conference depends on the quality of the program. We are indebted to our program committee members and the external referees for the wonderful job they did.