1. Record Nr. UNISA996465773503316

Titolo	Applied Cryptography and Network Security [[electronic resource]] : First International Conference, ACNS 2003. Kunming, China, October 16-19, 2003, Proceedings / / edited by Jianying Zhou, Moti Yung, Yongfei Han
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2003
ISBN	3-540-45203-6
Edizione	[1st ed. 2003.]
Descrizione fisica	1 online resource (XII, 440 p.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 2846
Disciplina	005.8/2
Soggetti	Computer networks Cryptography Data encryption (Computer science) Operating systems (Computers) Computers and civilization Electronic data processing—Management Computer Communication Networks Cryptology Operating Systems Computers and Society IT Operations
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	Cryptographic Applications -- Multi-party Computation from Any Linear Secret Sharing Scheme Unconditionally Secure against Adaptive Adversary: The Zero-Error Case -- Optimized ? 2-Attack against RC6 -- Anonymity-Enhanced Pseudonym System -- Intrusion Detection -- Using Feedback to Improve Masquerade Detection -- Efficient Presentation of Multivariate Audit Data for Intrusion Detection of Web-Based Internet Services -- An IP Traceback Scheme Integrating DPM and PPM -- Cryptographic Algorithms -- Improved Scalable Hash Chain Traversal -- Round Optimal Distributed Key Generation of Threshold Cryptosystem Based on Discrete Logarithm Problem -- On the Security

of Two Threshold Signature Schemes with Traceable Signers -- Digital Signature -- Proxy and Threshold One-Time Signatures -- A Threshold GQ Signature Scheme -- Generalized Key-Evolving Signature Schemes or How to Foil an Armed Adversary -- A Ring Signature Scheme Based on the Nyberg-Rueppel Signature Scheme -- Security Modelling -- Modelling and Evaluating Trust Relationships in Mobile Agents Based Systems -- An Authorization Model for E-consent Requirement in a Health Care Application -- PLI: A New Framework to Protect Digital Content for P2P Networks -- Web Security -- Improved Algebraic Traitor Tracing Scheme -- Common Vulnerability Markup Language -- Trust on Web Browser: Attack vs. Defense -- Security Protocols -- Security Protocols for Biometrics-Based Cardholder Authentication in Smartcards -- Does It Need Trusted Third Party? Design of Buyer-Seller Watermarking Protocol without Trusted Third Party -- Using OCSP to Secure Certificate-Using Transactions in M-commerce -- Cryptanalysis -- Differential Fault Analysis on A.E.S -- Side-Channel Attack on Substitution Blocks -- Timing Attack against Implementation of a Parallel Algorithm for Modular Exponentiation -- A Fast Correlation Attack for LFSR-Based Stream Ciphers -- Key Management -- Making the Key Agreement Protocol in Mobile ad hoc Network More Efficient -- An Efficient Tree-Based Group Key Agreement Using Bilinear Map -- A Key Recovery Mechanism for Reliable Group Key Management -- Efficient Implementations -- Efficient Software Implementation of LFSR and Boolean Function and Its Application in Nonlinear Combiner Model -- Efficient Distributed Signcryption Scheme as Group Signcryption -- Architectural Enhancements for Montgomery Multiplication on Embedded RISC Processors.

Sommario/riassunto

The 1st International Conference on “Applied Cryptography and Network Se- rity” (ACNS 2003) was sponsored and organized by ICISA (International Communications and Information Security Association), in cooperation with MiAn Pte. Ltd. and the Kunming government. It was held in Kunming, China in October 2003. The conference proceedings was published as Volume 2846 of the Lecture Notes in Computer Science (LNCS) series of Springer-Verlag. The conference received 191 submissions, from 24 countries and regions; 32 of these papers were accepted, representing 15 countries and regions (acceptance rate of 16.75%). In this volume you will ?nd the revised versions of the accepted papers that were presented at the conference. In addition to the main track of presentations of accepted papers, an additional track was held in the conference where presentations of an industrial and technical nature were given. These presentations were also carefully selected from a large set of presentation proposals. This new international conference series is the result of the vision of Dr. Yongfei Han. The conference concentrates on current developments that advance the - eas of applied cryptography and its application to systems and network security. The goal is to represent both academic research works and developments in industrial and technical frontiers. We thank Dr. Han for initiating this conference and for serving as its General Chair.