1. Record Nr. UNINA9910144150803321

| | |
|---|---|
| Titolo | Applied Cryptography and Network Security : Second International Conference, ACNS 2004, Yellow Mountain, China, June 8-11, 2004. Proceedings / / edited by Markus Jakobsson, Moti Yung, Jianying Zhou |
| Pubbl/distr/stampa | Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2004 |
| ISBN | 9783540248528<br>3-540-24852-8 |
| Edizione | [1st ed. 2004.] |
| Descrizione fisica | 1 online resource (XIII, 511 p.) |
| Collana | Lecture Notes in Computer Science, , 1611-3349 ; ; 3089 |
| Disciplina | 005.8 |
| Soggetti | Cryptography<br>Data encryption (Computer science)<br>Computer networks<br>Operating systems (Computers)<br>Information storage and retrieval systems<br>Application software<br>Electronic data processing—Management<br>Cryptology<br>Computer Communication Networks<br>Operating Systems<br>Information Storage and Retrieval<br>Computer and Information Systems Applications<br>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 | Security and Storage -- CamouflageFS: Increasing the Effective Key Length in Cryptographic Filesystems on the Cheap -- Private Keyword-Based Push and Pull with Applications to Anonymous Communication -- Secure Conjunctive Keyword Search over Encrypted Data -- Provably Secure Constructions -- Evaluating Security of Voting Schemes in the Universal Composability Framework -- Verifiable Shuffles: A Formal Model and a Paillier-Based Efficient Construction with Provable Security |

-- On the Security of Cryptosystems with All-or-Nothing Transform -- Internet Security -- Centralized Management of Virtual Security Zones in IP Networks -- S-RIP: A Secure Distance Vector Routing Protocol -- A Pay-per-Use DoS Protection Mechanism for the Web -- Digital Signature -- Limited Verifier Signature from Bilinear Pairings -- Deniable Ring Authentication Revisited -- A Fully-Functional Group Signature Scheme over Only Known-Order Group -- Security Modelling -- Some Observations on Zap and Its Applications -- Security Measurements of Steganographic Systems -- X2Rep: Enhanced Trust Semantics for the XRep Protocol -- Authenticated Key Exchange -- One-Round Protocols for Two-Party Authenticated Key Exchange -- Password Authenticated Key Exchange Using Quadratic Residues -- Key Agreement Using Statically Keyed Authenticators -- Security of Deployed Systems -- Low-Latency Cryptographic Protection for SCADA Communications -- A Best Practice for Root CA Key Update in PKI -- SQLrand: Preventing SQL Injection Attacks -- Cryptosystems: Design and Analysis -- Cryptanalysis of a Knapsack Based Two-Lock Cryptosystem -- Success Probability in ? 2-Attacks -- More Generalized Clock-Controlled Alternating Step Generator -- Cryptographic Protocols -- FDLKH: Fully Decentralized Key Management Scheme on Logical Key Hierarchy -- Unconditionally Non-interactive Verifiable Secret Sharing Secure against Faulty Majorities in the Commodity Based Model -- Cryptanalysis of Two Anonymous Buyer-Seller Watermarking Protocols and an Improvement for True Anonymity -- Side Channels and Protocol Analysis -- Security Analysis of CRT-Based Cryptosystems -- Cryptanalysis of the Countermeasures Using Randomized Binary Signed Digits -- Weaknesses of a Password-Authenticated Key Exchange Protocol between Clients with Different Passwords -- Intrusion Detection and DoS -- Advanced Packet Marking Mechanism with Pushback for IP Traceback -- A Parallel Intrusion Detection System for High-Speed Networks -- A Novel Framework for Alert Correlation and Understanding -- Cryptographic Algorithms -- An Improved Algorithm for uP+vQ Using JSF -- New Table Look-Up Methods for Faster Frobenius Map Based Scalar Multiplication Over GF(p n ) -- Batch Verification for Equality of Discrete Logarithms and Threshold Decryptions.

Sommario/riassunto

The second International Conference on Applied Cryptography and Network Security (ACNS 2004) was sponsored and organized by ICISA (the International Communications and Information Security Association). It was held in Yellow Mountain, China, June 8–11, 2004. The conference proceedings, representing papers from the academic track, are published in this volume of the Lecture Notes in Computer Science (LNCS) of Springer-Verlag. The area of research that ACNS covers has been gaining importance in recent years due to the development of the Internet, which, in turn, implies global exposure of computing resources. Many ?elds of research were covered by the program of this track, presented in this proceedings volume. We feel that the papers herein indeed re?ect the state of the art in security and cryptography research, worldwide. The program committee of the conference received a total of 297 submissions from all over the world, of which 36 submissions were selected for presentation during the academic track. In addition to this track, the conference also hosted a technical/industrial track of presentations that were carefully selected as well. All submissions were reviewed by experts in the relevant areas.