1. Record Nr. UNISA996465520103316

Titolo	Applied Cryptography and Network Security [[electronic resource]] : 4th International Conference, ACNS 2006, Singapore, June 6-9, 2006, Proceedings / / edited by Jianying Zhou, Moti Yung, Feng Bao
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2006
ISBN	3-540-34704-6
Edizione	[1st ed. 2006.]
Descrizione fisica	1 online resource (XIV, 490 p.)
Collana	Security and Cryptology ; ; 3989
Disciplina	005.8
Soggetti	Computer networks Cryptography Data encryption (Computer science) Operating systems (Computers) Application software Computers and civilization Electronic data processing—Management Computer Communication Networks Cryptology Operating Systems Computer and Information Systems Applications 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	Intrusion Avoidance and Detection -- Adaptive Detection of Local Scanners -- Probabilistic Proof of an Algorithm to Compute TCP Packet Round-Trip Time for Intrusion Detection -- DSO: Dependable Signing Overlay -- Cryptographic Applications -- Do Broken Hash Functions Affect the Security of Time-Stamping Schemes? -- A Handy Multi-coupon System -- An Efficient Single-Key Pirates Tracing Scheme Using Cover-Free Families -- DoS: Attacks and Countermeasures -- Efficient Memory Bound Puzzles Using Pattern Databases -- Effect of Malicious

Synchronization -- Misusing Unstructured P2P Systems to Perform DoS Attacks: The Network That Never Forgets -- Key Management -- Password Based Server Aided Key Exchange -- Secure Password-Based Authenticated Group Key Agreement for Data-Sharing Peer-to-Peer Networks -- Stateful Subset Cover -- Cryptanalysis -- The Rainbow Attack on Stream Ciphers Based on Maiorana-McFarland Functions -- Breaking a New Instance of TTM Cryptosystems -- Cryptanalysis of the N-Party Encrypted Diffie-Hellman Key Exchange Using Different Passwords -- Security of Limited Devices -- An AES Smart Card Implementation Resistant to Power Analysis Attacks -- Physical Security Bounds Against Tampering -- Flexible Exponentiation with Resistance to Side Channel Attacks -- Cryptography -- An Improved Poly1305 MAC -- Certificateless Public-Key Signature: Security Model and Efficient Construction -- High Diffusion Cipher: Encryption and Error Correction in a Single Cryptographic Primitive -- Authentication and Web Security -- Authentication for Paranoids: Multi-party Secret Handshakes -- On the Security of the Authentication Module of Chinese WLAN Standard Implementation Plan -- W3Bcrypt: Encryption as a Stylesheet -- Ad Hoc and Sensor Network Security -- Combinatorial Structures for Design of Wireless Sensor Networks -- Public Key Cryptography Sans Certificates in Ad Hoc Networks -- Location-Aware Key Management Using Multi-layer Grids for Wireless Sensor Networks -- Cryptographic Constructions -- A General Methodology for Pipelining the Point Multiplication Operation in Curve Based Cryptography -- Results on Almost Resilient Functions -- Real Perfect Contrast Visual Secret Sharing Schemes with Reversing -- Security and Privacy -- On Optimizing the Security-Throughput Trade-Off in Wireless Networks with Adversaries -- Improving the Randomized Initial Point Countermeasure Against DPA -- Syntax-Driven Private Evaluation of Quantified Membership Queries.

Sommario/riassunto

The 4th International Conference on Applied Cryptography and Network Security(ACNS 2006)washeldin Singapore,during June6-9,2006.ACNS 2006 brought together individuals from academia and industry involved in multiple research disciplines of cryptography and security to foster exchange of ideas. This volume (LNCS 3989) contains papers presented in the academic track. ACNS was set a high standard when it was initiated in 2003. There has been a steady improvement in the quality of its program in the past 4 years: ACNS 2003 (Kunming, China), ACNS 2004 (Yellow Mountain, China), ACNS 2005 (New York, USA), ACNS 2006 (Singapore). The average acc- tance rate is kept at around 16%. We wish to receive the continued support from the community of cryptographyand security worldwide to further improve its quality and make ACNS one of the leading conferences. The Program Committee of ACNS 2006 received a total of 218 submissions fromalloverthe world, ofwhich33wereselectedforpresentationattheacademic track. In addition to this track, the conference also hosted an industrial track of presentations that were carefully selected as well. All submissions were reviewed by experts in the relevant areas. We are indebted to our Program Committee members and the external reviewers for the great job they have performed. The proceedings contain revised versions of the accepted papers. However, revisions were not checked and the authors bear full responsibility for the content of their papers.