

1. Record Nr.	UNISA996466127903316
Titolo	Applied Cryptography and Network Security [[electronic resource]] : Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings // edited by John Ioannidis, Angelos D. Keromytis, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XII, 530 p.)
Collana	Security and Cryptology ; ; 3531
Disciplina	005.8/2
Soggetti	Computer networks Cryptography Data encryption (Computer science) Operating systems (Computers) Information storage and retrieval systems Application software Electronic data processing—Management Computer Communication Networks Cryptography Operating Systems Information Storage and Retrieval Computer and Information Systems Applications 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	Two-Server Password-Only Authenticated Key Exchange -- Strengthening Password-Based Authentication Protocols Against Online Dictionary Attacks -- Cryptanalysis of an Improved Client-to-Client Password-Authenticated Key Exchange (C2C-PAKE) Scheme -- Efficient Security Mechanisms for Overlay Multicast-Based Content Distribution -- A Traitor Tracing Scheme Based on RSA for Fast Decryption -- N-Party Encrypted Diffie-Hellman Key Exchange Using Different

Passwords -- Messin' with Texas Deriving Mother's Maiden Names
Using Public Records -- Mitigating Network Denial-of-Service Through
Diversity-Based Traffic Management -- Searching for High-Value Rare
Events with Uncheatable Grid Computing -- Digital Signatures Do Not
Guarantee Exclusive Ownership -- Thompson's Group and Public Key
Cryptography -- Rainbow, a New Multivariable Polynomial Signature
Scheme -- Badger -- A Fast and Provably Secure MAC -- IDS False Alarm
Reduction Using Continuous and Discontinuous Patterns -- Indexing
Information for Data Forensics -- Model Generalization and Its
Implications on Intrusion Detection -- Intrusion-Resilient Secure
Channels -- Optimal Asymmetric Encryption and Signature Paddings --
Efficient and Leakage-Resilient Authenticated Key Transport Protocol
Based on RSA -- Identity Based Encryption Without Redundancy --
OACerts: Oblivious Attribute Certificates -- Dynamic k-Times
Anonymous Authentication -- Efficient Anonymous Roaming and Its
Security Analysis -- Quantifying Security in Hybrid Cellular Networks --
Off-Line Karma: A Decentralized Currency for Peer-to-peer and Grid
Applications -- Building Reliable Mix Networks with Fair Exchange --
SCARE of the DES -- Robust Key Extraction from Physical Uncloneable
Functions -- Efficient Constructions for One-Way Hash Chains --
Privacy Preserving Keyword Searches on Remote Encrypted Data -- An
Efficient Solution to the Millionaires' Problem Based on Homomorphic
Encryption -- Non-interactive Zero-Knowledge Arguments for Voting
-- Short Signature and Universal Designated Verifier Signature Without
Random Oracles -- Efficient Identity Based Ring Signature -- New
Signature Schemes with Coupons and Tight Reduction.

Sommario/riassunto

The 3rd International Conference on Applied Cryptography and
Network Security (ACNS 2005) was sponsored and organized by ICISA
(the International Commu- cations and Information Security
Association). It was held at Columbia University in New York, USA, June
7–10, 2005. This conference proceedings volume contains papers
presented in the academic/research track. ACNS covers a large number
of research areas that have been gaining importance in recent years
due to the development of the Internet, wireless communication and
the increased global exposure of computing resources. The papers in
this volume are representative of the state of the art in security and
cryptography research, worldwide. The Program Committee of the
conference received a total of 158 submissions from all over the world,
of which 35 submissions were selected for presentation at the a-
demic track. In addition to this track, the conference also hosted a technical/
industrial/ short papers track whose presentations were also carefully
selected from among the submissions. All submissions were reviewed
by experts in the relevant areas.
