1. Record Nr. UNISA996465979303316

Titolo	Applied Cryptography and Network Security [[electronic resource]] : 7th International Conference, ACNS 2009, Paris-Rocquencourt, France, June 2-5, 2009, Proceedings / / edited by Michel Abdalla, David Pointcheval, Pierre-Alain Fouque, Damien Vergnaud
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2009
ISBN	3-642-01957-9
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XIII, 535 p.)
Collana	Security and Cryptology ; ; 5536
Disciplina	005.8
Soggetti	Data encryption (Computer science) Computer communication systems Computer security Application software Coding theory Information theory Data structures (Computer science) Cryptology Computer Communication Networks Systems and Data Security Information Systems Applications (incl. Internet) Coding and Information Theory Data Structures and Information Theory
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	Key Exchange -- Group Key Exchange Enabling On-Demand Derivation of Peer-to-Peer Keys -- Session-state Reveal Is Stronger Than Ephemeral Key Reveal: Attacking the NAXOS Authenticated Key Exchange Protocol -- Secure Pairing of “Interface-Constrained” Devices Resistant against Rushing User Behavior -- How to Extract and Expand Randomness: A Summary and Explanation of Existing Results -- Secure Computation -- Novel Precomputation Schemes for Elliptic Curve

Cryptosystems -- Practical Secure Evaluation of Semi-private Functions -- Secure Hamming Distance Based Computation and Its Applications -- Efficient Robust Private Set Intersection -- Public-Key Encryption -- A New Variant of the Cramer-Shoup KEM Secure against Chosen Ciphertext Attack -- An Efficient Identity-Based Online/Offline Encryption Scheme -- Dual-Policy Attribute Based Encryption -- Construction of Threshold Public-Key Encryptions through Tag-Based Encryptions -- Network Security I -- Malyzer: Defeating Anti-detection for Application-Level Malware Analysis -- A New Message Recognition Protocol with Self-recoverability for Ad Hoc Pervasive Networks -- Traitor Tracing -- Breaking Two k-Resilient Traitor Tracing Schemes with Sublinear Ciphertext Size -- Tracing and Revoking Pirate Rebroadcasts -- Authentication and Anonymity -- Efficient Deniable Authentication for Signatures -- Homomorphic MACs: MAC-Based Integrity for Network Coding -- Algorithmic Tamper Proof (ATP) Counter Units for Authentication Devices Using PIN -- Performance Measurements of Tor Hidden Services in Low-Bandwidth Access Networks -- Hash Functions -- Cryptanalysis of Twister -- Cryptanalysis of CubeHash -- Collision Attack on Boole -- Network Security II -- Integrity Protection for Revision Control -- Fragility of the Robust Security Network: 802.11 Denial of Service -- Fast Packet Classification Using Condition Factorization -- Lattices -- Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches -- Broadcast Attacks against Lattice-Based Cryptosystems -- Partial Key Exposure Attack on CRT-RSA -- Side-Channel Attacks -- How to Compare Profiled Side-Channel Attacks? -- Theoretical and Practical Aspects of Mutual Information Based Side Channel Analysis -- Attacking ECDSA-Enabled RFID Devices.

Sommario/riassunto

This book constitutes the refereed proceedings of the 7th International Conference on Applied Cryptography and Network Security, ACNS 2009, held in Paris-Rocquencourt, France, in June 2009. The 32 revised full papers presented were carefully reviewed and selected from 150 submissions. The papers are organized in topical sections on key exchange, secure computation, public-key encryption, network security, traitor tracing, authentication and anonymity, hash fundtions, lattices, and side-channel attacks.