

1. Record Nr.	UNISA996465668703316
Titolo	Applied Cryptography and Network Security [[electronic resource]] : 8th International Conference, ACNS 2010, Beijing, China, June 22-25, 2010, Proceedings // edited by Jianying Zhou, Moti Yung
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-38725-4 9786613565174 3-642-13708-3
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (XIII, 564 p. 83 illus.)
Collana	Security and Cryptology ; ; 6123
Disciplina	005.8
Soggetti	Computer networks Cryptography Data encryption (Computer science) Computer science—Mathematics Discrete mathematics Electronic data processing—Management Algorithms Data protection Computer Communication Networks Cryptography Discrete Mathematics in Computer Science IT Operations Data and Information Security
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	Public Key Encryption -- On the Broadcast and Validity-Checking Security of pkcs#1 v1.5 Encryption -- How to Construct Interval Encryption from Binary Tree Encryption -- Shrinking the Keys of Discrete-Log-Type Lossy Trapdoor Functions -- Digital Signature -- Trapdoor Sanitizable Signatures Made Easy -- Generic Constructions for Verifiably Encrypted Signatures without Random Oracles or NIZKs --

Redactable Signatures for Tree-Structured Data: Definitions and Constructions -- Block Ciphers and Hash Functions -- Impossible Differential Cryptanalysis on Feistel Ciphers with SP and SPS Round Functions -- Multi-trail Statistical Saturation Attacks -- Multiset Collision Attacks on Reduced-Round SNOW 3G and SNOW 3G??? -- High Performance GHASH Function for Long Messages -- Side-Channel Attacks -- Principles on the Security of AES against First and Second-Order Differential Power Analysis -- Adaptive Chosen-Message Side-Channel Attacks -- Secure Multiplicative Masking of Power Functions -- Zero Knowledge and Multi-party Protocols -- Batch Groth-Sahai -- Efficient and Secure Evaluation of Multivariate Polynomials and Applications -- Efficient Implementation of the Orlandi Protocol -- Improving the Round Complexity of Traitor Tracing Schemes -- Key Management -- Password Based Key Exchange Protocols on Elliptic Curves Which Conceal the Public Parameters -- Okamoto-Tanaka Revisited: Fully Authenticated Diffie-Hellman with Minimal Overhead -- Deniable Internet Key Exchange -- Authentication and Identification -- A New Human Identification Protocol and Coppersmith's Baby-Step Giant-Step Algorithm -- Secure Sketch for Multiple Secrets -- A Message Recognition Protocol Based on Standard Assumptions -- Privacy and Anonymity -- Affiliation-Hiding Key Exchange with Untrusted Group Authorities -- Privacy-Preserving Group Discovery with Linear Complexity -- Two New Efficient PIR-Writing Protocols -- Regulatory Compliant Oblivious RAM -- RFID Security and Privacy -- Revisiting Unpredictability-Based RFID Privacy Models -- On RFID Privacy with Mutual Authentication and Tag Corruption -- Internet Security -- Social Network-Based Botnet Command-and-Control: Emerging Threats and Countermeasures -- COP: A Step toward Children Online Privacy -- A Hybrid Method to Detect Deflation Fraud in Cost-Per-Action Online Advertising.

Sommario/riassunto

ACNS 2010, the 8th International Conference on Applied Cryptography and Network Security, was held in Beijing, China, during June 22-25, 2010. ACNS 2010 brought together individuals from academia and industry involved in multiple research disciplines of cryptography and security to foster the exchange of ideas. ACNS was initiated in 2003, and there has been a steady improvement in the quality of its program over the past 8 years: ACNS 2003 (Kunming, China), ACNS 2004 (Yellow Mountain, China), ACNS 2005 (New York, USA), ACNS 2006 (Singapore), ACNS 2007 (Zhuhai, China), ACNS 2008 (New York, USA), ACNS2009 (Paris, France). The average acceptance rate has been kept at around 17%, and the average number of participants has been kept at around 100. The conference received a total of 178 submissions from all over the world. Each submission was assigned to at least three committee members. Submissions co-authored by members of the Program Committee were assigned to at least four committee members. Due to the large number of high-quality submissions, the review process was challenging and we are deeply grateful to the committee members and the external reviewers for their outstanding work. After extensive discussions, the Program Committee selected 32 submissions for presentation in the academic track, and these are the articles that are included in this volume (LNCS 6123). Additionally, a few other submissions were selected for presentation in the non-archival industrial track.
