1. Record Nr. UNINA9910483820803321

Titolo	Applied cryptography and network security : 6th international conference, ACNS 2008, New York, NY, USA, June 3-6, 2008 : proceedings / / Steven M. Bellovin ... [et al.] (eds.)
Pubbl/distr/stampa	Berlin ; ; New York, : Springer, 2008
ISBN	3-540-68914-1
Edizione	[1st ed. 2008.]
Descrizione fisica	1 online resource (XI, 508 p.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 5037 LNCS sublibrary. SL 4, Security and cryptology
Altri autori (Persone)	BellovinSteven M
Disciplina	005.8
Soggetti	Telecommunication - Security measures Data encryption (Computer science) Cryptography
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	On the Effectiveness of Internal Patching Against File-Sharing Worms -- Peeking Through the Cloud: DNS-Based Estimation and Its Applications -- Pushback for Overlay Networks: Protecting Against Malicious Insiders -- PPAA: Peer-to-Peer Anonymous Authentication -- Generic Constructions of Stateful Public Key Encryption and Their Applications -- Traceable and Retrievable Identity-Based Encryption -- Attribute-Based Encryption with Partially Hidden Encryptor-Specified Access Structures -- Attacking Reduced Round SHA-256 -- Dakota – Hashing from a Combination of Modular Arithmetic and Symmetric Cryptography -- Getting the Best Out of Existing Hash Functions; or What if We Are Stuck with SHA? -- Replay Attack in a Fair Exchange Protocol -- Improved Conditional E-Payments -- Anonymity in Transferable E-cash -- Generic Security-Amplifying Methods of Ordinary Digital Signatures -- New Differential-Algebraic Attacks and Reparametrization of Rainbow -- Trapdoor Sanitizable Signatures and Their Application to Content Protection -- Multi-factor Authenticated Key Exchange -- Repelling Detour Attack Against Onions with Re-encryption -- Analysis of EAP-GPSK Authentication Protocol -- Efficient Device Pairing Using “Human-Comparable” Synchronized Audiovisual Patterns -- PUF-HB: A Tamper-Resilient HB Based Authentication

Protocol -- An Authentication Scheme Based on the Twisted Conjugacy Problem -- Restricted Queries over an Encrypted Index with Applications to Regulatory Compliance -- A Practical and Efficient Tree-List Structure for Public-Key Certificate Validation -- On the Security of the CCM Encryption Mode and of a Slight Variant -- wNAF *, an Efficient Left-to-Right Signed Digit Recoding Algorithm -- A Very Compact “Perfectly Masked” S-Box for AES -- Steel, Cast Iron and Concrete: Security Engineering for Real World Wireless Sensor Networks -- Traceable Privacy of Recent Provably-Secure RFID Protocols -- The Security of EPC Gen2 Compliant RFID Protocols.

Sommario/riassunto

This book constitutes the refereed proceedings of the 6th International Conference on Applied Cryptography and Network Security, ACNS 2008, held in New York, NY, USA, in June 2008. The 30 revised full papers presented were carefully reviewed and selected from 131 submissions. The papers address all aspects of applied cryptography and network security with special focus on novel paradigms, original directions, and non-traditional perspectives.