1. Record Nr. UNINA9910483950503321

Titolo	Security and cryptography for networks : 7th International Conference, SCN 2010, Amalfi, Italy, September 13-15, 2010 : proceedings / / Juan A. Garay, Roberto De Prisco (eds.)
Pubbl/distr/stampa	Berlin ; ; New York, : Springer, 2010
ISBN	3-642-15317-8
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (VII, 474 p. 54 illus.)
Collana	LNCS sublibrary. SL 4, Security and cryptology Lecture notes in computer science, , 0302-9743 ; ; 6280
Altri autori (Persone)	GarayJuan A De PriscoRoberto
Disciplina	005.8
Soggetti	Computer networks - Security measures Computer security 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	Encryption I -- Time-Specific Encryption -- Public-Key Encryption with Efficient Amortized Updates -- Generic Constructions of Parallel Key-Insulated Encryption -- Invited Talk -- Heuristics and Rigor in Lattice-Based Cryptography -- Cryptanalysis -- Differential Fault Analysis of LEX -- Generalized RC4 Key Collisions and Hash Collisions -- Hash Functions -- On the Indifferentiability of the Grøstl Hash Function -- Side Channel Attacks and Leakage Resilience -- Algorithmic Tamper-Proof Security under Probing Attacks -- Leakage-Resilient Storage -- Encryption II -- Searching Keywords with Wildcards on Encrypted Data -- Threshold Attribute-Based Signcryption -- Cryptographic Protocols I -- Efficiency-Improved Fully Simulatable Adaptive OT under the DDH Assumption -- Improved Primitives for Secure Multiparty Integer Computation -- How to Pair with a Human -- Authentication and Key Agreement -- A New Security Model for Authenticated Key Agreement -- A Security Enhancement and Proof for Authentication and Key Agreement (AKA) -- Authenticated Key Agreement with Key Re-use in the Short Authenticated Strings Model -- Cryptographic Primitives and Schemes -- Kleptography from Standard Assumptions and Applications

-- Provably Secure Convertible Undeniable Signatures with Unambiguity -- History-Free Aggregate Message Authentication Codes -- Lattice-Based Cryptography -- Recursive Lattice Reduction -- Adaptively Secure Identity-Based Identification from Lattices without Random Oracles -- Groups Signatures and Authentication -- The Fiat–Shamir Transform for Group and Ring Signature Schemes -- Get Shorty via Group Signatures without Encryption -- Group Message Authentication -- Cryptographic Protocols II -- Fast Secure Computation of Set Intersection -- Distributed Private-Key Generators for Identity-Based Cryptography -- Anonymity -- Solving Revocation with Efficient Update of Anonymous Credentials.