1.	Record Nr.	UNISA996465663903316
	Titolo	Security and cryptography for networks : 6th international conference, scn 2008, amalfi, italy, september 10-12, 2008, proceedings / / edited by Rafail Ostrovsky, Roberto de Prisco, Ivan Visconti
	Pubbl/distr/stampa	Berlin, Germany : , : Springer, , [2008] ©2008
	ISBN	3-540-85855-5
	Edizione	[1st ed. 2008.]
	Descrizione fisica	1 online resource (XI, 423 p.)
	Collana	Security and Cryptology ; ; 5229
	Disciplina	005.82
	Soggetti	Computer security Cryptography Computer networks - Security measures
	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	Invited Talk -- Storage Encryption: A Cryptographer’s View -- Session 1: Implementations -- Implementing Two-Party Computation Efficiently with Security Against Malicious Adversaries -- CLL: A Cryptographic Link Layer for Local Area Networks -- Faster Multi-exponentiation through Caching: Accelerating (EC)DSA Signature Verification -- Session 2: Protocols I -- Privacy Preserving Data Mining within Anonymous Credential Systems -- Improved Privacy of the Tree-Based Hash Protocols Using Physically Unclonable Function -- Session 3: Encryption I -- Two Generic Constructions of Probabilistic Cryptosystems and Their Applications -- Cramer-Shoup Satisfies a Stronger Plaintext Awareness under a Weaker Assumption -- Session 4: Encryption II -- General Certificateless Encryption and Timed-Release Encryption -- Efficient Certificate-Based Encryption in the Standard Model -- Session 5: Primitives -- An Improved Robust Fuzzy Extractor -- On Linear Secret Sharing for Connectivity in Directed Graphs -- Session 6: Signatures -- Expressive Subgroup Signatures -- Anonymous Proxy Signatures -- Multisignatures Using Proofs of Secret Key Possession, as Secure as the Diffie-Hellman Problem -- Session 7: Hardware and Cryptanalysis -- Using Normal Bases for Compact Hardware Implementations of the AES S-Box -- A New Analysis of the

McEliece Cryptosystem Based on QC-LDPC Codes -- Full Cryptanalysis of LPS and Morgenstern Hash Functions -- A New DPA Countermeasure Based on Permutation Tables -- Session 8: Protocols II -- Simplified Submission of Inputs to Protocols -- Unconditionally Reliable and Secure Message Transmission in Directed Networks Revisited -- Session 9: Encryption III -- Linear Bandwidth Naccache-Stern Encryption -- Immunising CBC Mode Against Padding Oracle Attacks: A Formal Security Treatment -- Constructing Strong KEM from Weak KEM (or How to Revive the KEM/DEM Framework) -- Session 10: Key Exchange -- New Anonymity Notions for Identity-Based Encryption -- A Universally Composable Group Key Exchange Protocol with Minimum Communication Effort -- An Identity-Based Key Agreement Protocol for the Network Layer.

Sommario/riassunto

This book constitutes the refereed proceedings of the 6th International Conference on Security and Cryptology for Networks, SCN 2008, held in Amalfi, Italy, in September 2008. The book contains one invited talk and 26 revised full papers which were carefully reviewed and selected from 71 submissions. The papers are organized in topical sections on Implementations, Protocols, Encryption, Primitives, Signatures, Hardware and Cryptanalysis, and Key Exchange.