1. Record Nr. UNINA9910483625903321

Titolo	Advances in Cryptology - CRYPTO 2005 : 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings / / edited by Victor Shoup
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (XII, 572 p.)
Collana	Security and Cryptology, , 2946-1863 ; ; 3621
Altri autori (Persone)	ShoupVictor
Disciplina	003.54
Soggetti	Coding theory Information theory Cryptography Data encryption (Computer science) Computer networks Operating systems (Computers) Computer science - Mathematics Discrete mathematics Computers and civilization Coding and Information Theory Cryptology Computer Communication Networks Operating Systems Discrete Mathematics in Computer Science Computers and Society
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	Efficient Collision Search Attacks on SHA-0 -- Finding Collisions in the Full SHA-1 -- Pebbling and Proofs of Work -- Composition Does Not Imply Adaptive Security -- On the Discrete Logarithm Problem on Algebraic Tori -- A Practical Attack on a Braid Group Based Cryptographic Protocol -- The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption -- Unconditional

Characterizations of Non-interactive Zero-Knowledge -- Impossibility and Feasibility Results for Zero Knowledge with Public Keys -- Communication-Efficient Non-interactive Proofs of Knowledge with Online Extractors -- A Formal Treatment of Onion Routing -- Simple and Efficient Shuffling with Provable Correctness and ZK Privacy -- Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions -- Private Searching on Streaming Data -- Privacy-Preserving Set Operations -- Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys -- Generic Transformation for Scalable Broadcast Encryption Schemes -- Authenticating Pervasive Devices with Human Protocols -- Secure Communications over Insecure Channels Based on Short Authenticated Strings -- On Codes, Matroids and Secure Multi-party Computation from Linear Secret Sharing Schemes -- Black-Box Secret Sharing from Primitive Sets in Algebraic Number Fields -- Secure Computation Without Authentication -- Constant-Round Multiparty Computation Using a Black-Box Pseudorandom Generator -- Secure Computation of Constant-Depth Circuits with Applications to Database Search Problems -- Analysis of Random Oracle Instantiation Scenarios for OAEP and Other Practical Schemes -- Merkle-Damgård Revisited: How to Construct a Hash Function -- On the Generic Insecurity of the Full Domain Hash -- New Monotones and Lower Bounds inUnconditional Two-Party Computation -- One-Way Secret-Key Agreement and Applications to Circuit Polarization and Immunization of Public-Key Encryption -- A Quantum Cipher with Near Optimal Key-Recycling -- An Efficient CDH-Based Signature Scheme with a Tight Security Reduction -- Improved Security Analyses for CBC MACs -- HMQV: A High-Performance Secure Diffie-Hellman Protocol.