Advances in Cryptology – CRYPTO 2010 : 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings /

Rabin, Tal.,
editor

Springer Berlin Heidelberg,
2010

Libros electrónicos | Recursos electrónicos

Monografía

Título: Advances in Cryptology – CRYPTO 2010 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings edited by Tal Rabin

Editorial: Berlin, Heidelberg Springer Berlin Heidelberg 2010

Descripción física: 1 recurso en línea XIV, 744 p. 63 illus

Mención de serie: Lecture Notes in Computer Science 0302-9743 6223 Springer eBooks

Contenido: Leakage -- Circular and Leakage Resilient Public-Key Encryption under Subgroup Indistinguishability -- Leakage-Resilient Pseudorandom Functions and Side-Channel Attacks on Feistel Networks -- Protecting Cryptographic Keys against Continual Leakage -- Securing Computation against Continuous Leakage -- Lattice -- An Efficient and Parallel Gaussian Sampler for Lattices -- Lattice Basis Delegation in Fixed Dimension and Shorter-Ciphertext Hierarchical IBE -- Homomorphic Encryption -- Toward Basing Fully Homomorphic Encryption on Worst-Case Hardness -- Additively Homomorphic Encryption with d-Operand Multiplications -- i-Hop Homomorphic Encryption and Rerandomizable Yao Circuits -- Theory and Applications -- Interactive Locking, Zero-Knowledge PCPs, and Unconditional Cryptography -- Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption -- Structure-Preserving Signatures and Commitments to Group Elements -- Efficient Indifferentiable Hashing into Ordinary Elliptic Curves -- Key Exchange, OAEP/RSA, CCA -- Credential Authenticated Identification and Key Exchange -- Password-Authenticated Session-Key

Generation on the Internet in the Plain Model -- Instantiability of RSA-OAEP under Chosen-Plaintext Attack -- Efficient Chosen-Ciphertext Security via Extractable Hash Proofs -- Attacks -- Factorization of a 768-Bit RSA Modulus -- Correcting Errors in RSA Private Keys -- Improved Differential Attacks for ECHO and Grstl -- A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony -- Composition -- Universally Composable Incoercibility -- Concurrent Non-Malleable Zero Knowledge Proofs -- Equivalence of Uniform Key Agreement and Composition Insecurity -- Computation Delegation and Obfuscation -- Non-interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers -- Improved Delegation of Computation Using Fully Homomorphic Encryption -- Oblivious RAM Revisited -- On Strong Simulation and Composable Point Obfuscation -- Multiparty Computation -- Protocols for Multiparty Coin Toss with Dishonest Majority -- Multiparty Computation for Dishonest Majority: From Passive to Active Security at Low Cost -- Secure Multiparty Computation with Minimal Interaction -- A Zero-One Law for Cryptographic Complexity with Respect to Computational UC Security -- Pseudorandomness -- On Generalized Feistel Networks -- Cryptographic Extraction and Key Derivation: The HKDF Scheme -- Time Space Tradeoffs for Attacks against One-Way Functions and PRGs -- Pseudorandom Functions and Permutations Provably Secure against Related-Key Attacks -- Quantum -- Secure Two-Party Quantum Evaluation of Unitaries against Specious Adversaries -- On the Efficiency of Classical and Quantum Oblivious Transfer Reductions -- Sampling in a Quantum Population, and Applications

Detalles del sistema: Modo de acceso: World Wide Web

ISBN: 9783642146237

Materia: Computer science Computer communication systems Computer security Data encryption (Computer science) Computer science- Mathematics Computers and civilization Management information systems Computer Science Data Encryption Management of Computing and Information Systems Computer Communication Networks Systems and Data Security Computers and Society Discrete Mathematics in Computer Science

Autores: Rabin, Tal., editor

Entidades: SpringerLink (Online service)

Punto acceso adicional serie-Título: Lecture Notes in Computer Science 0302-9743 6223
