1. Record Nr. UNINA9910484218603321

Titolo	Advances in Cryptology -- CRYPTO 2010 : 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010, Proceedings / / edited by Tal Rabin
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	3-642-14623-6
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (XIV, 744 p. 63 illus.)
Collana	Security and Cryptology, , 2946-1863 ; ; 6223
Altri autori (Persone)	RabinTal
Disciplina	005.8
Soggetti	Cryptography Data encryption (Computer science) Electronic data processing - Management Computer networks Data protection Computers and civilization Computer science - Mathematics Discrete mathematics Cryptology IT Operations Computer Communication Networks Data and Information Security Computers and Society Discrete Mathematics in Computer Science
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	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 Grøstl -- 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.

Sommario/riassunto

CRYPTO2010, the30thAnnualInternationalCryptologyConference, wassp- sored by the International Association for Cryptologic Research (IACR) in - operation with the IEEE Computer Society Technical Committee on Security and Privacy and the Computer Science Department of the University of C- ifornia at Santa Barbara. The conference was held in Santa Barbara, Calif- nia, during August 15-19, 2010, in conjunction with CHES 2010 (Workshop on Cryptographic Hardware and Embedded Systems). Zul'kar Ramzan served as the General Chair. The conference received 203 submissions. The quality of the submissions was very high, and the selection process was a challenging one. The Program C- mittee, aided by a 159 external reviewers, reviewed the submissions and after an intensive review period the committee accepted 41 of these submissions. Three submissions were merged into a single paper and two papers were merged into a single talk, yielding a total of 39 papers in the proceedings and 38 presen- tions at the conference. The revised versions of the 39 papers appearing in the proceedings were not subject to editorial review and the authors bear full - sponsibility for their contents. The best-paper award was awarded to the paper "Toward Basing Fully Homomorphic Encryption on Worst-Case

Hardness" by Craig Gentry. The conference featured two invited presentations. This year we celebrated 25 years from the publication of the ground-breaking work of Sha? Goldwasser, Silvio Micali and Charles Racko? "The Knowledge Complexity of Interactive Proof-Systems.