1. Record Nr. UNISA996466569303316

Titolo	Advances in Cryptology – EUROCRYPT 2013 [[electronic resource]] : 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013, Proceedings / / edited by Thomas Johansson, Phong Q. Nguyen
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2013
ISBN	3-642-38348-3
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (XIV, 736 p. 77 illus.)
Collana	Security and Cryptology ; ; 7881
Disciplina	005.82
Soggetti	Data encryption (Computer science) Algorithms Computer security Computer science—Mathematics Cryptology Algorithm Analysis and Problem Complexity Systems and Data Security 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 contenuto	Candidate Multilinear Maps from Ideal Lattices -- Lossy Codes and a New Variant of the Learning-With-Errors Problem -- A Toolkit for Ring-LWE Cryptography -- Regularity of Lossy RSA on Subdomains and Its Applications -- Efficient Cryptosystems from 2k-th Power Residue Symbols -- Deterministic Public-Key Encryption for Adaptively Chosen Plaintext Distributions -- How to Watermark Cryptographic Functions -- Security Evaluations beyond Computing Power: How to Analyze Side-Channel Attacks You Cannot Mount? -- Masking against Side-Channel Attacks: A Formal Security Proof -- Leakage-Resilient Cryptography from Minimal Assumptions -- Faster Index Calculus for the Medium Prime Case Application to 1175-bit and 1425-bit Finite Fields -- Fast Cryptography in Genus 2 -- Graph-Theoretic Algorithms for the “Isomorphism of Polynomials” Problem -- Cryptanalysis of Full

RIPEMD-128 -- New Collision Attacks on SHA-1 Based on Optimal Joint Local-Collision Analysis -- Improving Local Collisions: New Attacks on Reduced SHA-256 -- Dynamic Proofs of Retrievability via Oblivious RAM -- Message-Locked Encryption and Secure Deduplication -- Batch Fully Homomorphic Encryption over the Integers -- Practical Homomorphic MACs for Arithmetic Circuits -- Streaming Authenticated Data Structures -- Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting -- New Links between Differential and Linear Cryptanalysis -- Towards Key-Length Extension with Optimal Security: Cascade Encryption and Xor-cascade Encryption -- Ideal-Cipher (Ir)reducibility for Blockcipher-Based Hash Functions -- Limitations of the Meta-reduction Technique: The Case of Schnorr Signatures -- Practical Signatures from Standard Assumptions -- Locally Computable UOWHF with Linear Shrinkage -- Amplification of Chosen-Ciphertext Security -- Circular Chosen-Ciphertext Security with Compact Ciphertexts -- MiniLEGO: Efficient Secure Two-Party Computation from General Assumptions -- How to Hide Circuits in MPC an Efficient Framework for Private Function Evaluation -- Multi-party Computation of Polynomials and Branching Programs without Simultaneous Interaction -- Quantum-Secure Message Authentication Codes -- One-Sided Device-Independent QKD and Position-Based Cryptography from Monogamy Games -- Quadratic Span Programs and Succinct NIZKs without PCPs -- Zero-Knowledge Argument for Polynomial Evaluation with Application to Blacklists -- Resource-Restricted Indifferentiability -- On Concurrently Secure Computation in the Multiple Ideal Query Model -- Universally Composable Secure Computation with (Malicious) Physically Uncloneable Functions -- How to Garble RAM Programs?.

Sommario/riassunto

This book constitutes the proceedings of the 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2013, held in Athens, Greece, in May 2013. The 41 full papers included in this volume were carefully reviewed and selected from 201 submissions. They deal with cryptanalysis of hash functions, side-channel attacks, number theory, lattices, public key encryption, digital signatures, homomorphic cryptography, quantum cryptography, storage, tools, and secure computation.