1. Record Nr. UNINA9910349306503321

Titolo	Advances in Cryptology – CRYPTO 2019 : 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part I / / edited by Alexandra Boldyreva, Daniele Micciancio
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-26948-5
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XXIII, 771 p. 1614 illus., 51 illus. in color.)
Collana	Security and Cryptology ; ; 11692
Disciplina	005.8 005.82
Soggetti	Data encryption (Computer science) Software engineering Coding theory Information theory Computers Computers and civilization Artificial intelligence Cryptology Software Engineering/Programming and Operating Systems Coding and Information Theory Information Systems and Communication Service Computers and Society Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Award Papers -- Cryptanalysis of OCB2: Attacks on Authenticity and Confidentiality -- Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE -- Fully Secure Attribute-Based Encryption for t-CNF from LWE -- Lattice-Based ZK -- Noninteractive Zero Knowledge for NP from (Plain) Learning With Errors -- Lattice-Based Zero-Knowledge Proofs: New Techniques for Shorter and Faster

Constructions and Applications -- Efficient Lattice-Based Zero-Knowledge Arguments with Standard Soundness: Construction and Applications -- Algebraic Techniques for Short(er) Exact Lattice-Based Zero-Knowledge Proofs -- Symmetric Cryptography -- Seedless Fruit is the Sweetest: Random Number Generation, Revisited -- Nonces are Noticed: AEAD Revisited -- How to Build Pseudorandom Functions From Public Random Permutations -- Mathematical Cryptanalysis -- New Results on Modular Inversion Hidden Number Problem and Inversive Congruential Generator -- On the Shortness of Vectors to be found by the Ideal-SVP Quantum Algorithm -- Proofs of Storage -- Proofs of Replicated Storage Without Timing Assumptions -- Simple Proofs of Space-Time and Rational Proofs of Storage -- Non-Malleable Codes -- Non-Malleable Codes for Decision Trees -- Explicit Rate-1 Non-malleable Codes for Local Tampering -- Continuous Space-Bounded Non-Malleable Codes from Stronger Proofs-of-Space -- SNARKs and Blockchains -- Synchronous, with a Chance of Partition Tolerance -- Subvector Commitments with Application to Succinct Arguments -- Batching Techniques for Accumulators with Applications to IOPs and Stateless Blockchains -- Homomorphic Cryptography -- On the Plausibility of Fully Homomorphic Encryption for RAMs -- Homomorphic Time-Lock Puzzles and Applications -- Symmetric Primitives with Structured Secrets -- Leakage Models and Key Reuse -- Unifying Leakage Models on a Rényi Day -- Leakage Certification Revisited: Bounding Model Errors in Side-Channel Security Evaluations -- Security in the Presence of Key Reuse: Context-Separable Interfaces and their Applications.

Sommario/riassunto

The three-volume set, LNCS 11692, LNCS 11693, and LNCS 11694, constitutes the refereed proceedings of the 39th Annual International Cryptology Conference, CRYPTO 2019, held in Santa Barbara, CA, USA, in August 2019. The 81 revised full papers presented were carefully reviewed and selected from 378 submissions. The papers are organized in the following topical sections: Part I: Award papers; lattice-based ZK; symmetric cryptography; mathematical cryptanalysis; proofs of storage; non-malleable codes; SNARKs and blockchains; homomorphic cryptography; leakage models and key reuse. Part II: MPC communication complexity; symmetric cryptanalysis; (post) quantum cryptography; leakage resilience; memory hard functions and privacy amplification; attribute based encryption; foundations. Part III: Trapdoor functions; zero knowledge I; signatures and messaging; obfuscation; watermarking; secure computation; various topics; zero knowledge II; key exchange and broadcast encryption.