1. Record Nr. UNINA9910349306303321

Titolo	Advances in Cryptology – CRYPTO 2019 : 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part III / / edited by Alexandra Boldyreva, Daniele Micciancio
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-26954-X
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XV, 859 p. 536 illus., 48 illus. in color.)
Collana	Security and Cryptology ; ; 11694
Disciplina	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	Trapdoor Functions -- Trapdoor Hash Functions and Their Applications -- CCA Security and Trapdoor Functions via Key-Dependent-Message Security -- Zero Knowledge I -- Zero-Knowledge Proofs on Secret-Shared Data via Fully Linear PCPs -- Non-Uniformly Sound Certificates with Applications to Concurrent Zero-Knowledge -- On Round Optimal Statistical Zero Knowledge Arguments -- Signatures and Messaging -- Repudiability and Claimability of Ring Signatures -- Two-Party ECDSA

from Hash Proof Systems and Efficient Instantiations -- Asymmetric Message Franking: Content Moderation for Metadata-Private End-to-End Encryption -- Obfuscation -- Statistical Zeroizing Attack: Cryptanalysis of Candidates of BP Obfuscation over GGH15 Multilinear Map -- Indistinguishability Obfuscation Without Multilinear Maps: New Paradigms via Low Degree Weak Pseudorandomness and Security Amplification -- Watermarking -- Watermarking PRFs from Lattices: Stronger Security via Extractable PRFs -- Watermarking Public-Key Cryptographic Primitives -- Secure Computation -- SpOT-Light: Lightweight Private Set Intersection from Sparse OT Extension -- Universally Composable Secure Computation with Corrupted Tokens -- Reusable Non-Interactive Secure Computation -- Efficient Pseudorandom Correlation Generators: Silent OT Extension and More -- Various Topics -- Adaptively Secure and Succinct Functional Encryption: Improving Security and Efficiency, Simultaneously -- Non-Interactive Non-Malleability from Quantum Supremacy -- Cryptographic Sensing -- Public-Key Cryptography in the Fine-Grained Setting -- Zero Knowledge II -- Exploring Constructions of Compact NIZKs from Various Assumptions -- New Constructions of Reusable Designated-Verifier NIZKs -- Scalable Zero Knowledge with no Trusted Setup -- Libra: Succinct Zero-Knowledge Proofs with Optimal Prover Computation -- Key Exchange and Broadcast Encryption -- Highly Efficient Key Exchange Protocols with Optimal Tightness -- Strong Asymmetric PAKE based on Trapdoor CKEM -- Broadcast and Trace with N Ciphertext Size from Standard Assumptions -- .

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.