1. Record Nr.	UNINA9910349306403321
Titolo	Advances in Cryptology – CRYPTO 2019 : 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II / / edited by Alexandra Boldyreva, Daniele Micciancio
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-26951-5
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (XV, 861 p. 1632 illus., 100 illus. in color.)
Collana	Security and Cryptology ; ; 11693
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 contenuto	MPC Communication Complexity -- The Communication Complexity of Threshold Private Set Intersection -- Adaptively Secure MPC with Sublinear Communication Complexity -- Communication Lower Bounds for Statistically Secure MPC, with or without Preprocessing -- Communication-Efficient Unconditional MPC with Guaranteed Output Delivery -- Symmetric Cryptanalysis -- Efficient Collision Attack Frameworks for RIPEMD-160 -- Improving Attacks on Round-Reduced

Speck32/64 Using Deep Learning -- Correlation of Quadratic Boolean Functions: Cryptanalysis of All Versions of Full MORUS -- Low Memory Attacks against Two-Round Even-Mansour using the 3-XOR Problem -- (Post) Quantum Cryptography -- How to Record Quantum Queries, and Applications to Quantum Indifferentiability -- Quantum security proofs using semi-classical oracles -- Quantum Indistinguishability of Random Sponges -- Revisiting Post-Quantum Fiat-Shamir -- Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model -- Leakage Resilience -- Unconditionally Secure Computation Against Low-Complexity Leakage -- Tight Leakage-Resilient CCA-Security from Quasi-Adaptive Hash Proof System -- Non-Malleable Secret Sharing in the Computational Setting: Adaptive Tampering, Noisy-Leakage Resilience, and Improved Rate -- Leakage Resilient Secret Sharing and Applications -- Stronger Leakage-Resilient and Non-Malleable Secret Sharing Schemes for General Access Structures -- Memory Hard Functions and Privacy Amplification -- Memory-Hard Functions from Cryptographic Primitives -- Data-Independent Memory Hard Functions: New Attacks and Stronger Constructions -- Simultaneous Amplification: The Case of Non-Interactive Zero-Knowledge -- The Privacy Blanket of the Shuffle Model -- Attribute Based Encryption -- Realizing Chosen Ciphertext Security Generically in Attribute-Based Encryption and Predicate Encryption -- Match Me if You Can: Matchmaking Encryption and its Applications -- ABE for DFA from k-Lin -- Attribute Based Encryption (and more) for Nondeterministic Finite Automata from LWE -- Foundations -- The Distinction Between Fixed and Random Generators in Group-Based Assumptions -- Unifying computational entropies via Kullback–Leibler divergence.

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.