1. Record Nr. UNISA996418316303316

Titolo	Advances in Cryptology – CRYPTO 2020 [[electronic resource]] : 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part III / / edited by Daniele Micciancio, Thomas Ristenpart
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-56877-6
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XV, 832 p. 448 illus., 31 illus. in color.)
Collana	Security and Cryptology ; ; 12172
Disciplina	005.82
Soggetti	Data encryption (Computer science) Data structures (Computer science) Computer communication systems Computer security Application software Software engineering Cryptology Data Structures and Information Theory Computer Communication Networks Systems and Data Security Information Systems Applications (incl. Internet) Software Engineering/Programming and Operating Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Multi-Party Computation: Two-Sided Malicious Security for Private Intersection-Sum with Cardinality -- Private Set Intersection in the Internet Setting From Lightweight Oblivious PRF -- Multiparty Generation of an RSA Modulus -- Secret Sharing -- Non-Malleability against Polynomial Tampering -- Non-Malleable Secret Sharing against Bounded Joint-Tampering Attacks in the Plain Model -- Nearly Optimal Robust Secret Sharing against Rushing Adversaries -- Cryptanalysis -- Cryptanalytic Extraction of Neural Network Models -- Automatic

Verification of Differential Characteristics: Application to Reduced Gimli -- The MALICIOUS Framework: Embedding Backdoors into Tweakable Block Ciphers -- Cryptanalysis of The Lifted Unbalanced Oil Vinegar Signature Scheme -- Out of Oddity -- New Cryptanalytic Techniques against Symmetric Primitives Optimized for Integrity Proof Systems -- Improved Differential-Linear Attacks with Applications to ARX Ciphers -- Cryptanalysis Results on Spook: Bringing Full-round Shadow-512 to the Light -- Cryptanalysis of LEDAcrypt -- Alzette: a 64-bit ARX-box (feat. CRAX and TRAX) -- Delay functions -- Order-Fairness for Byzantine Consensus -- Generically Speeding-Up Repeated Squaring is Equivalent to Factoring: Sharp Thresholds for All Generic-Ring Delay Functions -- Zero Knowledge -- Compressed Sigma-Protocol Theory and Practical Application to Plug & Play Secure Algorithmics -- A Tight Parallel Repetition Theorem for Partially Simulatable Interactive Arguments via Smooth KL-Divergence -- Interactive Proofs for Social Graphs -- The Measure-and-Reprogram Technique 2.0: Multi-Round Fiat-Shamir and More -- Fiat-Shamir for Repeated Squaring with Applications to PPAD-Hardness and VDFs -- PPAD-Hardness and Delegation with Unambiguous Proofs -- New Techniques for Zero-Knowledge: Leveraging Inefficient Provers to Reduce Assumptions, Interaction, and Trust -- Spartan: Efficient and general-purpose zkSNARKs -- NIZK from LPN and Trapdoor Hash via Correlation Intractability for Approximable Relations -- Shorter Non-Interactive Zero-Knowledge Arguments and ZAPs for Algebraic Languages -- Non-Interactive Zero-Knowledge Arguments for QMA, with preprocessing.

Sommario/riassunto

Conference on Cryptologic Research, CRYPTO 2020, which was held during August 17–21, 2020. Crypto has traditionally been held at UCSB every year, but due to the COVID-19 pandemic it will be an online event in 2020. The 85 papers presented in the proceedings were carefully reviewed and selected from a total of 371 submissions. They were organized in topical sections as follows: Part I: Security Models; Symmetric and Real World Cryptography; Hardware Security and Leakage Resilience; Outsourced encryption; Constructions. Part II: Public Key Cryptanalysis; Lattice Algorithms and Cryptanalysis; Lattice-based and Post Quantum Cryptography; Multi-Party Computation. Part III: Multi-Party Computation; Secret Sharing; Cryptanalysis; Delay functions; Zero Knowledge. .