1. Record Nr. UNISA996418317103316

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 II / / edited by Daniele Micciancio, Thomas Ristenpart
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-56880-6
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XV, 856 p. 737 illus., 27 illus. in color.)
Collana	Security and Cryptology ; ; 12171
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 bibliografia	Includes bibliographical references and index.
Nota di contenuto	Public Key Cryptanalysis- A Polynomial-Time Algorithm for Solving the Hidden Subset Sum Problem -- Asymptotic complexities of discrete logarithm algorithms in pairing-relevant finite fields -- Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment -- Breaking the decisional Diffie-Hellman problem for class group actions using genus theory -- A Classification of Computational Assumptions in the Algebraic Group Model -- Lattice Algorithms and Cryptanalysis -- Fast reduction of algebraic lattices over cyclotomic

fields -- Faster Enumeration-based Lattice Reduction: Root Hermite Factor k^(1/(2k)) in Time k^(k/8 + o(k)) -- Lattice Reduction for Modules, or How to Reduce ModuleSVP to ModuleSVP -- Random Self-reducibility of Ideal-SVP via Arakelov Random Walks -- Slide Reduction, Revisited,ÄîFilling the Gaps in SVP Approximation -- Rounding in the Rings -- Lattice-based and post-quantum cryptography -- LWE with Side Information: Attacks and Concrete Security Estimation -- A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM -- Efficient Pseudorandom Correlation Generators from Ring-LPN -- Scalable Pseudorandom Quantum States -- A non-PCP Approach to Succinct Quantum-Safe Zero-Knowledge -- Practical Product Proofs for Lattice Commitments.-Lattice-Based Blind Signatures, Revisited -- Multi-Party Computation -- 12171 Round-optimal Black-box Commit-and-prove with Succinct Communication -- Efficient Constant-Round MPC with Identifiable Abort and Public Verifiability -- Black-box use of One-way Functions is Useless for Optimal Fair Coin-Tossing -- Guaranteed Output Delivery Comes Free in Honest Majority MPC -- Black-Box Transformations from Passive to Covert Security with Public Verifiability -- MPC with Friends and Foes -- Always Have a Backup Plan: Fully Secure Synchronous MPC with Asynchronous Fallback -- Reverse Firewalls for Actively Secure MPCs -- Stacked Garbling: Garbled Circuit Proportional to Longest Execution Path -- Better Concrete Security for Half-Gates Garbling (in the Multi-Instance Setting) -- Improved Primitives for MPC over Mixed Arithmetic-Binary Circuits.

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. .