1.	Record Nr.	UNINA9910416082803321
	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 I / / edited by Daniele Micciancio, Thomas Ristenpart
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
	ISBN	3-030-56784-2
	Edizione	[1st ed. 2020.]
	Descrizione fisica	1 online resource (XXIII, 870 p. 624 illus., 36 illus. in color.)
	Collana	Security and Cryptology ; ; 12170
	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	Security models -- Handling Adaptive Compromise for Practical Encryption Schemes -- Overcoming Impossibility Results in Composable Security using Interval-Wise Guarantees -- Indifferentiability for Public Key Cryptosystems -- Quantifying the Security Cost of Migrating Protocols to Practice -- Symmetric and Real World Cryptography -- The Memory-Tightness of Authenticated Encryption -- Time-Space Tradeoffs and Short Collisions in Merkle-Damgård Hash Functions -- The Summation-Truncation Hybrid:

	Reusing Discarded Bits for Free -- Security Analysis of NIST CTR-DRBG -- Security Analysis and Improvements for the IETF MLS Standard for Group Messaging -- Universally Composable Relaxed Password Authenticated Key Exchange -- Anonymous Tokens with Private Metadata Bit -- Hardware Security and Leakage Resilience -- Random Probing Security: Verification, Composition, Expansion and New Constructions -- Mode-Level vs. Implementation-Level Physical Security in Symmetric Cryptography: A Practical Guide Through the Leakage-Resistance Jungle -- Leakage-Resilient Key Exchange and Two-Seed Extractors -- Outsourced encryption -- Lower Bounds for Encrypted Multi-Maps and Searchable Encryption in the Leakage Cell Probe Model -- Fast and Secure Updatable Encryption -- Incompressible Encodings -- Constructions -- New Constructions of Hinting PRGs, OWFs with Encryption, and more -- Adaptively Secure Constrained Pseudorandom Functions in the Standard Model -- Collusion Resistant Watermarkable PRFs from Standard Assumptions -- Verifiable Registration-Based Encryption -- New Techniques for Traitor Tracing: Size N^{1/3} and More from Pairings -- Public Key Cryptography -- Functional Encryption for Attribute-Weighted Sums from k-Lin -- Amplifying the Security of Functional Encryption, Unconditionally -- Dynamic Decentralized Functional Encryption -- On Succinct Arguments and Witness Encryption from Groups -- Fully Deniable Interactive Encryption -- Chosen Ciphertext Security from Injective Trapdoor Functions.
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. .