1.	Record Nr.	UNISA996418312303316
	Titolo	Theory of cryptography . Part I : 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, proceedings / / Rafael Pass, Krzysztof Pietrzak (editors)
	Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2020] Â©2020
	ISBN	3-030-64375-1
	Edizione	[1st ed. 2020.]
	Descrizione fisica	1 online resource (XVI, 707 p. 54 illus., 3 illus. in color.)
	Collana	Security and Cryptology ; ; 12550
	Disciplina	005.82
	Soggetti	Data encryption (Computer science)
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Lossiness and Entropic Hardness for Ring-LWE -- Multi-key Fully-Homomorphic Encryption in the Plain Model -- Constant Ciphertext-Rate Non-Committing Encryption from Standard Assumptions -- Efficient Range-Trapdoor Functions and Applications: Rate-1 OT and CP-ABE for Circuits (and more) in the Symmetric Key Setting -- Optimal Broadcast Encryption from LWE and Pairings in the Standard Model -- Equipping Public-Key Cryptographic Primitives with Watermarking (or: A Hole Is to Watermark) -- Functional Encryption for Quadratic Functions from k-Lin, Revisited -- On Perfect Correctness in (Lockable) Obfuscation -- Can a Public Blockchain Keep a Secret -- Blockchains from Non-Idealized Hash Functions -- Ledger Combiners for Fast Asynchronous Byzantine Agreement with Subquadratic Communication -- Expected Constant Round Byzantine Broadcast under Dishonest Majority -- Round-Efficient Byzantine Broadcast under Strongly Adaptive and Majority Corruptions -- A Lower Bound for One-Round Oblivious RAM -- Lower Bounds for Multi-Server Oblivious RAMs -- On Computational Shortcuts for Information-Theoretic PIR -- Characterizing Deterministic-Prover Zero Knowledge -- NIZK from SNARG -- Weakly Extractable One-Way Functions -- Towards Non-Interactive Witness Hiding -- FHE-Based Bootstrapping of Designated-Prover NIZK -- Perfect Zero Knowledge: New Upperbounds and Relativized Separations.

Sommario/riassunto

This three-volume set, LNCS 12550, 12551, and 12552, constitutes the refereed proceedings of the 18th International Conference on Theory of Cryptography, TCCC 2020, held in Durham, NC, USA, in November 2020. The total of 71 full papers presented in this three-volume set was carefully reviewed and selected from 167 submissions. Amongst others they cover the following topics: study of known paradigms, approaches, and techniques, directed towards their better understanding and utilization; discovery of new paradigms, approaches and techniques that overcome limitations of the existing ones, formulation and treatment of new cryptographic problems; study of notions of security and relations among them; modeling and analysis of cryptographic algorithms; and study of the complexity assumptions used in cryptography. Due to the Corona pandemic this event was held virtually.

2.

Record Nr.	UNISALENTO991003475049707536
Autore	Pailleron, Marie Louise
Titolo	François Buloz et ses amis : la vie littéraire sous Louis Philippe / par Marie-Louise Pailleron
Pubbl/distr/stampa	Paris : Firmin-Didot, 1930
Edizione	[Nouvelle éd. rev]
Descrizione fisica	460 p., ill. ; 20 cm
Disciplina	840.9
Soggetti	Buloz, François Buloz, François
Lingua di pubblicazione	Francese
Formato	Materiale a stampa
Livello bibliografico	Monografia