1. Record Nr. UNINA9910508444103321

Titolo	Theory of Cryptography : 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8–11, 2021, Proceedings, Part III / / edited by Kobbi Nissim, Brent Waters
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-90456-3
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (525 pages)
Collana	Security and Cryptology, , 2946-1863 ; ; 13044
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Coding theory Information theory Application software Computer networks Data protection Cryptology Coding and Information Theory Computer and Information Systems Applications Computer Communication Networks Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Covert Learning: How to Learn with an Untrusted Intermediary -- Random-Index PIR and Applications -- Forward Secret Encrypted RAM: Lower Bounds and Applications -- Laconic Private Set Intersection and Applications -- Amortizing Rate-1 OT and Applications to PIR and PSI -- Ring-based Identity Based Encryption { Asymptotically Shorter MPK and Tighter Security -- Cryptographic Shallots: A Formal Treatment of Repliable Onion Encryption -- Grafting Key Trees: Efficient Key Management for Overlapping Groups -- Updatable Public Key Encryption in the Standard Model -- Towards Tight Adaptive Security of

Non-Interactive Key Exchange -- On the Impossibility of Purely Algebraic Signatures -- Policy-Compliant Signatures -- Simple and Efficient Batch Verification Techniques for Verifiable Delay Functions -- Non-Malleable Vector Commitments via Local Equivocability -- Non-Malleable Time-Lock Puzzles and Applications -- Vector and Functional Commitments from Lattices.-.

Sommario/riassunto

The three-volume set LNCS 13042, LNCS 13043 and LNCS 13044 constitutes the refereed proceedings of the 19th International Conference on Theory of Cryptography, TCC 2021, held in Raleigh, NC, USA, in November 2021. The total of 66 full papers presented in this three-volume set was carefully reviewed and selected from 161 submissions. They cover topics on proof systems, attribute-based and functional encryption, obfuscation, key management and secure communication.