| | | |
|---|---|---|
| 1. | Record Nr. | UNINA9910447246403321 |
| | Titolo | Theory of Cryptography : 18th International Conference, TCC 2020, Durham, NC, USA, November 16–19, 2020, Proceedings, Part II / / edited by Rafael Pass, Krzysztof Pietrzak |
| | Pubbl/distr/stampa | Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020 |
| | ISBN | 3-030-64378-6 |
| | Edizione | [1st ed. 2020.] |
| | Descrizione fisica | 1 online resource (XII, 715 p. 139 illus., 25 illus. in color.) |
| | Collana | Security and Cryptology, , 2946-1863 ; ; 12551 |
| | Disciplina | 005.82 |
| | Soggetti | Cryptography<br>Data encryption (Computer science)<br>Software engineering<br>Data structures (Computer science)<br>Information theory<br>Computer networks - Security measures<br>Data protection<br>Computer networks<br>Cryptology<br>Software Engineering<br>Data Structures and Information Theory<br>Mobile and Network Security<br>Data and Information Security<br>Computer Communication Networks |
| | Lingua di pubblicazione | Inglese |
| | Formato | Materiale a stampa |
| | Livello bibliografico | Monografia |
| | Nota di contenuto | Proof-Carrying Data from Accumulation Schemes -- Linear-Time Arguments with Sublinear Verification from Tensor Codes -- Barriers for Succinct Arguments in the Random Oracle Model -- Accumulators in (and Beyond) Generic Groups: Non-Trivial Batch Verification Requires Interaction -- Batch Verification and Proofs of Proximity with Polylog Overhead -- Batch Verification for Statistical Zero Knowledge Proofs -- Public-Coin Zero-Knowledge Arguments with (almost) Minimal Time |

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.