

1. Record Nr.	UNINA9910512159703321
Titolo	Security and Trust Management : 17th International Workshop, STM 2021, Darmstadt, Germany, October 8, 2021, Proceedings / / edited by Rodrigo Roman, Jianying Zhou
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2021
ISBN	3-030-91859-9
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (208 pages)
Collana	Security and Cryptology, , 2946-1863 ; ; 13075
Disciplina	005.8
Soggetti	Data protection Application software Computer engineering Computer networks Cryptography Data encryption (Computer science) Data and Information Security Computer and Information Systems Applications Computer Engineering and Networks Cryptology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Applied Cryptography -- An Aggregate Signature with Pre-Communication in the Plain Public Key Model -- The Adversary Capabilities In Practical Byzantine Fault Tolerance -- Privacy -- Where to Meet a Driver Privately: Recommending Pick-Up Locations for Ride-Hailing Services -- Efficient permutation protocol for MPC in the head -- Efficient Scalable Multi-Party Private Set Intersection Using Oblivious PRF 78 -- Formal Methods for Security and Trust -- Secure Implementation of a Quantum-Future GAKE Protocol -- Deciding a Fragment of (alpha, beta)-Privacy -- Systems Security -- TLS beyond the broker: Enforcing ne-grained security and trust in publish/subscribe environments for IoT -- Root-of-Trust Abstractions for Symbolic Analysis: Application to Attestation Protocols -- Towards

Sommario/riassunto

This book constitutes the proceedings of the 17th International Workshop on Security and Trust Management, STM 2021, co-located with the 26th European Symposium on Research in Computer Security, ESORICS 2021. The conference was planned to take place in Darmstadt, Germany. It was held online on October 8, 2021, due to the COVID-19 pandemic. The 10 papers presented in this volume were carefully reviewed and selected from 26 submissions. They were organized in topical sections on applied cryptography; privacy; formal methods for security and trust; and systems security. .

---