1. Record Nr. UNISA996418305203316

Titolo	Advances in Cryptology – EUROCRYPT 2020 [[electronic resource]] : 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part I / / edited by Anne Canteaut, Yuval Ishai
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-45721-4
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (xxv, 797 pages) : illustrations
Collana	Security and Cryptology ; ; 12105
Disciplina	001.5436
Soggetti	Data encryption (Computer science) Computers Computer communication systems Computer security Data structures (Computer science) Cryptology Information Systems and Communication Service Computer Communication Networks Systems and Data Security Data Structures and Information Theory
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Invited Talk -- Best Paper Awards -- Obfuscation and Functional Encryption -- Symmetric Cryptanalysis -- Randomness Extraction -- Symmetric Cryptography I -- Secret Sharing -- Fault-Attack Security -- Succinct Proofs.
Sommario/riassunto	The three volume-set LNCS 12105, 12106, and 12107 constitute the thoroughly refereed proceedings of the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2020, which was due to be held in Zagreb, Croatia, in May 2020. The conference was held virtually due to the COVID-19 pandemic. The 81 full papers presented were carefully

reviewed and selected from 375 submissions. The papers are organized into the following topical sections: invited talk; best paper awards; obfuscation and functional encryption; symmetric cryptanalysis; randomness extraction; symmetric cryptography I; secret sharing; fault-attack security; succinct proofs; generic models; secure computation I; quantum I; foundations; isogeny-based cryptography; lattice-based cryptography; symmetric cryptography II; secure computation II; asymmetric cryptanalysis; verifiable delay functions; signatures; attribute-based encryption; side-channel security; non-interactive zero-knowledge; public-key encryption; zero-knowledge; quantum II.