1. Record Nr. UNINA9910409666203321

Titolo	Advances in Cryptology – EUROCRYPT 2020 : 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part III / / edited by Anne Canteaut, Yuval Ishai
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-45727-3
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (xv, 821 pages) : illustrations
Collana	Security and Cryptology, , 2946-1863 ; ; 12107
Disciplina	005.8 005.824
Soggetti	Cryptography Data encryption (Computer science) Database management Computer networks Data protection Artificial intelligence Cryptology Database Management System Computer Communication Networks Security Services Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Asymmetric Cryptanalysis -- Verifiable Delay Functions -- Signatures -- Attribute-Based Encryption -- Side-Channel Security -- Non-Interactive Zero-Knowledge -- Public-Key Encryption -- Zero-Knowledge -- Quantum II.
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.