

1. Record Nr.	UNISA996466232303316
Titolo	Advances in Cryptology – EUROCRYPT 2018 [[electronic resource]] : 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II / / edited by Jesper Buus Nielsen, Vincent Rijmen
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-319-78375-0
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (XIX, 805 p. 105 illus.)
Collana	Security and Cryptology ; ; 10821
Disciplina	005.8
Soggetti	Data encryption (Computer science) Software engineering Coding theory Information theory Computers and civilization Data mining Artificial intelligence Cryptology Software Engineering/Programming and Operating Systems Coding and Information Theory Computers and Society Data Mining and Knowledge Discovery Artificial Intelligence
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	The three volumes LNCS 10820, 10821, and 10822 constitute the thoroughly refereed proceedings of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2018, held in Tel Aviv, Israel, in April/May 2018. The 69 full papers presented were carefully reviewed and selected from 294 submissions. The papers are organized into the

following topical sections: foundations; lattices; random oracle model; fully homomorphic encryption; permutations; galois counter mode; attribute-based encryption; secret sharing; blockchain; multi-collision resistance; signatures; private simultaneous messages; masking; theoretical multiparty computation; obfuscation; symmetric cryptanalysis; zero-knowledge; implementing multiparty computation; non-interactive zero-knowledge; anonymous communication; isogeny; leakage; key exchange; quantum; non-malleable codes; and provable symmetric cyptography. .
