1. Record Nr. UNISA996465772103316

Titolo	Public-Key Cryptography – PKC 2018 [[electronic resource]] : 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part II / / edited by Michel Abdalla, Ricardo Dahab
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2018
ISBN	3-319-76581-7
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (XIX, 760 p. 95 illus.)
Collana	Security and Cryptology ; ; 10770
Disciplina	005.82
Soggetti	Data encryption (Computer science) Software engineering Computer organization Computers Cryptology Software Engineering/Programming and Operating Systems Computer Systems Organization and Communication Networks Computing Milieux
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Key-Dependent-Message and Selective-Opening Security -- Searchable and Fully Homomorphic Encryption -- Public-Key Encryption -- Encryption with Bad Randomness -- Subversion Resistance -- Cryptanalysis -- Composable Security -- Oblivious Transfer -- Multiparty Computation -- Signatures -- Structure-Preserving Signatures -- Functional Encryption -- Foundations -- Obfuscation-Based Cryptographic Constructions -- Protocols -- Blockchain -- Zero-Knowledge -- Lattices.
Sommario/riassunto	The two-volume set LNCS 10769 and 10770 constitutes the refereed proceedings of the 21st IACR International Conference on the Practice and Theory of Public-Key Cryptography, PKC 2018, held in Rio de Janeiro, Brazil, in March 2018. The 49 revised papers presented were carefully reviewed and selected from 186 submissions. They are

organized in topical sections such as Key-Dependent-Message and Selective-Opening Security; Searchable and Fully Homomorphic Encryption; Public-Key Encryption; Encryption with Bad Randomness; Subversion Resistance; Cryptanalysis; Composable Security; Oblivious Transfer; Multiparty Computation; Signatures; Structure-Preserving Signatures; Functional Encryption; Foundations; Obfuscation-Based Cryptographic Constructions; Protocols; Blockchain; Zero-Knowledge; Lattices.