1.	Record Nr.	UNISA996418213903316
	Titolo	Public-Key Cryptography – PKC 2020 [[electronic resource]] : 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4–7, 2020, Proceedings, Part I / / edited by Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, Vassilis Zikas
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
	ISBN	3-030-45374-X
	Edizione	[1st ed. 2020.]
	Descrizione fisica	1 online resource (692 pages)
	Collana	Security and Cryptology ; ; 12110
	Disciplina	005.8
	Soggetti	Data encryption (Computer science)
		Computer security
		Computer networks - Security measures
		Computer communication systems
		Coding theory
		Information theory
		Computers
		Cryptology
		Security Services
		Mobile and Network Security
		Computer Communication Networks
		Coding and Information Theory
		Computing Milieux
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	Functional encryption -- Identity-based encryption -- Obfuscation and applications -- Encryption schemes -- Secure channels -- Basic primitives with special properties -- Proofs and arguments -- Lattice-based cryptography -- Isogeny-based cryptography -- Multiparty protocols -- Secure computation and related primitives -- Post-quantum primitives -- Privacy-preserving schemes.

Sommario/riassunto   The two-volume set LNCS 12110 and 12111 constitutes the refereed proceedings of the 23rd IACR International Conference on the Practice and Theory of Public-Key Cryptography, PKC 2020, held in Edinburgh, UK, in May 2020. The 44 full papers presented were carefully reviewed and selected from 180 submissions. They are organized in topical sections such as: functional encryption; identity-based encryption; obfuscation and applications; encryption schemes; secure channels; basic primitives with special properties; proofs and arguments; lattice-based cryptography; isogeny-based cryptography; multiparty protocols; secure computation and related primitives; post-quantum primitives; and privacy-preserving schemes.