1.	Record Nr.	UNINA9910349309803321
	Titolo	Code-Based Cryptography : 7th International Workshop, CBC 2019, Darmstadt, Germany, May 18–19, 2019, Revised Selected Papers / / edited by Marco Baldi, Edoardo Persichetti, Paolo Santini
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
	ISBN	3-030-25922-6
	Edizione	[1st ed. 2019.]
	Descrizione fisica	1 online resource (VII, 149 p. 57 illus., 11 illus. in color.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 11666
	Disciplina	005.82
	Soggetti	Cryptography
		Data encryption (Computer science)
		Computer engineering
		Computer networks
		Coding theory
		Information theory
		Computer science - Mathematics
		Cryptology
		Computer Engineering and Networks
		Coding and Information Theory
		Symbolic and Algebraic Manipulation
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di bibliografia	Includes bibliographical references and index.
	Nota di contenuto	Quantum Resistant Public Key Encryption Scheme HermitianRLCE -- LEDAcrypt: QC-LDPC code-based cryptosystems with bounded decryption failure rate -- Introducing arithmetic failures to accelerate QC-MDPC code-based cryptography -- DAGS: Reloaded Revisiting Dyadic Key Encapsulation -- Practical Algebraic Attack on DAGS -- Weak Keys in the Faure-Loidreau Cryptosystem -- Analysis of reaction and timing attacks against cryptosystems based on sparse parity-check codes -- On IND-CCA1 Security of Randomized McEliece Encryption in the Standard Model.
	Sommario/riassunto	This book constitutes the refereed and revised post-conference

proceedings of the 7th International Workshop on Code-Based Cryptography, CBC 2019, held in Darmstadt, Germany, in May 2019. The eight papers presented in this book were carefully reviewed and selected from numerous submissions. These contributions are divided into two groups: The first four papers deal with the design of code-based cryptosystems, while the following four papers are on cryptanalysis of code-based cryptosystems.