1.	Record Nr.	UNINA9910413437703321
	Titolo	Code-Based Cryptography : 8th International Workshop, CBCrypto 2020, Zagreb, Croatia, May 9–10, 2020, Revised Selected Papers / / edited by Marco Baldi, Edoardo Persichetti, Paolo Santini
	Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
	ISBN	3-030-54074-X
	Edizione	[1st ed. 2020.]
	Descrizione fisica	1 online resource (IX, 139 p. 97 illus., 14 illus. in color.)
	Collana	Security and Cryptology, , 2946-1863 ; ; 12087
	Disciplina	005.82
	Soggetti	Cryptography Data encryption (Computer science) Computer engineering Computer networks Data structures (Computer science) Information theory Computer science - Mathematics Software engineering Cryptology Computer Engineering and Networks Computer Communication Networks Data Structures and Information Theory Mathematics of Computing Software Engineering
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	On the Security of NTS-KEM in the Quantum Random Oracle Model -- On the Decipherment of Sidel'nikov-type Cryptosystems -- A New Code-Based Cryptosystem -- On Constant-time QC-MDPC Decoders with Negligible Failure Rate -- Protograph-Based Decoding of Low-Density Parity-Check Codes with Hamming Weight Amplifiers -- MURAVE: A New Rank Code-based Signature with MUltiple RAnk VErification -- Optimized and secure implementation of ROLLO-I.

Sommario/riassunto

This book constitutes the refereed and revised post-conference proceedings of the 8th International Workshop on Code-Based Cryptography, CBCrypto 2020, held in Zagreb, Croatia, in May 2020.* The seven papers presented in this book were carefully reviewed and selected from numerous submissions. These contributions focus on various topics such as code-based cryptography, from design to implementation, security, new systems, and improved decoding algorithms. * The conference was held virtually due to the COVID-19 pandemic.