1. Record Nr. UNINA9911007356803321

Titolo	Code-Based Cryptography : 12th International Workshop, CBCrypto 2024, Zurich, Switzerland, May 25–26, 2024, Revised Selected Papers / / edited by Violetta Weger, Jean-Christophe Deneuville, Anna-Lena Horlemann
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
ISBN	3-031-90229-7
Edizione	[1st ed. 2025.]
Descrizione fisica	1 online resource (IX, 111 p. 16 illus., 14 illus. in color.)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15531
Disciplina	005.824
Soggetti	Cryptography Data encryption (Computer science) Computer networks Computer science - Mathematics Application software Data protection Cryptology Computer Communication Networks Mathematics of Computing Computer and Information Systems Applications Data and Information Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	-- HQC Beyond the BSC: Towards Error Structure-Aware Decoding. -- Generalizing the Augot-Finiasz PKE to Other Code Classes. -- McEliece Parameter Sets Optimized for Processing in Memory Architectures. -- Breaking HWQCS: a code-based signature scheme from high weight QC-LDPC codes. -- Increasing Index Sizes for Information Set Decoding Algorithms.
Sommario/riassunto	This book constitutes the refereed proceedings of the 12th International Conference on Code-Based Cryptography, CBCrypto 2024, held in Zurich, Switzerland, during May 25–26, 2024. The 5 full papers presented in this book were carefully reviewed and selected from 41

submissions. The conference offers a wide range of many important aspects of code-based cryptography such as cryptanalysis of existing schemes, the proposal of new cryptographic systems and protocols as well as improved decoding algorithms.