1. Record Nr. UNINA9910299745303321

Autore	Baldi Marco
Titolo	QC-LDPC Code-Based Cryptography / / by Marco Baldi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2014
ISBN	3-319-02556-2
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (128 p.)
Collana	SpringerBriefs in Electrical and Computer Engineering, , 2191-8112
Disciplina	005.82
Soggetti	Electrical engineering Coding theory Information theory Computer security Communications Engineering, Networks Coding and Information Theory Systems and Data Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references at the end of each chapters and index.
Nota di contenuto	Introduction -- Low-Density Parity-Check Codes -- Quasi-Cyclic Codes -- Quasi-Cyclic Low-Density Parity-Check Codes -- The McEliece and Niederreiter Cryptosystems -- QC-LDPC Code-based Cryptosystems.
Sommario/riassunto	This book describes the fundamentals of cryptographic primitives based on quasi-cyclic low-density parity-check (QC-LDPC) codes, with a special focus on the use of these codes in public-key cryptosystems derived from the McEliece and Niederreiter schemes. In the first part of the book, the main characteristics of QC-LDPC codes are reviewed, and several techniques for their design are presented, while tools for assessing the error correction performance of these codes are also described. Some families of QC-LDPC codes that are best suited for use in cryptography are also presented. The second part of the book focuses on the McEliece and Niederreiter cryptosystems, both in their original forms and in some subsequent variants. The applicability of QC-LDPC codes in these frameworks is investigated by means of

theoretical analyses and numerical tools, in order to assess their benefits and drawbacks in terms of system efficiency and security. Several examples of QC-LDPC code-based public key cryptosystems are presented, and their advantages over classical solutions are highlighted. The possibility of also using QC-LDPC codes in symmetric encryption schemes and digital signature algorithms is also briefly examined.