1.

Record Nr.	UNINA9910800117103321
Autore	Mechkaroska Daniela
Titolo	Cryptocoding Based on Quasigroups / / by Daniela Mechkaroska, Aleksandra Popovska-Mitrovikj, Verica Bakeva
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	3-031-50125-X
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (100 pages)
Collana	SpringerBriefs in Information Security and Cryptography, , 2731-9563
Disciplina	003.54
Soggetti	Data protection Coding theory Information theory Computer networks Cryptography Data encryption (Computer science) Set theory Algebra Data and Information Security Coding and Information Theory Computer Communication Networks Cryptology Set Theory Order, Lattices, Ordered Algebraic Structures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Quasigroups and quasigroups string transformation -- Cryptcodes based on quasigroup -- Experimental results for cryptcodes based on quasigroups for transmission through a binary-symmetric channel -- Experimental results for cryptcodes based on quasigroups for transmission through a Gaussian channel -- Fast algorithms for cryptcodes based on quasigroups -- Cryptcodes based on quasigroups for burst channels.
Sommario/riassunto	This book presents the concept of cryptcoding which arises from the need to obtain secure and accurate transmission. Therefore, it is

necessary to improve constantly existing and develop new algorithms that will ensure accurate and secure data transfer. This leads to the intensive development of coding theory and cryptography as scientific fields which solve these problems. To ensure efficient and secure data transmission at the same time, the concept of cryptcoding is developed such that the coding and encryption processes are merged into one process. Cryptcodes provide correction of a certain number of errors in the transmitted message and data confidentiality, using only one algorithm. The main research in this field is to define new algorithms for coding that detects and corrects errors, random codes, stream ciphers, block ciphers, pseudo-random generators, hash functions, etc. This monograph examines an application of quasigroups for designing error-correcting cryptcodes, called Random Codes Based on Quasigroups (RCBQ). These codes are a combination of cryptographic algorithms and error-correcting codes and depend on several parameters. Some modifications (new coding/decoding algorithms) of RCBQ for improving their performances for transmission ordinary messages, images, and audio files trough a binary-symmetric channel, Gaussian channel, and burst channels are considered. Also, authors propose and analyze filter for visually enhance of the decoded images and improving the quality of decoded audio files.