1. Record Nr. UNISA996550551403316

Autore	Nita Stefania Loredana
Titolo	Advances to Homomorphic and Searchable Encryption [[electronic resource] /] / by Stefania Loredana Nita, Marius Iulian Mihailescu
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2023
ISBN	3-031-43214-2
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (146 pages)
Altri autori (Persone)	MihailescuMarius Iulian
Disciplina	005.8
Soggetti	Data protection Quantum communication Artificial intelligence - Data processing Cryptography Data encryption (Computer science) Security systems Data and Information Security Quantum Communications and Cryptography Data Science Cryptology Security Science and Technology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1. Introduction -- 2. Background and Preliminaries -- 3. Homomorphic Encryption -- 4. Searchable Encryption.
Sommario/riassunto	This book presents the current state of the literature on the fields of homomorphic and searchable encryption, from both theoretical and practical points of view. Homomorphic and searchable encryption are still relatively novel and rapidly evolving areas and face practical constraints in the contexts of large-scale cloud computing and big data. Both encryption methods can be quantum-resistant if they use the right mathematical techniques. In fact, many fully homomorphic encryption schemes already use quantum-resistant techniques, such as lattices or characteristics of polynomials – which is what motivated the authors to present them in detail. On the one hand, the book highlights

the characteristics of each type of encryption, including methods, security elements, security requirements, and the main types of attacks that can occur. On the other, it includes practical cases and addresses aspects like performance, limitations, etc. As cloud computing and big data already represent the future in terms of storing, managing, analyzing, and processing data, these processes need to be made as secure as possible, and homomorphic and searchable encryption hold huge potential to secure both the data involved and the processes through which it passes. This book is intended for graduates, professionals and researchers alike. Homomorphic and searchable encryption involve advanced mathematical techniques; accordingly, readers should have a basic background in number theory, abstract algebra, lattice theory, and polynomial algebra.