1. Record Nr. UNINA9910906200703321

Autore	Adir Allon
Titolo	Homomorphic Encryption for Data Science (HE4DS) / / by Allon Adir, Ehud Aharoni, Nir Drucker, Ronen Levy, Hayim Shaul, Omri Soceanu
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031654947 3031654943
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (311 pages)
Altri autori (Persone)	AharoniEhud DruckerNir LevyRonen ShaulHayim SoceanuOmri
Disciplina	005.8 323.448
Soggetti	Data protection - Law and legislation Cryptography Data encryption (Computer science) Machine learning Computer networks - Security measures Privacy Cryptology Machine Learning Mobile and Network Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Part I Introduction and Basic Homomorphic Encryption (HE) Concepts -- Chapter 1 Introduction to Data Science -- Chapter 2 Modern Homomorphic Encryption - Introduction -- Chapter 3 Modern HE - Security Models -- Chapter 4 Approaches for Writing HE Applications -- Part II Approximations -- Chapter 5 Approximation Methods Part I: A General Overview -- Chapter 6 Approximation Methods Part II: Approximations of Standard Functions -- Part III Packing Methods -- Chapter 7 SIMD Packing Part I: Basic Packing Techniques -- Chapter 8

SIMD Packing Part II – Tile Tensor Basics -- Chapter 9 SIMD Packing Part III: Advanced Tile Tensors -- Part IV Use Cases and Other Approaches -- Chapter 10 Privacy-Preserving Machine Learning with HE -- Chapter 11 Case Study: Neural Network.

Sommario/riassunto

This book provides basic knowledge required by an application developer to understand and use the Fully Homomorphic Encryption (FHE) technology for privacy preserving Data-Science applications. The authors present various techniques to leverage the unique features of FHE and to overcome its characteristic limitations. Specifically, this book summarizes polynomial approximation techniques used by FHE applications and various data packing schemes based on a data structure called tile tensors, and demonstrates how to use the studied techniques in several specific privacy preserving applications. Examples and exercises are also included throughout this book. The proliferation of practical FHE technology has triggered a wide interest in the field and a common wish to experience and understand it. This book aims to simplify the FHE world for those who are interested in privacy preserving data science tasks, and for an audience that does not necessarily have a deep cryptographic background, including undergraduate and graduate-level students in computer science, and data scientists who plan to work on private data and models.