1. Record Nr. UNINA9910627259803321

Autore	Santikellur Pranesh
Titolo	Deep Learning for Computational Problems in Hardware Security : Modeling Attacks on Strong Physically Unclonable Function Circuits / / by Pranesh Santikellur, Rajat Subhra Chakraborty
Pubbl/distr/stampa	Singapore : , : Springer Nature Singapore : , : Imprint : Springer, , 2023
ISBN	981-19-4017-7
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (92 pages)
Collana	Studies in Computational Intelligence, , 1860-9503 ; ; 1052
Disciplina	006.3
Soggetti	Electronic circuits Artificial intelligence Mathematics Computers, Special purpose Computer science Electronic Circuits and Systems Artificial Intelligence Mathematics in Popular Science Special Purpose and Application-Based Systems Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Chapter 1: Introduction -- Chapter 2: Fundamental Concepts of Machine Learning -- Chapter 3: Supervised Machine Learning Algorithms for PUF Modeling Attacks -- Chapter 4: Deep Learning based PUF Modeling Attacks -- Chapter 5: Tensor Regression based PUF Modeling Attack -- Chapter 6: Binarized Neural Network based PUF Modeling -- Chapter 7: Conclusions and Future Work. .
Sommario/riassunto	The book discusses a broad overview of traditional machine learning methods and state-of-the-art deep learning practices for hardware security applications, in particular the techniques of launching potent "modeling attacks" on Physically Unclonable Function (PUF) circuits, which are promising hardware security primitives. The volume is self-contained and includes a comprehensive background on PUF circuits,

and the necessary mathematical foundation of traditional and advanced machine learning techniques such as support vector machines, logistic regression, neural networks, and deep learning. This book can be used as a self-learning resource for researchers and practitioners of hardware security, and will also be suitable for graduate-level courses on hardware security and application of machine learning in hardware security. A stand-out feature of the book is the availability of reference software code and datasets to replicate the experiments described in the book.