1. Record Nr. UNINA9910635396903321

Autore	Tehranipoor Mohammad H. <1974->
Titolo	Hardware Security Primitives [[electronic resource] /] / by Mark Tehranipoor, Nitin Pundir, Nidish Vashistha, Farimah Farahmandi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023
ISBN	3-031-19185-4
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (356 pages)
Disciplina	929.605
Soggetti	Electronic circuits Electronic circuit design Microprocessors Computer architecture Electronic Circuits and Systems Electronics Design and Verification Processor Architectures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Introduction -- Hardware Security Primitives and their Applications -- Racetrack PUF -- TERO PUF -- Direct Characterization PUF -- Volatile Memory Based PUF -- Emerging Memory Based PUF -- Extrinsic Characterization of PUF -- Radio PUFs and CoAs -- Optical PUFs -- True Random Number Generators -- Hardware Camouflaging -- Temper Detection Methods -- Embedded Watermarking -- Counterfeit and Recycled IC Detection -- Package-Level Counterfeit IC Detection -- Side Channels Protection in Cryptographic Hardware -- Fault Injection Resistant Cryptographic Hardware -- Energy and Performance Optimization for Cryptography -- Lightweight Cryptography -- Post-Quantum Cryptography -- Virtual Proof of Reality -- Analog Security.
Sommario/riassunto	This book provides an overview of current hardware security primitives, their design considerations, and applications. The authors provide a comprehensive introduction to a broad spectrum (digital and analog) of hardware security primitives and their applications for securing modern devices. Readers will be enabled to understand the various methods for

exploiting intrinsic manufacturing and temporal variations in silicon devices to create strong security primitives and solutions. This book will benefit SoC designers and researchers in designing secure, reliable, and trustworthy hardware. Provides guidance and security engineers for protecting their hardware designs; Covers a variety digital and analog hardware security primitives and applications for securing modern devices; Helps readers understand PUF, TRNGs, silicon odometer, and cryptographic hardware design for system security.