1. Record Nr. UNINA9910760263503321

Autore	Zamiri Azar Kimia
Titolo	Understanding Logic Locking [[electronic resource] /] / by Kimia Zamiri Azar, Hadi Mardani Kamali, Farimah Farahmandi, Mark Tehranipoor
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
ISBN	3-031-37989-6
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (385 pages)
Altri autori (Persone)	Mardani KamaliHadi FarahmandiFarimah TehranipoorMark
Disciplina	005.8
Soggetti	Electronic circuit design Embedded computer systems Electronic circuits Electronics Design and Verification Embedded Systems Electronic Circuits and Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Basics of VLSI Design -- Basics of VLSI Testing and Debug -- IP Protection in VLSI Design: A Historical View -- Making a Case for Logic Locking -- Fundamentals of Logic Locking -- Infrastructure around Logic Locking -- Impact of Satisfiability Solvers on Logic Locking -- Post-Satisfiability Era: Countermeasures and Threats -- Design-for-Testability and its Impact on Logic Locking -- Emergence of Cutting-edge Technologies on Logic Locking -- Logic Locking in Future IC Supply Chain Environments -- Multilayer Approach to Logic Locking -- A Step-by-Step Guide for Protecting/Locking Your IP -- A Step-by-Step Guide for Security Evaluation of Protected/Locked IP.
Sommario/riassunto	This book demonstrates the breadth and depth of IP protection through logic locking, considering both attacker/adversary and defender/designer perspectives. The authors draw a semi-chronological picture of the evolution of logic locking during the last decade, gathering and describing all the DO’s and DON’Ts in this

approach. They describe simple-to-follow scenarios and guide readers to navigate/identify threat models and design/evaluation flow for further studies. Readers will gain a comprehensive understanding of all fundamentals of logic locking. Covers modern VLSI design, testability and debug, and hardware security threats at different levels of abstraction; Provides a comprehensive overview of logic locking techniques and their applications to hardware security; Covers logic locking from implementation to evaluation, different assumptions, models and abstraction layers.