

1. Record Nr.	UNINA9910299470503321
Autore	Tehranipoor Mohammad
Titolo	Integrated circuit authentication : hardware trojans and counterfeit detection // Mohammad Tehranipoor, Hassan Salmani, Xuehui Zhang
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , 2014
ISBN	3-319-00816-1
Edizione	[1st ed. 2014.]
Descrizione fisica	1 online resource (xvi, 222 pages) : illustrations (some color)
Collana	Gale eBooks
Disciplina	004.1 004.22 620 621.3815
Soggetti	Integrated circuits - Verification Hardware Trojans (Computers)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Introduction -- Hardware Trojan Detection: Untrusted Third-party IP Cores -- Hardware Trojan Detection: Untrusted Manufactured Integrated Circuits -- Design for Hardware Trust: Dummy Scan Flip-flop Insertion -- Design for Hardware Trust: Layout-aware Scan Cell Reordering -- Design for Hardware Trust: Ring Oscillator Network -- Design Vulnerability Analysis -- Trojan Prevention: Built-In Self-Authentication -- Counterfeit Ics: Taxonomies, Assessment, and Challenges -- Counterfeit Ics: Detection and Prevention of Recycled Ics Using On-chip Sensors -- Counterfeit Ics: Pathy-Delay Fingerprinting.
Sommario/riassunto	This book provides readers with a comprehensive introduction to hardware Trojans. The authors explain the hardware Trojan taxonomy in detail, while delivering deep understanding of the potential impacts throughout the integrated circuit (IC) lifecycle. While discussing the shortcomings of current, industrial IC testing techniques for hardware Trojans, the authors describe the details of emerging techniques to detect them and to prevent their insertion into products. · Provides a comprehensive introduction to hardware Trojans and their potential impact on the integrated circuit lifecycle; · Equips designers with tools for identifying potential

vulnerabilities throughout the design cycle and manufacturing;

- Describes state-of-the-art techniques for hardware Trojan design, detection, and prevention;
- Analyzes susceptibility at the behavioral-, gate-, layout-level to Trojan insertion.

---