1. Record Nr. UNINA9910254168603321

Titolo	Hardware Security and Trust : Design and Deployment of Integrated Circuits in a Threatened Environment / / edited by Nicolas Sklavos, Ricardo Chaves, Giorgio Di Natale, Francesco Regazzoni
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2017
ISBN	3-319-44318-6
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (X, 254 p. 99 illus., 47 illus. in color.)
Disciplina	621.3815
Soggetti	Electronic circuits Microprocessors Electronics Microelectronics Circuits and Systems Processor Architectures Electronics and Microelectronics, Instrumentation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	AES Datapaths on FPGAs: a State of the Art Analysis -- Fault Attacks, Injection Techniques and Tools for Simulation -- Recent developments in side-channel analysis on Elliptic Curve Cryptography implementations -- Practical Session: Differential Power Analysis for Beginners -- Fault and Power Analysis Attack Protection Techniques for Standardized Public Key Cryptosystems -- Scan Design: Basics, Advancements and Vulnerabilities -- Manufacturing Testing & Security Countermeasures -- Malware Threats and Solutions for Trustworthy Mobile Systems Design -- Ring Oscillators and Hardware Trojan Detection -- Notions on Silicon Physically Unclonable Functions -- Implementation of delay-based PUFs on Altera FPGAs -- Implementation and Analysis of Ring Oscillator Circuits on Xilinx FPGAs.-.
Sommario/riassunto	This book provides a comprehensive introduction to hardware security, from specification to implementation. Applications discussed include

embedded systems ranging from small RFID tags to satellites orbiting the earth. The authors describe a design and synthesis flow, which will transform a given circuit into a secure design incorporating counter-measures against fault attacks. In order to address the conflict between testability and security, the authors describe innovative design-for-testability (DFT) computer-aided design (CAD) tools that support security challenges, engineered for compliance with existing, commercial tools. Secure protocols are discussed, which protect access to necessary test infrastructures and enable the design of secure access controllers. Covers all aspects of hardware security including design, manufacturing, testing, reliability, validation and utilization; Describes new methods and algorithms for the identification/detection of hardware trojans; Defines new architectures capable of detecting faults and resisting fault attacks; Establishes a design and synthesis flow to transform a given circuit into a secure design, incorporating counter-measures against fault attacks.