1. Record Nr. UNINA9910742492103321

Autore	Tehranipoor Mohammad H. <1974->
Titolo	Hardware Security Training, Hands-on! / / by Mark Tehranipoor, N. Nalla Anandakumar, Farimah Farahmandi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2023
ISBN	3-031-31034-9
Edizione	[1st ed. 2023.]
Descrizione fisica	1 online resource (XXIV, 320 p. 250 illus., 218 illus. in color.)
Disciplina	621.3815 005.8071
Soggetti	Electronic circuits Embedded computer systems Electronic circuit design Electronic Circuits and Systems Embedded Systems Electronics Design and Verification
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Chapter 1. Physical Unclonable Functions (PUFs) -- Chapter 2. True Random Number Generator (TRNG) -- Chapter 3. Recycled Chip Detection using RO-based Odometer -- Chapter 4. Recycled FPGA Detection -- Chapter 5. Hardware Trojan Insertion -- Chapter 6. Hardware Trojan Detection -- Chapter 7. Security Verification -- Chapter 8. Power Analysis Attacks on AES -- Chapter 9. EM Side-Channel Attack on AES -- Chapter 10. Logic Locking Insertion and Assessment -- Chapter 11. Clock Glitch Fault Attack on FSM in AES Controller -- Chapter 12. Voltage Glitch Attack on an FPGA AES Implementation -- Chapter 13. Laser Fault Injection Attack (FIA) -- Chapter 14. Optical Probing Attack on Logic Locking -- Chapter 15. Universal Fault Sensor -- Chapter 16. Scanning Electron Microscope Training.
Sommario/riassunto	This is the first book dedicated to hands-on hardware security training. It includes a number of modules to demonstrate attacks on hardware devices and to assess the efficacy of the countermeasure techniques.

This book aims to provide a holistic hands-on training to upper-level undergraduate engineering students, graduate students, security researchers, practitioners, and industry professionals, including design engineers, security engineers, system architects, and chief security officers. All the hands-on experiments presented in this book can be implemented on readily available Field Programmable Gate Array (FPGA) development boards making it easy for academic and industry professionals to replicate the modules at low cost. This book enables readers to gain experiences on side-channel attacks, fault-injection attacks, optical probing attack, PUF, TRNGs, odometer, hardware Trojan insertion and detection, logic locking insertion and assessment, and more. Discusses attacks including side-channel, fault-injection, optical probing, PUF, TRNGs, hardware Trojans and more Provides hands-on experiments, with step-by-step description, for attacks and countermeasure mechanisms Enables design of secure, reliable, and trustworthy hardware, via hands-on experience.