1. Record Nr. UNINA9910366578803321

Autore	Farahmandi Farimah
Titolo	System-on-Chip Security : Validation and Verification / / by Farimah Farahmandi, Yuanwen Huang, Prabhat Mishra
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-30596-1
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (295 pages)
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 contenuto	Introduction -- Security Verification Using Formal Methods -- Simulation-Based Security Validation Approaches -- Security Validation Using Side-Channel Analysis -- Automated Vulnerability Detection And Mitigation -- Conclusion.
Sommario/riassunto	This book describes a wide variety of System-on-Chip (SoC) security threats and vulnerabilities, as well as their sources, in each stage of a design life cycle. The authors discuss a wide variety of state-of-the-art security verification and validation approaches such as formal methods and side-channel analysis, as well as simulation-based security and trust validation approaches. This book provides a comprehensive reference for system on chip designers and verification and validation engineers interested in verifying security and trust of heterogeneous SoCs. Outlines a wide variety of hardware security threats and vulnerabilities as well as their sources in each of the stages of a design life cycle; Summarizes unsafe current design practices that lead to security and trust vulnerabilities; Covers state-of-the-art techniques as

well as ongoing research efforts in developing scalable security validation using formal methods including symbolic algebra, model checkers, SAT solvers, and theorem provers; Explains how to leverage security validation approaches to prevent side-channel attacks; Presents automated debugging and patching techniques in the presence of security vulnerabilities; Includes case studies for security validation of arithmetic circuits, controller designs, as well as processor-based SoCs.