1. Record Nr. UNINA9910799231803321

Titolo	Security of FPGA-Accelerated Cloud Computing Environments [[electronic resource] /] / edited by Jakub Szefer, Russell Tessier
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
ISBN	3-031-45395-6
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (X, 328 p. 187 illus., 157 illus. in color.)
Disciplina	621.3815
Soggetti	Electronic circuits Electronic circuit design Cooperating objects (Computer systems) Electronic Circuits and Systems Electronics Design and Verification Cyber-Physical Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction to, and history of, Cloud FPGAs -- FPGA device level security issues and countermeasures -- FPGA interfacing security issues (buses attacks, memory interfaces, etc -- IP protection for FPGAs in the cloud -- Software system security for cloud FPGAs (hypervisor leaks, shared memory use) -- Cross-node/network security – (e.g., voltage attack across nodes, network flooding by FPGAs) -- Likely future attacks -- Summary and conclusion.
Sommario/riassunto	This book addresses the security of FPGA-accelerated cloud computing environments. It presents a comprehensive review of the state-of-the-art in security threats and defenses. The book further presents design principles to help in the evaluation and design of cloud-based FPGA deployments which are secure from information leaks and potential attacks. Describes security threats of deploying FPGAs in cloud computing datacenters – and how to protect against them; Provides an overview of various security attacks of which cloud providers should be aware; Discusses defenses that can be deployed at system and hardware levels; Teaches readers about principles for securing cloud-

based FPGAs.