1. Record Nr. UNINA9910299942803321

Titolo	Fault Tolerant Architectures for Cryptography and Hardware Security / / edited by SIKHAR PATRANABIS, Debdeep Mukhopadhyay
Pubbl/distr/stampa	Singapore : , : Springer Singapore : , : Imprint : Springer, , 2018
ISBN	981-10-1387-X
Edizione	[1st ed. 2018.]
Descrizione fisica	1 online resource (242 pages)
Collana	Computer Architecture and Design Methodologies, , 2367-3478
Disciplina	004.2
Soggetti	Electronic circuits Data encryption (Computer science) System safety Circuits and Systems Cryptology Security Science and Technology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction to Fault Analysis -- Classical Fault Analysis -- Recent Trends and Advances in Fault Analysis -- Automation of Fault Analysis -- Countermeasures and Fault Tolerant Architectures -- Practical Perspectives of Fault Tolerant Design.
Sommario/riassunto	This book uses motivating examples and real-life attack scenarios to introduce readers to the general concept of fault attacks in cryptography. It offers insights into how the fault tolerance theories developed in the book can actually be implemented, with a particular focus on a wide spectrum of fault models and practical fault injection techniques, ranging from simple, low-cost techniques to high-end equipment-based methods. It then individually examines fault attack vulnerabilities in symmetric, asymmetric and authenticated encryption systems. This is followed by extensive coverage of countermeasure techniques and fault tolerant architectures that attempt to thwart such vulnerabilities. Lastly, it presents a case study of a comprehensive FPGA-based fault tolerant architecture for AES-128, which brings together of a number of the fault tolerance techniques presented. It concludes with a discussion on how fault tolerance can be combined

with side channel security to achieve protection against implementation-based attacks. The text is supported by illustrative diagrams, algorithms, tables and diagrams presenting real-world experimental results.