

Contents

1	AES Datapaths on FPGAs: A State of the Art Analysis	1
	João Carlos Resende and Ricardo Chaves	
2	Fault Attacks, Injection Techniques and Tools for Simulation	27
	Roberta Piscitelli, Shivam Bhasin and Francesco Regazzoni	
3	Recent Developments in Side-Channel Analysis on Elliptic Curve Cryptography Implementations	49
	Louiza Papachristodoulou, Lejla Batina and Nele Mentens	
4	Practical Session: Differential Power Analysis for Beginners	77
	Jiří Buček, Martin Novotný and Filip Štěpánek	
5	Fault and Power Analysis Attack Protection Techniques for Standardized Public Key Cryptosystems	93
	Apostolos P. Fournaris	
6	Scan Design: Basics, Advancements, and Vulnerabilities	107
	Samah Mohamed Saeed, Sk Subidh Ali and Ozgur Sinanoglu	
7	Manufacturing Testing and Security Countermeasures	127
	Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre and Paul-Henri Pugliesi-Conti	
8	Malware Threats and Solutions for Trustworthy Mobile Systems Design	149
	Jelena Milosevic, Francesco Regazzoni and Miroslaw Malek	
9	Ring Oscillators and Hardware Trojan Detection	169
	Paris Kitsos, Nicolas Sklavos and Artemios G. Voyiatzis	
10	Notions on Silicon Physically Unclonable Functions	189
	Mario Barbareschi	
11	Implementation of Delay-Based PUFs on Altera FPGAs	211
	Linus Feiten, Matthias Sauer and Bernd Becker	

12 Implementation and Analysis of Ring Oscillator
Circuits on Xilinx FPGAs 237
Mario Barbareschi, Giorgio Di Natale and Lionel Torres

Index 253



<http://www.springer.com/978-3-319-44316-4>

Hardware Security and Trust

Design and Deployment of Integrated Circuits in a
Threatened Environment

Sklavos, N.; Chaves, R.; Di Natale, G.; Regazzoni, F.
(Eds.)

2017, X, 254 p. 99 illus., 47 illus. in color., Hardcover

ISBN: 978-3-319-44316-4