

Contents

Part I Introduction

1	Security and Trust Vulnerabilities in Third-Party IPs	3
	Prabhat Mishra, Mark Tehranipoor, and Swarup Bhunia	

Part II Trust Analysis

2	Security Rule Check	17
	Adib Nahiyani, Kan Xiao, Domenic Forte, and Mark Tehranipoor	
3	Digital Circuit Vulnerabilities to Hardware Trojans	37
	Hassan Salmani and Mark Tehranipoor	
4	Code Coverage Analysis for IP Trust Verification	53
	Adib Nahiyani and Mark Tehranipoor	
5	Analyzing Circuit Layout to Probing Attack	73
	Qihang Shi, Domenic Forte, and Mark M. Tehranipoor	
6	Testing of Side-Channel Leakage of Cryptographic Intellectual Properties: Metrics and Evaluations	99
	Debapriya Basu Roy, Shivam Bhasin, Sikhar Patranabis, and Debdeep Mukhopadhyay	

Part III Effective Countermeasures

7	Hardware Hardening Approaches Using Camouflaging, Encryption, and Obfuscation	135
	Qiaoyan Yu, Jaya Dofe, Yuejun Zhang, and Jonathan Frey	
8	A Novel Mutating Runtime Architecture for Embedding Multiple Countermeasures Against Side-Channel Attacks	165
	Sorin A. Huss and Marc Stöttinger	

Part IV Security and Trust Validation

9 Validation of IP Security and Trust	187
Farimah Farahmandi and Prabhat Mishra	
10 IP Trust Validation Using Proof-Carrying Hardware	207
Xiaolong Guo, Raj Gautam Dutta, and Yier Jin	
11 Hardware Trust Verification	227
Qiang Xu and Lingxiao Wei	
12 Verification and Trust for Unspecified IP Functionality	255
Nicole Fern and Kwang-Ting (Tim) Cheng	
13 Verifying Security Properties in Modern SoCs Using Instruction-Level Abstractions.....	287
Pramod Subramanyan and Sharad Malik	
14 Test Generation for Detection of Malicious Parametric Variations ...	325
Yuanwen Huang and Prabhat Mishra	

Part V Conclusion

15 The Future of Trustworthy SoC Design.....	343
Prabhat Mishra, Swarup Bhunia and Mark Tehranipoor	
Index.....	351

Hardware IP Security and Trust

Mishra, P.; Bhunia, S.; Tehranipoor, M.M. (Eds.)

2017, XII, 353 p. 131 illus., 78 illus. in color., Hardcover

ISBN: 978-3-319-49024-3