

Contents

1	Introduction	1
1.1	Hardware Security and Trust	1
1.1.1	Hardware Trojans	3
1.1.2	Counterfeit ICs	12
	References	16
2	Hardware Trojan Detection: Untrusted Third-Party IP Cores	19
2.1	A Case Study for Hardware Trojan Detection in Third-Party Digital IP Cores	20
2.1.1	Formal Verification and Coverage Analysis	20
2.1.2	Techniques for Suspicious Signals Reduction	22
2.1.3	Simulation Results	25
2.2	Summary	30
	References	30
3	Hardware Trojan Detection: Untrusted Manufactured Integrated Circuits	31
3.1	A Case Study for Hardware Trojan Detection in Integrated Circuits	31
3.2	Summary	38
	References	38
4	Design for Hardware Trust: Dummy Scan Flip-Flop Insertion	39
4.1	Trojan Activation Time Analysis	39
4.2	Dummy Scan Flip-Flop Insertion	44
4.2.1	Removing Rare Triggering Conditions	47
4.2.2	Dummy Scan Flip-Flop Insertion Procedure	48
4.3	Transition Probability Threshold Analysis	50
4.4	Simulation Results	52
4.4.1	Without Dummy Flip-Flop	56
4.4.2	$P_{th} = 10e-05$	56
4.4.3	$P_{th} = 10e-04$	56

4.4.4	$P_{th} = 10e-03$	58
4.4.5	$P_{th} = 10e-02$	58
4.4.6	TE Attack Analysis	61
4.4.7	Transient Power Analysis	62
4.4.8	Sequential Trojan Analysis	65
4.5	Summary	65
	References	66
5	Design for Hardware Trust: Layout-Aware Scan Cell Reordering ...	69
5.1	Scan Cell Reordering	69
5.2	Trojan Detection and Isolation Flow	73
5.3	Switching Activity Localization Analysis	75
5.3.1	Localization Impact on Circuit Switching Activity	75
5.3.2	Localization Impact on Trojan Power Consumption	76
5.3.3	Localization Impact on Process Variations	78
5.4	Simulation Results	81
5.5	Summary	89
	References	89
6	Design for Hardware Trust: Ring Oscillator Network	91
6.1	Analyzing Impact of Power Supply Noise on Ring Oscillators ...	91
6.2	The Relationship Between RO Frequency and Localized and Total Dynamic Current	94
6.3	Ring Oscillator Network Structure	97
6.4	Measurement Flow and Statistical Analysis	99
6.5	Simulation Results and FPGA Implementation Analysis	101
6.5.1	Effectiveness Demonstration	103
6.5.2	Sensitivity Analysis	107
6.5.3	Experimental Results from Spartan-6 FPGA	110
6.6	ASIC Evaluation	113
6.6.1	Test Chip Design	113
6.6.2	Hardware Trojan Design	115
6.6.3	Experimental Setup	116
6.6.4	Experimental Results and Analysis	117
6.7	Summary	123
	References	123
7	Design Vulnerability Analysis	125
7.1	Vulnerability Analysis Flow	125
7.2	Vulnerability Analysis at the Behavioral Level	127
7.2.1	Statement Hardness	128
7.2.2	Observability	131
7.2.3	Trojans Insertion at the Behavioral Level	133
7.3	Vulnerability Analysis at the Gate Level	135
7.3.1	The Proposed Flow	135
7.3.2	Trojan Insertion at the Gate Level	137

7.4	Vulnerability Analysis at the Layout Level	140
7.5	Alleviating Circuit Vulnerabilities	141
7.6	Summary	143
	References	144
8	Trojan Prevention: Built-In Self-Authentication	147
8.1	BISA Structure and Insertion Flow	148
8.1.1	BISA Structure and Function	148
8.1.2	BISA Insertion Flow	150
8.1.3	BISA Design in System-On-Chips (SOCs)	154
8.2	Analyzing BISA Structure	154
8.2.1	BISA Test Coverage	154
8.2.2	Potential Attacks	155
8.2.3	Yield	156
8.3	Results and Analysis	156
8.4	Summary	160
	References	160
9	Counterfeit ICs: Taxonomies, Assessment, and Challenges	161
9.1	Counterfeit Taxonomy	161
9.1.1	Recycled	162
9.1.2	Remarked	162
9.1.3	Overproduced	164
9.1.4	Out-of-Spec/Defective	164
9.1.5	Cloned	165
9.1.6	Forged Documentation	165
9.1.7	Tampered	165
9.2	Electronic Component Supply Chain Vulnerabilities	166
9.3	Counterfeit Defects and Detection Methods	167
9.3.1	Defect Taxonomy	167
9.3.2	Detection Method Taxonomy	169
9.4	Challenges Ahead and Roadmap	172
9.4.1	Current State of Knowledge	172
9.4.2	Detection and Prevention Policies	173
9.4.3	The Need for Evaluating the Effectiveness of Detection Methods	173
9.4.4	Roadmap and Research Opportunities	175
9.5	Summary	177
	References	177
10	Counterfeit ICs: Detection and Prevention of Recycled ICs Using On-Chip Sensors	179
10.1	Background	183
10.1.1	Aging Analysis	183
10.1.2	Antifuse Memory	187

10.2	Recycled-IC Detection Sensors	187
10.2.1	RO-Based Sensor	188
10.2.2	AF-Based Sensor	190
10.3	Results and Analysis	193
10.3.1	RO-Based Sensor	193
10.3.2	AF-Based Sensors	200
10.3.3	Attack Analysis	202
10.4	Summary	204
	References	204
11	Counterfeit ICs: Path-Delay Fingerprinting	207
11.1	Path-Delay Degradation Analysis	207
11.2	Path-Delay Fingerprinting Considering Aging	210
11.3	Statistical Data Analysis	213
11.4	Results and Analysis	214
11.4.1	Process and Temperature Variations Analysis	214
11.4.2	Benchmark Analysis	219
11.5	Summary	220
	References	220
	Index	221

Integrated Circuit Authentication

Hardware Trojans and Counterfeit Detection

Tehraniipoor, M.; Salmani, H.; Zhang, X.

2014, XVI, 222 p. 120 illus., 65 illus. in color., Hardcover

ISBN: 978-3-319-00815-8