

Trusted Digital Circuits

Hassan Salmani

Trusted Digital Circuits

Hardware Trojan Vulnerabilities, Prevention
and Detection



Springer

Hassan Salmani
EECS Department
Howard University
Washington, DC, USA

ISBN 978-3-319-79080-0 ISBN 978-3-319-79081-7 (eBook)
<https://doi.org/10.1007/978-3-319-79081-7>

Library of Congress Control Number: 2018937677

© Springer International Publishing AG, part of Springer Nature 2018

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG part of Springer Nature.

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To Maryam and Karim

Preface

The complexity of modern designs, the significant cost of research and development, and the shrinking time-to-market window heavily enforce the horizontal integrated circuit design flow. Many entities across the globe might be involved in the flow and none are necessarily trusted. A malicious party can launch a hardware Trojan attack through manipulating a circuit to undermine its characteristics under rare circumstances at different stages of the flow before and after circuit manufacturing. Detection of hardware Trojans using existing pre-silicon and post-silicon verification techniques is a very challenging task because of the complexity of modern designs, their variety of application, and limited time for verification.

This book is entirely dedicated to study hardware Trojans across the integrated circuit design flow. Unprecedentedly, the book carefully studies integrated circuits at register-transfer level, gate level, and layout level against hardware Trojans. Vulnerabilities of each level to hardware Trojan insertion are discussed, and existing solutions for preventing and detecting hardware Trojans are studied. The book extends its study to hardware Trojan detection after integrated circuit manufacturing and deliberates current testing techniques for hardware Trojan detection. Vulnerabilities of mixed-signal circuits do not remain hidden, and the book studies possible hardware Trojan design in mixed-signal circuits and evaluates existing techniques for hardware Trojan prevention and detection in mixed-signal circuits.

This book is organized into nine chapters. Chapter 1 provides insights into the global integrated supply chain accompanied by statistics. It further defines hardware Trojans and explores their details. Chapter 2 studies vulnerabilities of an integrated circuit at the register-transfer level to hardware Trojan insertion. It comprehensively studies some of promising techniques for vulnerability quantification. In two major parts, Chap. 3 continues with hardware Trojan prevention and detection at the register-transfer level and discusses their effectiveness. Chapter 4 targets the vulnerabilities of gate-level circuits to hardware Trojans. Its main focuses are on techniques suggesting vulnerability quantifications at this level. Chapter 5 presents some of the best known techniques for hardware Trojan prevention and detection in a gate-level circuit. Chapter 6 continues with vulnerabilities of an integrated circuit to hardware Trojan insertion at the layout level. Chapter 7 then discusses some of

the known techniques for hardware Trojan prevention and detection at the layout level in detail. Chapter 8 presents an overview on some existing trusted test pattern generation for hardware Trojan detection after integrated circuit manufacturing. Chapter 9, the last chapter, demonstrates hardware Trojan implementation in mixed-signal circuits. It then studies some of the existing techniques for their prevention and detection.

The book offers a comprehensive and detailed analysis of hardware Trojans before and after integrated circuit manufacturing. This book provides design practitioners with guidance on protecting their designs against hardware Trojans and reveals research shortcomings that require attention to address hardware Trojans. The author would like to acknowledge that a part of this book is based on his research during a PhD program under the supervision of Dr. Tehranipoor at the University of Connecticut.

Washington, DC, USA

Hassan Salmani

Contents

1	The Global Integrated Circuit Supply Chain Flow and the Hardware Trojan Attack	1
1.1	The Global Integrated Circuit Supply Chain	1
1.2	The Hardware Trojan Attack	5
1.3	Conclusions	10
	References	11
2	Circuit Vulnerabilities to Hardware Trojans at the Register-Transfer Level	13
2.1	Circuits at the Register-Transfer Level	13
2.2	Value Range Analyses for Vulnerability Assessments	14
2.2.1	Statement Analysis	14
2.2.2	Observerability Analysis	18
2.2.3	Application of Value Range-Based Vulnerability Analysis ...	20
2.3	Unspecified IP Functionality	23
2.3.1	Hardware Trojans in Don't Cares	24
2.3.2	Dangerous Don't Cares Identification	24
2.4	Formal Verification and Coverage Analysis for Vulnerability Analyses	26
2.5	Conclusions	27
	References	28
3	Design Techniques for Hardware Trojans Prevention and Detection at the Register-Transfer Level	31
3.1	Hardware Trojan Prevention at the Register-Transfer Level	31
3.1.1	Dual Modular Redundant Schedule at High-Level Synthesis	31
3.1.2	Proof-Carrying Hardware	33
3.2	Hardware Trojan Detection at the Register-Transfer Level	35
3.2.1	Control-Flow Subgraph Matching	35
3.3	Conclusions	37
	References	38

4	Circuit Vulnerabilities to Hardware Trojans at the Gate Level	39
4.1	Circuits at the Gate-Level	39
4.2	Analyzing Vulnerabilities Based on Functional Analyses	39
4.3	Analyzing Vulnerabilities Based on Structural and Parametric Analyses	40
4.3.1	Hardware Trojan Ranking	43
4.4	Analyzing Vulnerabilities in Finite State Machines and Design-for-Test Structures	45
4.5	Conclusions	47
	References	47
5	Design Techniques for Hardware Trojans Prevention and Detection at the Gate Level	49
5.1	Hardware Trojan Prevention at the Gate Level	49
5.1.1	Information Flow Tracking for Hardware Trojan Prevention	49
5.2	Hardware Trojan Detection at the Gate Level	51
5.2.1	Signal Correlation-Based Clustering for Hardware Trojan Detection	51
5.2.2	Score-Based Classification for Hardware Trojans Detection	53
5.2.3	The Controllability and Observability Hardware Trojan Detection (COTD)	55
5.3	Conclusions	66
	References	67
6	Circuit Vulnerabilities to Hardware Trojan at the Layout Level	69
6.1	Circuits at the Layout Level	69
6.2	Motivation	70
6.3	Layout Vulnerability Analysis Flow	74
6.3.1	Cell and Routing Analyses	74
6.3.2	Net Analysis	76
6.4	Simulation Results	77
6.5	Conclusions	91
	References	92
7	Design Techniques for Hardware Trojans Prevention and Detection at the Layout Level	93
7.1	Hardware Trojan Prevention at the Layout Level	93
7.1.1	Dummy Scan Flip-flop Insertion and Layout-Aware Scan Cell Reordering	93
7.1.2	Ring Oscillator Network	95
7.1.3	Trojan Prevention and Detection (TPAD) Technique	95
7.1.4	Infrastructure IP for Security (IIPS) Technique	98

- 7.2 Hardware Trojan Detection at the Layout Level..... 99
 - 7.2.1 The Current Integration Technique 99
 - 7.2.2 Delay-Based Hardware Trojan Detection Using Shadow Registers 100
 - 7.2.3 Temperature-Based Hardware Trojan Detection 101
 - 7.2.4 Circuit Layout Reverse Engineering for Hardware Trojan Detection 104
- 7.3 Conclusions 106
- References 106
- 8 Trusted Testing Techniques for Hardware Trojan Detection 109**
 - 8.1 Fault Simulation-Based Test Pattern Generation 109
 - 8.2 Multiple Excitation of Rare Switching (MERS)..... 111
 - 8.3 Sustained Test Vector Methodology..... 113
 - 8.4 Monte Carlo-Based Test Pattern Generation Method 114
 - 8.5 Test Pattern Generation Based on ATPG and Model Checking..... 115
 - 8.6 Test Pattern Generation for Malicious Parametric Variations 117
 - 8.7 Conclusions 119
 - References 119
- 9 Hardware Trojans in Analog and Mixed-Signal Integrated Circuits .. 121**
 - 9.1 Hardware Trojans Design in Analog and Mixed-Signal Integrated Circuits 121
 - 9.1.1 Hardware Trojans in Wireless Cryptographic ICs..... 121
 - 9.1.2 Dynamic Analog Hardware Trojans 122
 - 9.1.3 Hardware Trojan Trigger by Capacitor 125
 - 9.1.4 Stealthy Dopant-Level Hardware Trojans 125
 - 9.2 Hardware Trojans Prevention and Detection in Analog and Mixed-Signal Integrated Circuits..... 127
 - 9.2.1 Positive Feedback Loop Analyses 127
 - 9.2.2 Information Flow Tracking in AMS Circuits..... 127
 - 9.2.3 Side-Channel Fingerprinting 128
 - 9.3 Conclusions 129
 - References 130