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

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