Preface

Outsourcing the design and fabrication of integrated circuits (ICs) has raised major concerns about their security and reliability. Realized by the intentional modification of design characteristics, hardware Trojans can obstruct a system's availability or intercept its confidentiality. Counterfeiting is also a growing issue that has raised serious concerns for the government and for industry. Counterfeit electronic components are unauthorized products that do not conform to their original design specifications. In addition to diminishing system dependability, counterfeiting reduces companies' total revenue from their research and development, discourages innovation through the theft of intellectual properties (IPs), and produces low-quality products under established brand names.

This book is intended to address these issues by presenting comprehensive and practice-oriented solutions for IC authentication. It provides insight into the IC supply chain and studies its vulnerabilities to hardware Trojans and counterfeiting.

This book is organized into 11 chapters. The first chapter provides an introduction to VLSI system integration and discusses hardware Trojans and counterfeiting as its two most challenging security issues. Chapter 2 presents a case study on the use of formal verification and code coverage analysis to detect Trojans inserted into third-party IP cores. Chapter 3 demonstrates a side-channel signal analysis technique for detecting Trojans in integrated circuits fabricated by untrusted foundries. Chapters 4 and 5 describe two design for hardware trust techniques to improve hardware Trojan detection. These techniques help activate a Trojan more effectively and increase side-channel signals induced by Trojans, making detection much easier for test engineers. Chapter 6 presents another design for hardware trust technique, an on-chip structure based on a ring oscillator network (RON) designed to monitor voltage fluctuations induced by Trojans and to differentiate noise created by hardware Trojans from noise made by process variations. Chapter 7 provides a comprehensive vulnerability analysis to effectively quantify the difficulties of the activation and observation of each circuit part. Further, it defines the Trojan detectability metric as a measurement of Trojan impact on circuit characteristics. Chapter 8 introduces the built-in self-authentication (BISA) technique as a means

to prevent Trojan insertion during GDSII development and mask generation by an untrusted foundry.

Chapter 9 presents a detailed taxonomy of counterfeit electronic components, defects, and anomalies associated with each of the counterfeit types and identifies the available detection techniques. It also discusses the major challenges for detecting and preventing counterfeit electronics. Chapter 10 demonstrates design of lightweight sensors that prevent counterfeiters from recycling parts found in used electronic systems. When such parts are recycled, test engineers can detect them extremely easily with these sensors, which provide information about the chip's usage in the field. Finally, Chap. 11 discusses a fingerprinting technique for the detection of counterfeit parts using circuit timing analysis.

Storrs, CT, USA

Mohammad Tehranipoor
Hassan Salmani
Xuehui Zhang

http://www.springer.com/978-3-319-00815-8

Integrated Circuit Authentication
Hardware Trojans and Counterfeit Detection
Tehranipoor, M.; Salmani, H.; Zhang, X.
2014, XVI, 222 p. 120 illus., 65 illus. in color., Hardcover
ISBN: 978-3-319-00815-8