

# Preface

Over the last two decades, the semiconductor industry has slowly moved toward the globalization of its supply chain. Due to increasing costs and complexity, it is no longer possible for a single corporation or entity to design, test, and fabricate today's integrated circuits (ICs) under one roof. With state-of-the-art semiconductor fabrication facilities or 'foundries' located across the world, the ability for IC design houses to monitor their own intellectual property (IP) has become limited. Similarly, system-on-chips or SoCs have also given rise to the concept of reusable IP-based design, whereby IP cores are sourced from several different vendors and integrated into one single SoC design. These trends have helped the industry to deal with the ever-growing complexity of ICs while keeping costs low and accelerating time-to-market.

Unfortunately, the benefits of globalization come at the inevitable cost of security. The convoluted supply chain introduces numerous opportunities for malicious parties to engage in IP piracy, counterfeiting and even introducing backdoors into a design. These malicious parties could be in the form of (i) untrusted foundries that fabricate the IC, (ii) third-party IP vendors, (iii) electronic design automation (EDA) tools, (iv) rogue insiders and disgruntled employees in a design house, (v) test or assembly facilities, and (vi) reverse engineers once the IC enters the supply chain. Thus, threats exist in each stage of the supply chain, and it is virtually impossible for one entity to 'trust' others with their IP in such a global landscape.

This book introduces the state of the art in hardware obfuscation which can be used to protect semiconductor IP at various levels of abstraction (e.g., register transfer, gate, or layout level). Hardware obfuscation techniques either conceal or lock the functionality and/or structure of the IC/IP so that it becomes difficult for a malicious or unauthorized party to engage in piracy or backdoor insertion. In contrast to watermarks or patents which are passive methods for IP protection, hardware obfuscation techniques are active; i.e., they deter reverse engineering and prevent piracy from ever happening in the first place.

While software obfuscation has received much attention over the years, the field of hardware obfuscation is relatively new. The past five years have seen an almost exponential growth in the amount of research work that has been done in the field.

Further, semiconductor companies and government entities have also shown an increased interest in developing viable options for hardware obfuscation, especially in light of numerous recent news on IP infringement cases, potential backdoors in chips manufactured offshore, IC reverse engineering techniques which were once thought to be impossible, and so on.

This book provides a comprehensive overview of various hardware obfuscation techniques that have been recently proposed by the research community. Although none of the individual techniques can provide a one-size-fits-all solution for all problems in hardware IP protection, they counter specific threats in the semiconductor supply chain, be it in the form of an untrusted foundry, reverse engineers in the supply chain, or a SoC designer willing to compromise a vendor's IP. The proposed techniques are also applicable to various levels of design abstraction, with some of them working to protect register transfer or gate-level IPs and others working to secure an IC layout.

A brief outline of the book is provided below.

1. **Hardware Obfuscation Preliminaries:** The first part of the book includes two introductory chapters on hardware obfuscation and background topics.
  - Chapter 1 describes the modern semiconductor supply chain, including each step of IC design and fabrication, the parties involved in these steps, and the resulting threats to security and trust. Recent advances in the field of hardware obfuscation, which are the subject of the remaining book chapters, are introduced as well. In addition, hardware obfuscation is differentiated from software obfuscation, cryptography, and other related work.
  - Chapter 2 provides background material on VLSI verification and testing. Topics include satisfiability, equivalence, fault modeling, controllability, observability, design-for-test, and other testing concepts that are often applied during hardware obfuscation methods and attacks. Popular hardware security primitives such as physical unclonable functions (PUFs) and true random number generators (TRNGs) that appear frequently throughout the book are also discussed.
2. **Logic-Based Hardware Obfuscation:** The second part of the book focuses on hardware obfuscation for combinational logic circuits, based on mechanisms such as key-based locking, permutation, and secure test infrastructure.
  - Chapter 3 introduces the concept of logic encryption, which involves ‘locking’ the functionality of a combinational circuit by inserting key-controlled gates. The chapter introduces basic logic encryption techniques, heuristics for inserting key gates, recent attacks on logic encryption (such as boolean satisfiability attacks and key propagation), and appropriate countermeasures.
  - Chapter 4 introduces the concept of circuit camouflaging, which involves configuring cells to perform different functionalities while maintaining an identical look to reverse engineers. A circuit partition-based attack and corresponding mitigation approach are proposed. The advantages of multiplexer-based circuit obfuscation cells are also discussed.

- Chapter 5 focuses on permutation-based obfuscation. The authors discuss the impact of permutation networks (such as Benes network) on resistance to brute-force attacks, discuss details of obfuscation on printed circuit boards (PCBs), and analyze the resiliency of permutation-based obfuscation to various physical attacks.
  - Chapter 6 discusses data leakage vulnerabilities introduced by test infrastructures such as scan chains and JTAG. Obfuscation techniques that lock the scan chain, scramble test responses, etc., are discussed to protect against such attacks.
3. **Finite State Machine (FSM) Based Hardware Obfuscation:** The third part of the book deals with sequential circuit obfuscation by locking of the finite-state machine (FSM) description of the circuit.
- Chapter 7 introduces the concept and flow of active hardware metering where the finite-state machine (FSM) description of a design is modified with additional states and a PUF. The security of the proposed approach is evaluated against FSM reverse engineering and brute-force attacks to guess the state transitions needed to unlock the design.
  - Chapter 8 introduces a hybrid scheme for FSM locking, in which modifications to the state transition graph of a circuit are combined with modifications to the original circuit in order to maximally deviate the circuit from its correct functionality. The benefits of this approach with respect to IP protection and targeted hardware Trojan insertion are also discussed.
  - Chapter 9 introduces the concept of ‘best possible obfuscation’ for sequential circuits. Four unique structural transformation operations along with a key are employed to lock the IC which functions in a degraded mode unless it is initialized properly.
4. **Hardware Obfuscation Based on Emerging Integration Approaches:** The fourth part of the book looks at emerging integration technologies such as 2.5D/3D ICs and split manufacturing for obfuscation against untrusted foundries.
- Chapter 10 leverages split manufacturing techniques to securely conceal design information from an untrusted foundry. Heuristic algorithms and gate anonymity metrics are introduced for lifting wires to the trusted back-end-of-line or BEOL layers.
  - Chapter 11 discusses the limitations of using split manufacturing and built-in self-authentication (BISA) independently against an untrusted foundry. A combined technique, called obfuscated BISA (OBISA), is introduced in order to combat both piracy and hardware Trojan threats. In OBISA, wire-lifting and filling of white spaces with fully testable functional filler cells are simultaneously performed to actively detect any tampering done by an untrusted foundry.
  - Chapter 12 leverages 2.5D IC technology in order to protect the design against an untrusted foundry. In 2.5D integration, an interposer layer

connecting different die is kept secret. Algorithms that partition a gate-level netlist and place-and-route with security and performance in mind are described.

5. **Other Hardware Obfuscation Building Blocks:** The fifth and last part of the book looks at secure mechanisms for key exchange to enable obfuscation at various steps in the semiconductor supply chain.
  - Chapter 13 discusses the building blocks and cryptographic primitives needed to transfer and protect secret keys (used by obfuscation) in different application instances (3PIP vendor and SoC designer, SoC designer and foundry, etc.). The IEEE P1735 standard is combined with hardware obfuscation and digest mechanisms in order to protect from additional attacks such as IP piracy and tampering.

We hope that this book serves as an invaluable reference for students, researchers, and practitioners in the field of hardware IP protection.

Gainesville, FL, USA

Domenic Forte  
Swarup Bhunia  
Mark M. Tehranipoor

Hardware Protection through Obfuscation

Forte, D.; Bhunia, S.; Tehranipoor, M.M. (Eds.)

2017, XII, 349 p. 148 illus., 121 illus. in color.,

Hardcover

ISBN: 978-3-319-49018-2