Analog Circuits and Signal Processing

The Analog Circuits and Signal Processing book series, formerly known as the Kluwer International Series in Engineering and Computer Science, is a high level academic and professional series publishing research on the design and applications of analog integrated circuits and signal processing circuits and systems. Typically per year we publish between 5–15 research monographs, professional books, handbooks, edited volumes and textbooks with worldwide distribution to engineers, researchers, educators, and libraries.

The book series promotes and expedites the dissemination of new research results and tutorial views in the analog field. There is an exciting and large volume of research activity in the field worldwide. Researchers are striving to bridge the gap between classical analog work and recent advances in very large scale integration (VLSI) technologies with improved analog capabilities. Analog VLSI has been recognized as a major technology for future information processing. Analog work is showing signs of dramatic changes with emphasis on interdisciplinary research efforts combining device/circuit/technology issues. Consequently, new design concepts, strategies and design tools are being unveiled.

Topics of interest include:

Analog Interface Circuits and Systems;

Data converters;

Active-RC, switched-capacitor and continuous-time integrated filters;

Mixed analog/digital VLSI;

Simulation and modeling, mixed-mode simulation;

Analog nonlinear and computational circuits and signal processing;

Analog Artificial Neural Networks/Artificial Intelligence;

Current-mode Signal Processing;

Computer-Aided Design (CAD) tools;

Analog Design in emerging technologies (Scalable CMOS, BiCMOS, GaAs, heterojunction and floating gate technologies, etc.);

Analog Design for Test;

Integrated sensors and actuators;

Analog Design Automation/Knowledge-based Systems;

Analog VLSI cell libraries;

Analog product development;

RF Front ends, Wireless communications and Microwave Circuits;

Analog behavioral modeling, Analog HDL.

More information about this series at http://www.springer.com/series/7381

Muhammad Yasin • Jeyavijayan (JV) Rajendran
Ozgur Sinanoglu

Trustworthy Hardware Design: Combinational Logic Locking Techniques

Springer

Muhammad Yasin
New York University Abu Dhabi
Saadiyaat Island, Abu Dhabi
United Arab Emirates

Ozgur Sinanoglu
New York University Abu Dhabi
Saadiyaat Island, Abu Dhabi
United Arab Emirates

Jeyavijayan (JV) Rajendran
Department of Electrical & Computer
Engineering, WEB 333H
Texas A&M University
College Station, TX, USA

ISSN 1872-082X ISSN 2197-1854 (electronic)
Analog Circuits and Signal Processing
ISBN 978-3-030-15333-5 ISBN 978-3-030-15334-2 (eBook)
https://doi.org/10.1007/978-3-030-15334-2

Muhammad Yasin would like to dedicate this book to the memory of his loving father and Prof. Masood Ahmad.
Jeyavijayan (JV) Rajendran would like to dedicate this book to his foreparents and teachers.
Ozgur Sinanoglu would like to dedicate this book to Cansu, Batu, and Bora.

Foreword

Today, we live in a world of constant communication, streaming entertainment, self-driving cars, and artificial intelligence all made possible by microelectronics and integrated circuits (IC). National defense enjoys similar benefits from seamless distributed military operations to smart weapons and electronic warfare. Microelectronics and integrated circuits are central to both our way of life and our defense of it.

As the role of microelectronics has grown, the way we manufacture them has changed. In the past, the Department of Defense accounted for roughly 40% of the microelectronics market; now, it is less than 0.5%. Due to the fantastic competition and cost pressures, what was a mostly on-shore industry dominated by American companies has become a global enterprise with a world wide supply chain. In fact, many of the world's largest electronic companies, such as Apple, are fabless. To provide the best electronics at the lowest prices, they outsource all their manufacturing to hyper-specialized on- and off-shore companies. This has been an unmitigated boon to consumers but presents risks both to fabless companies and nations. These risks include, but are not limited to, hardware-level tampering, reverse-engineering and intellectual property piracy, overproduction, counterfeiting, etc. For nation-states, the implications of these risks are even more dire especially for integrated circuits deployed in security-critical applications.

The key to an adversary realizing the aforementioned risks is a successful reverse engineering of the electronic part. Therefore, protecting the hardware design is central to any defensive strategy. A promising solution to protect the hardware is logic locking. Locking a circuit from reverse engineering with cryptographic-like rigor seems to be the most effective way to protect hardware against current and future attacks.

In 2017, I started the DARPA's Obfuscated Manufacturing for GPS program to seek out, develop, and validate the best logic locking techniques in academia and industry. The authors of this book formed the core of one of the most successful teams on the program. Their important 2012 work defined the threat model that has been used since then for logic locking and developed the first attack on logic locking.

This book provides a chronological evolution of the logic locking field. It starts with the very early logic locking defenses and attacks upon them and follows their descendants on both attack and defense to the present day. In the process, the book defines security metrics, different classes of attacks, and describes various design methods to deliver resiliency against these attacks. It serves not only as a detailed logic locking survey but also as a primer, with simple-to-follow examples for practicing designers.

The authors of this book have first-hand experience in the painstaking iteration from defense to offense and back again that are the hallmark of a robust logic locking technique. This familiarity with both sides of the attack/defense makes them the right team to deliver this highly informative book on logic locking. I am confident that it will be of great value to both academia and industry.

DARPA Microsystems Technology Office Ken Plaks
Washington, DC, USA
May 2019

Preface

The evolving complexity of integrated circuits and the skyrocketing cost of owning and maintaining foundries have spawned the growth of fabless business model. Fabless companies concentrate their resources and efforts on product design and marketing and outsource the complex fabrication, test, and assembly processes to offshore foundries and test/assembly companies that specialize in these services. This outsourcing of services to global vendors makes it easier for untrusted entities to gain access to proprietary assets and even manipulate the processing steps. Consequently, the globalization of the IC supply chain has led to the emergence of multiple security threats such as IP piracy, overbuilding, counterfeiting, reverse engineering, and the insertion of hardware Trojans. Apart from the direct economic losses to the industry, these security vulnerabilities pose a severe risk to the safety and reliability of electronic systems, not barring even life-threatening scenarios.

Many countermeasures have been developed and deployed to mitigate the security threats and rebuild the trust in a globalized supply chain. These defenses include watermarking, split manufacturing, camouflaging, hardware metering, and logic locking. A common challenge for these countermeasures is to offer the maximum security at the minimal implementation cost and with minimal changes to the conventional IC design/fabrication process. Logic locking has emerged as the most promising, versatile, and easy-to-integrate solution among all the aforementioned defenses. By incorporating simple additional logic into a circuit during the design phase, logic locking can mitigate security against IP piracy, overbuilding, and reverse engineering.

Over the last decade, logic locking has been garnering increasing interest from the research community, including academia and industry. The continued emergence of different classes of logic locking defenses and attacks has led to ever-stronger defenses, raising the bar for the attackers. The authors of this book have been involved with the logic locking research since its inception, with the involvement spanning from the publication of multiple fundamental papers in this field to the development of the first logic locked chip. The significant advancements in this new field and the increasing interest of the research community have motivated multiple systematization-of-knowledge attempts in the form of book chapters and journal

papers of tutorial nature. However, such publications are typically a recompilation of one or more research papers, with a focus on summarizing the state-of-the-art research. To attract practitioners to the field of logic locking, and thus hardware security, there has been a dire need to convey the fundamental principles following a pedagogical approach.

This book is an attempt to cover both breadth and depth of logic locking. It presents a comprehensive summary of logic locking defenses and attacks, describes their fundamental principles, and highlights the important research results. Consistent with the research trends, the bulk of the book is dedicated to the countermeasures that defend against the powerful SAT attack. The book systematizes the knowledge on logic locking attacks and defenses. It groups similar attacks and defenses, explains the common principles in detail, and elaborates on the essential differences. It supplements every important concept with illustrative circuit examples.

The book contains 11 chapters and an appendix on VLSI testing. Each chapter has been planned to emphasize the fundamental principles behind different classes of logic locking attacks and algorithms, progressively relating the new concepts to the previous ones. The first two chapters are introductory in nature, defining logic locking and presenting its brief history followed by a classification of attacks and defenses. We classify logic locking defenses into two main classes, pre-SAT and post-SAT, and the attacks into four classes, algorithmic, approximate, removal, and side-channel. Each of the following chapters focuses on a specific attack/defense technique. The last chapter summarizes the approaches presented in the book, highlights their challenges, and presents a few future research directions. Below is a comprehensive description of the contents of each chapter:

Chapter 1 motivates the need of logic locking in the context of the existing security vulnerabilities, introduces the basic definitions associated with logic locking, and compares logic locking with other design-for-trust approaches.

Chapter 2 presents a comprehensive history of logic locking followed by a classification of the logic locking attacks and defenses. It also introduces the metrics used to evaluate various logic locking approaches.

Chapter 3 focuses on the earliest "pre-SAT" logic locking techniques and presents three locking techniques, random, fault analysis-based, and strong logic locking, which essentially select suitable locations for inserting the additional logic, i.e., the XOR/XNOR or MUX key gates, into a netlist. It also introduces the sensitization attack that leverages the principles of VLSI testing to extract individual key bits of the secret key.

Chapter 4 focuses on the SAT attack, which is the most powerful of all attacks mounted on logic locking and circumvents all pre-SAT logic locking techniques. The attack is based on the notion of Boolean satisfiability. The chapter includes a review of the fundamental concepts of Boolean satisfiability, in addition to describing the attack algorithm with illustrative examples.

We classify the post-SAT logic locking techniques, which aim mainly at thwarting the SAT attack, into three subclasses: (1) point function-based, (2) SAT-unresolvable structure-based, and (3) stripped functionality-based logic locking

(SFLL). Chapter 5 focuses on the first subclass, which resists the SAT attack by increasing the number of SAT attack iterations. The chapter introduces three-point function-based logic locking techniques: (1) SARLock that integrates a comparator with the original design, (2) Anti-SAT that utilizes two complementary Boolean functions, and (3) AND-tree detection that searches for and locks the point functions already present in the original netlist.

While the point function-based locking techniques exhibit significant resilience to the SAT attack, these techniques and their variants remain vulnerable to two types of attacks: the approximate attacks and the removal attacks. The next two chapters of the book focus on these two classes of attacks. Chapter 6 elaborates on the operation of the approximate attacks that target compound locking techniques that integrate pre- and post-SAT locking techniques. It also presents two attacks, namely, AppSAT and Double-DIP, which recover only an approximate key.

Chapter 7 describes removal attacks that rely on the structural properties of various implementations of point functions to identify and isolate the original netlist from the protection circuitry. It presents four removal attacks, with each attack targeting a different point function-based defense.

The next two chapters of the book discuss the remaining two subclasses of post-SAT logic locking techniques. Chapter 8 describes how the SAT attack can be thwarted by inserting special structures that are hard to resolve by a SAT solver. The chapter introduces cyclic logic locking and one-way function-based logic locking (ORF-Lock). While cyclic logic locking can be broken using the CycSAT attack, ORF-Lock incurs high implementation cost and also remains vulnerable to removal attacks.

Chapter 9 presents SFLL, where the idea is to implement a modified on-chip circuit and restore the original functionality of the chip only upon activation with the correct key. SFLL is the first technique to offer quantifiable protection against all classes of attacks.

Chapter 10 elaborates on the side-channel attacks that leverage physical channels such as power and timing to extract information about the secret key. The chapter presents four side-channel attacks: the differential power analysis attack, the test-data mining attack, the hill-climbing attack, and the de-synthesis attack.

We anticipate the primary audience of the book to be the senior/graduate students in electrical and computer engineering and professionals in IC design and CAD software development, who have at least a rudimentary familiarity with the IC design flow. This book can be used as a textbook for courses on hardware security, VLSI CAD, or IC design. It can also serve as a "designer's guide" to implement logic locking in hardware designs. The book introduces the basic concepts of logic locking systematically in a way easy to follow for readers new to this field.

College Station, TX, USA — Muhammad Yasin
College Station, TX, USA — Jeyavijayan (JV) Rajendran
Abu Dhabi, United Arab Emirates — Ozgur Sinanoglu
Jan 2019

Acknowledgments

The authors would like to thank Prof. Ramesh Karri for his support and encouragement to pursue this effort. They would also like to acknowledge Zhaokun Han for proofreading and verifying the examples used in this book. The research covered in this book has in part been supported by the National Science Foundation (NSF), Semiconductor Research Corporation (SRC), Army Research Office (ARO), Defense Advanced Research Projects Agency (DARPA), Mubadala-SRC Center of Excellence for Energy-Efficient Systems (ACE4S), NYU/NYUAD Center for Cyber Security (CCS), and Texas A&M University. The authors acknowledge the crucial role of all these agencies and institutes in enabling this effort.

Contents

Acronyms

3PIP	Third-party intellectual property
AGR	AppSAT-guided removal
ATPG	Automatic test pattern generation
BA	Basic Anti-SAT
BEOL	Back end of line
DfTr	Design for trust
DPA	Differential power analysis
EPIC	Ending piracy of integrated circuits
FEOL	Front end of line
FLL	Fault analysis-based logic locking
FSM	Finite state machine
IC	Integrated circuit
IP	Intellectual property
LUT	Look-up table
OA	Obfuscated Anti-SAT
OC	Output corruptibility
OER	Output error rate
ORF	One-way random function
OSAT	Outsourced assembly and test
PPT	Probabilistic polynomial time
RLL	Random logic locking
SAT	Boolean satisfiability
SEM	Scanning electron microscope
SFLL	Stripped-functionality logic locking
SGS	Sensitization-guided SAT
SLL	Strong logic locking
SoC	System on chip
SPS	Signal probability skew
TDM	Test-data mining
TTLock	Tenacious and traceless logic locking