A Synergistic Framework for Hardware IP Privacy and Integrity Protection

Meng Li • David Z. Pan

A Synergistic Framework for Hardware IP Privacy and Integrity Protection

Springer

Meng Li
Department of Electrical
and Computer Engineering
The University of Texas at Austin
Austin, TX, USA

David Z. Pan
Department of Electrical
and Computer Engineering
The University of Texas at Austin
Austin, TX, USA

ISBN 978-3-030-41246-3 ISBN 978-3-030-41247-0 (eBook)
https://doi.org/10.1007/978-3-030-41247-0

This Springer imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

As the technology node scales down to 45 nm and beyond, the significant increase in design complexity and cost propels the globalization of the $400-billion semiconductor industry. However, such globalization comes at a cost. Although it has helped to reduce the overall cost by the worldwide distribution of integrated circuit (IC) design, fabrication, and deployment, it also introduces ever-increasing intellectual property (IP) privacy and integrity infringement. Recently, primary violations, including stealth hardware Trojan, unauthorized reverse engineering, and malicious fault attacks, have been reported by leading semiconductor companies and resulted in billions of dollars loss annually.

While hardware IP protection strategies are highly demanded, the researches were just initiated lately and still remain preliminary. Firstly, the lack of the mathematical abstractions for these IP violations makes it difficult to formally evaluate and guarantee the effectiveness of the protections. Secondly, the poor scalability and cost-effectiveness of the state-of-the-art protection strategies make them impractical for real-world applications. Moreover, the absence of a holistic IP protection further diminishes the chance to address these highly correlated IP violations which exploit physical clues throughout the whole IC design flow.

To protect hardware IP privacy and integrity, the book proposes a synergistic framework with a focus on security-aware design, optimization, and evaluation. The proposed framework consists of five interacting components that directly target at the primary IP violations. First, to prevent the insertion of the hardware Trojan, a split manufacturing strategy is proposed that achieves formal security guarantee while minimizing the introduced overhead. Then, to hinder reverse engineering, a fast security evaluation algorithm and a provably secure IC camouflaging strategy are proposed. Meanwhile, to impede the fault attacks, a new security primitive, named as public physical unclonable function (PPUF), is designed as an alternative to the existing cryptographic modules. A novel cross-level fault attack evaluation procedure also is proposed to help designers identify security-critical components to protect general purpose processors and compare different security enhancement strategies against the fault attack. All the five algorithms are developed based on

rigorous mathematical modeling for primary IP violations and focus on different stages of IC design, which can be combined synergistically to provide a formal security guarantee.

We are particularly grateful to Dr. Meng Li's PhD dissertation committee members, as the major material of this book is based on his dissertation. In particular, we want to thank Prof. Yier Jin for his detailed technical suggestions and guidance. It was a great pleasure to work with him and his group on the exciting area and projects on hardware security. We also want to thank Prof. Mohit Tiwari for his great course on the security issues in hardware/software interface and his insightful suggestions on this research projects. We would also like to thank Prof. Nan Sun and Prof. Nur A. Touba for the helpful discussions and their comments on this dissertation.

We are also grateful to Dr. Rob Aitken (Arm), Dr. Vikas Chandra (Facebook), Dr. Ben Gu (Cadence), Dr. Ru Huang (Peking University), Dr. Liangzhen Lai (Facebook), Dr. Sharad Mehrotra (Cadence), Dr. Jin Miao (Cadence), Dr. Runsheng Wang (Peking University), Dr. Ye Wang (Cadence), Dr. Haoxing Ren (Nvidia), Dr. Naveen Suda (Arm), and Dr. Albert Zeng (Cadence), for their valuable help, suggestions, and discussions on early draft of this book.

We would like to express our gratitude to the colleagues and alumni of the UTDA group at the University of Texas who gave us detailed expert feedback (e.g., Mohamed Baker Alawieh, Shounak Dhar, Wuxi Li, Derong Liu, Yibo Lin, Che-Lun Hsu, Jiaojiao Ou, Biying Xu, Xiaoqing Xu, Wei Ye, Zheng Zhao, Jingyi Zhou, Keren Zhu). Only through those inspiring discussions and productive collaborations that this book could be developed and polished.

We also thank the EDAA and the Springer Press publication team for their help and support in the development of this text. Last but not least, we would like to thank our families for their encouragement and support, as they endured the time demands that writing a book has imposed on us.

Austin, TX, USA — Meng Li
Austin, TX, USA — David Z. Pan
August 2018

Contents

Acronyms

BEOL	Back end of line
CRP	Challenge–reponse pair
ESG	Evaluation simulation gap
FEOL	Front end of line
FSM	Finite state machine
HD	Hamming distance
IC	Integrated circuit
IP	Intellectual property
KL	Kullback–Leibler
KNN	K-nearest neighbor
LDD	Lightly doped drain
LLN	Law of large number
LR	Lagrangian relaxation
MILP	Mixed-integer linear programming
MPU	Memory protection unit
PAC	Probably approximately correct
PPUF	Public physical unclonable function
PUF	Physical unclonable function
RBF	Radial basis function
RTL	Register-transfer level
SAT	Satisfiability
SD	Source degradation
SoC	System on chip
SPS	Signal probability skew
SSF	System security factor
SVM	Support vector machine
TU	Transformation unit