Studies in Computational Intelligence

Volume 1052

Series Editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland

The series “Studies in Computational Intelligence” (SCI) publishes new developments and advances in the various areas of computational intelligence—quickly and with a high quality. The intent is to cover the theory, applications, and design methods of computational intelligence, as embedded in the fields of engineering, computer science, physics and life sciences, as well as the methodologies behind them. The series contains monographs, lecture notes and edited volumes in computational intelligence spanning the areas of neural networks, connectionist systems, genetic algorithms, evolutionary computation, artificial intelligence, cellular automata, self-organizing systems, soft computing, fuzzy systems, and hybrid intelligent systems. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution, which enable both wide and rapid dissemination of research output.

Indexed by SCOPUS, DBLP, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

Pranesh Santikellur · Rajat Subhra Chakraborty

Deep Learning for Computational Problems in Hardware Security

Modeling Attacks on Strong Physically Unclonable Function Circuits

Springer

Pranesh Santikellur
Computer Science and Engineering
Indian Institute of Technology Kharagpur
Kharagpur, West Bengal, India

Rajat Subhra Chakraborty
Computer Science and Engineering
Indian Institute of Technology Kharagpur
Kharagpur, West Bengal, India

ISSN 1860-949X ISSN 1860-9503 (electronic)
Studies in Computational Intelligence
ISBN 978-981-19-4016-3 ISBN 978-981-19-4017-0 (eBook)
https://doi.org/10.1007/978-981-19-4017-0

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2023
This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Dedicated to,
Almighty "Gandhavahana", Appa, Amma,
my wife Anusha, our daughter Apeksha and
family members.

— Pranesh Santikellur

Dedicated to,
My wife Munmun and our daughter Agomoni.

— Dr. Rajat Subhra Chakraborty

Preface

Recent years have witnessed an increased focus on hardware security research. There have been significant advances in hardware security over the last decade. A recent discovery of chip vulnerabilities such as *Spectre* and *Meltdown* shows that the foundation of trust in hardware can also be insecure. Additionally, the tremendous growth of machine learning can either be a boon or a bane for hardware security. In the field of hardware security, Physically Unclonable Functions (PUFs) are being considered as a potential root of trust for solving hardware security problems. However, machine learning-based modeling attacks have been the greatest threat to PUF.

This book describes machine-learning applications for hardware security, focusing on modeling attacks against PUFs. The contents of this book are the results of our intensive research on the above-mentioned topic over the last few years. This book presents a practical guide for the use of machine learning in modeling attacks on PUF. We wrote this book to share our experience of research on modeling attacks on PUFs in a systematic and comprehensive way that covers both depth and breadth of the topic. Since this topic has not been covered in a single volume till date, we feel it would be of great value to any interested reader. The topics have been covered in sufficient depth to enable the reader to develop the understanding and skill-sets to explore it further. We have released the source-code corresponding to the PUF models and the modeling attacks in the public domain, to further aid the readers who would be interested in exploring this fascinating topic and enhancing the state of the art through future research.

Whether you are a complete beginner or an experienced researcher, the book brings together a formidable amount of theory and practical know-how under a single cover and will assist you in recollecting and gaining the knowledge of modeling attacks in the most comprehensive way.

Kharagpur, India
September 2021

Pranesh Santikellur
Dr. Rajat Subhra Chakraborty

Acknowledgements Pranesh Santikellur would like to acknowledge the financial support provided to him by Intel.

Contents

1 Introduction to Machine Learning for Hardware Security 1
1.1 Machine Learning: How is it Different from Traditional Algorithms? 3
1.2 Machine Learning for Hardware Security 4
1.2.1 ML for Hardware Attacks 4
1.2.2 ML for Hardware Attack Detection 5
1.2.3 ML for Attack on Countermeasures 6
1.3 Organization of the Book 6
References 7

2 Physically Unclonable Functions 9
2.1 Introduction 9
2.1.1 Properties of PUF 10
2.1.2 Quality Metrics of PUF 11
2.1.3 PUF Classification 12
2.2 Arbiter PUF (APUF) 13
2.2.1 Delay Model of Arbiter PUF 14
2.3 PUF Composition Types 14
2.3.1 XOR PUF Composition 16
2.3.2 Tribes PUF Composition 18
2.3.3 Multiplexer PUF (MPUF) and Its Variants 19
2.3.4 Interpose PUF (IPUF) 20
References 21

3 Machine-Learning Basics 23
3.1 Introduction 23
3.2 Machine-Learning Classification 24
3.3 Supervised ML Algorithms 25
3.3.1 Support Vector Machines 25
3.3.2 Logistic Regression 28
3.3.3 Artificial Neural Networks 30

3.4 Unsupervised ML Algorithms 33
3.4.1 K-means Clustering 33
References 34

4 Modeling Attacks on PUF 35
4.1 Introduction 35
4.2 Mathematical Model of Arbiter PUF (APUF) 36
4.3 Mathematical Model of XOR APUF 38
4.3.1 Motivation of Applying Deep Learning to PUF Modeling Attack 39
4.4 DFNN Architecture for Modeling Attack on APUF Compositions 40
4.4.1 Modeling Attack on XOR APUF 42
4.4.2 Modeling Attack on Double Arbiter PUF (DAPUF) 45
4.4.3 Modeling Attack on Multiplexer PUF and Its Variants 46
4.4.4 Modeling Attack on Interpose PUF (iPUF) 46
References 52

5 Improved Modeling Attack on PUFs based on Tensor Regression Network 55
5.1 Introduction 55
5.2 Tensor Basics 56
5.2.1 CP-Decomposition 57
5.2.2 Tensor Regression Networks 58
5.3 ECP-TRN: Efficient CP-Decomposition-Based Tensor Regression Networks 58
5.4 Experimental Results 61
5.4.1 Simulation and Modeling Setup 61
5.4.2 Modeling Accuracy Results 62
5.5 ECP-TRN-Based Modeling Attack XOR APUF Variants 65
5.5.1 ECP-TRN-Based Modeling Attack on Lightweight Secure PUF (LSPUF) 66
5.5.2 ECP-TRN-Based Modeling Attack on PC-XOR APUF 67
5.5.3 ECP-TRN-Based Modeling Attack on Mixed Challenge XOR APUF 67
References 68

6 Combinational Logic-Based Implementation of PUF 71
6.1 Introduction 71
6.1.1 ML-Based PUF Models in PUF-Based Authentication Protocols 72
6.2 Binarized Neural Networks 73
6.3 Optimized Combinational Logic-Based BNN Implementation 75

6.4 The APUF-BNN CAD Framework 77
6.4.1 BNN-Based Modeling Attack on APUF 78
6.4.2 Matrix Covering-Based Logic Optimization and Combinational Verilog Code Generation 78
6.5 Experimental Results 79
6.5.1 Setup 79
6.5.2 Experimental Results 79
References 81

7 Conclusion 83

About the Authors

Pranesh Santikellur is a Ph.D. student and a Senior Research Fellow in the Department of Computer Science and Engineering at the Indian Institute of Technology, Kharagpur. He received his B.E. degree in Electronics & Communication Engineering from Visvesvaraya Technological University, Belgaum, India, in 2010. He has a total of 6 years of industry experience at Horner Engineering India Pvt. Ltd. and Processor Systems. His primary research interest lies in hardware security, deep learning, and programmable logic controller security. He is an IEEE student member.

Rajat Subhra Chakraborty is an Associate Professor in the Department of Computer Science & Engineering of the Indian Institute of Technology, Kharagpur, India. He has professional experience working in National Semiconductor and Advanced Micro Devices (AMD). His research interest lies in the areas of hardware security, VLSI design, digital watermarking, and digital image forensics, in which he has published 4 books and over 100 papers in international journals and conferences of repute. He holds 2 granted U.S. patents. His publications have received over 3600 citations to date. Dr. Chakraborty has a Ph.D. in Computer Engineering from Case Western Reserve University, USA, and is a senior member of IEEE and ACM.