Physically Unclonable Functions (PUFs)

Applications, Models, and Future Directions

Synthesis Lectures on Information Security, Privacy, & Trust

Editors
Elisa Bertino, ***Yahoo! Labs***
Ravi Sandhu, ***University of Texas, San Antonio***

The Synthesis Lectures Series on Information Security, Privacy, and Trust publishes 50- to 100-page publications on topics pertaining to all aspects of the theory and practice of Information Security, Privacy, and Trust. The scope largely follows the purview of premier computer security research journals such as ACM Transactions on Information and System Security, IEEE Transactions on Dependable and Secure Computing and Journal of Cryptology, and premier research conferences, such as ACM CCS, ACM SACMAT, ACM AsiaCCS, ACM CODASPY, IEEE Security and Privacy, IEEE Computer Security Foundations, ACSAC, ESORICS, Crypto, EuroCrypt and AsiaCrypt. In addition to the research topics typically covered in such journals and conferences, the series also solicits lectures on legal, policy, social, business, and economic issues addressed to a technical audience of scientists and engineers. Lectures on significant industry developments by leading practitioners are also solicited.

Physically Unclonable Functions (PUFs): Applications, Models, and Future Directions
Christian Wachsmann and Ahmad-Reza Sadeghi
2014

Usable Security: History, Themes, and Challenges
Simson Garfinkel and Heather Richter Lipford
2014

Reversible Digital Watermarking: Theory and Practices
Ruchira Naskar and Rajat Subhra Chakraborty
2014

Mobile Platform Security
N. Asokan, Lucas Davi, Alexandra Dmitrienko, Stephan Heuser, Kari Kostiainen, Elena Reshetova, and Ahmad-Reza Sadeghi
2013

Security and Trust in Online Social Networks
Barbara Carminati, Elena Ferrari, and Marco Viviani
2013

RFID Security and Privacy
Yingjiu Li, Robert H. Deng, and Elisa Bertino
2013

Hardware Malware
Christian Krieg, Adrian Dabrowski, Heidelinde Hobel, Katharina Krombholz, and Edgar Weippl
2013

Private Information Retrieval
Xun Yi, Russell Paulet, and Elisa Bertino
2013

Privacy for Location-based Services
Gabriel Ghinita
2013

Enhancing Information Security and Privacy by Combining Biometrics with Cryptography
Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, and Bernadette Dorizzi
2012

Analysis Techniques for Information Security
Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps
2010

Operating System Security
Trent Jaeger
2008

© Springer Nature Switzerland AG 2022
Reprint of original edition © Morgan & Claypool 2015

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopy, recording, or any other except for brief quotations in printed reviews, without the prior permission of the publisher.

Physically Unclonable Functions (PUFs): Applications, Models, and Future Directions

Christian Wachsmann and Ahmad-Reza Sadeghi

ISBN: 978-3-031-01216-7 paperback
ISBN: 978-3-031-02344-6 ebook

DOI: 10.1007/978-3-031-02344-6

A Publication in the Springer series
SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST

Lecture #12
Series Editor: Elisa Bertino, *Yahoo! Labs*
Ravi Sandhu, *University of Texas, San Antonio*
Series ISSN
Print 1945-9742 Electronic 1945-9750

Physically Unclonable Functions (PUFs)

Applications, Models, and Future Directions

Christian Wachsmann
Intel Collaborative Research Institute for Secure Computing at TU Darmstadt, Germany

Ahmad-Reza Sadeghi
Technische Universität, Darmstadt, Germany

SYNTHESIS LECTURES ON INFORMATION SECURITY, PRIVACY, & TRUST #12

ABSTRACT

Today, embedded systems are used in many security-critical applications, from access control, electronic tickets, sensors, and smart devices (e.g., wearables) to automotive applications and critical infrastructures. These systems are increasingly used to produce and process both security-critical and privacy-sensitive data, which bear many security and privacy risks. Establishing trust in the underlying devices and making them resistant to software and hardware attacks is a fundamental requirement in many applications and a challenging, yet unsolved, task. Solutions solely based on software can never ensure their own integrity and trustworthiness while resource-constraints and economic factors often prevent the integration of sophisticated security hardware and cryptographic co-processors. In this context, Physically Unclonable Functions (PUFs) are an emerging and promising technology to establish trust in embedded systems with minimal hardware requirements.

This book explores the design of trusted embedded systems based on PUFs. Specifically, it focuses on the integration of PUFs into secure and efficient cryptographic protocols that are suitable for a variety of embedded systems. It exemplarily discusses how PUFs can be integrated into lightweight device authentication and attestation schemes, which are popular and highly relevant applications of PUFs in practice.

For the integration of PUFs into secure cryptographic systems, it is essential to have a clear view of their properties. This book gives an overview of different approaches to evaluate the properties of PUF implementations and presents the results of a large scale security analysis of different PUF types implemented in application-specific integrated circuits (ASICs). To analyze the security of PUF-based schemes as is common in modern cryptography, it is necessary to have a security framework for PUFs and PUF-based systems. In this book, we give a flavor of the formal modeling of PUFs that is in its beginning and that is still undergoing further refinement in current research.

The objective of this book is to provide a comprehensive overview of the current state of secure PUF-based cryptographic system design and the related challenges and limitations.

KEYWORDS

Physically Unclonable Functions (PUFs), physical security, embedded security, lightweight authentication, PUF-based remote attestation

Contents

Preface . . . . . **ix**

1 Introduction **1**

2 Basics of Physically Unclonable Functions **3**

2.1 PUF Concept, Properties, and Assumptions 3
2.2 PUF Types 3
2.2.1 Delay-based PUFs 4
2.2.2 Memory-based PUFs 9
2.2.3 Coating PUFs 12
2.2.4 Non-electric PUFs 12
2.3 Noise Compensation and Privacy Amplification 12

3 Attacks on PUFs and PUF-based Systems **15**

3.1 Emulation Attacks 15
3.2 Side Channel Attacks 15
3.3 Fault Injection Attacks 16
3.4 Invasive Attacks 16

4 Advanced PUF Concepts **19**

4.1 Controlled PUFs 19
4.2 Publicly Verifiable and Emulatable PUFs 19
4.3 Reconfigurable PUFs 20

5 PUF Implementations and Evaluation **23**

5.1 PUF Implementations in ASIC 23
5.2 Evaluation Methodology 25
5.2.1 Robustness Analysis 25
5.2.2 Unpredictability Analysis 26
5.3 Evaluation Results 30
5.3.1 Robustness Results 30
5.3.2 Unpredictability Results 32

5.3.3 Discussion . . . 32
5.4 Summary . . . 35

6 PUF-based Cryptographic Protocols . . . 37
6.1 Lightweight Authentication Based on PUFs . . . 37
6.1.1 Literature Overview of PUF-based Device Authentication . . . 38
6.1.2 Protocol Description and Specification . . . 39
6.1.3 Security Analysis . . . 41
6.2 PUF-based Attestation . . . 41
6.2.1 Protocol Description and Specification . . . 42
6.2.2 Security Analysis . . . 44

7 Security Model for PUF-based Systems . . . 47
7.1 Literature Overview of PUF Security Models . . . 47
7.2 Framework for Physical Functions . . . 48
7.2.1 Background and Rationale . . . 48
7.2.2 Formalization . . . 50
7.3 Robustness . . . 51
7.3.1 Rationale . . . 51
7.3.2 Formalization . . . 52
7.4 Physical Unclonability . . . 52
7.4.1 Rationale . . . 52
7.4.2 Formalization . . . 53
7.5 Unpredictability . . . 55
7.5.1 Rationale . . . 55
7.5.2 Formalization . . . 57
7.6 Conclusion . . . 59

8 Conclusion . . . 61

Terms and Abbreviations . . . 64

Bibliography . . . 65

Authors' Biographies . . . 81

Preface

Since embedded systems are deployed in many critical settings, their security, privacy, and safety aspects are of utmost concern. However, these systems are typically not protected against hardware attacks that aim at extracting the authentication secrets of these devices and to clone them. A general challenge for these systems is binding cryptographic protocols to the underlying hardware in a unique and unclonable way. In this context, Physically Unclonable Functions (PUFs) are a promising technology which exploits physical properties of hardware and can be integrated into cryptographic schemes. Since the introduction of PUFs in 2001 [91], researchers proposed many different PUF designs and a large variety of PUF-based security mechanisms. There are already some products using PUF technology in the market. PUFs were celebrated as promising primitives and many researchers investigated various aspects of PUFs including their design, implementation, and protocol integration as well as attacks on PUFs and PUF-based systems.

This book gives an introduction to PUFs and their integration into secure PUF-based cryptographic systems and security mechanisms. It explains the PUF concept and the state of the art of PUF-based protocol design on the example of PUF-based device authentication and remote attestation. The book gives insights into the formal modeling of PUFs, which is essential for the security analysis of PUF-based systems and still in its beginning.

We intend this book to be useful for students, active researchers, and practitioners. We hope that it serves as an introduction to PUFs and the design of secure PUF-based cryptographic schemes. Researchers starting their research on PUFs and PUF-based systems can use this book to familiarize themselves with the state of the art.

Parts of this book are based on Christian Wachsmann's doctoral dissertation [133]. Other parts are the result of joint collaborative research between the authors and our esteemed colleges and partners, including Frederik Armknecht, Anthony van Herrewege, Stefan Katzenbeisser, Ünal Koçabas, Farinaz Koushanfar, Joonho Kong, Vincent van der Leest, Roel Maes, Yossef Oren, Roel Peeters, Praveen K. Pendyala, Vladimir Rožić, Geert-Jan Schrijen, Heike Schröder, François-Xavier Standaert, and Ingrid Verbauwhede.

We thank Prof. Elisa Bertino for inviting us to write this book, Diane Cerra for supporting us in all organizational aspects, and Marina Blanton and Jorge Guajardo for their helpful comments.

Christian Wachsmann and Ahmad-Reza Sadeghi
December 2014