

Preface

Information security techniques are indispensable in a world that relies, in a continuously increasing extent, on digital information processing and communication systems. The use of cryptographic primitives enables us to reduce information security goals to physical security requirements, such as secure algorithm execution, and the secure generation and storage of secrets. *Physically unclonable functions*, or *PUFs*, are innovative physical security primitives which produce unclonable and inherent instance-specific measurements of physical objects; PUFs are in many ways the inanimate equivalent of biometrics for human beings. Since they are able to securely generate and store secrets, PUFs allow us to bootstrap the physical implementation of an information security system. In this book, we discuss PUFs in all their facets: the multitude of their physical *constructions*, the algorithmic and physical *properties* which describe them, and the techniques required to deploy them in security *applications*.

We first give an extensive overview and classification of PUF constructions, with a focus on *intrinsic PUFs*. We identify significant subclasses, implementation properties and general design techniques used to amplify sub-microscopic physical distinctions into observable digital response vectors. We list the useful properties attributed to PUFs and capture them in descriptive yet clear definitions. Through an elaborate comparative analysis, PUF-defining properties are distinguished from nice-to-have but not strictly required qualities. Additionally, a formal framework for deploying PUFs and similar physical primitives in cryptographic reductions is described.

In order to objectively compare the quality of different PUF constructions, we contributed to the development of a silicon test platform carrying six different intrinsic PUF structures. Based on experimental data from 192 distinct test devices, including measurements at temperature and supply voltage corner cases, the reliability, the uniqueness and the unpredictability of each of these constructions is assessed, and summarized in concise yet meaningful statistics.

Their instance-specific and unclonable nature enables us to use PUFs as entity identifiers. In combination with appropriate processing algorithms, they can even authenticate entities and securely generate and store secrets. We present techniques

to achieve PUF-based entity identification, entity authentication, and secure key generation. Additionally, we propose practical designs that implement these techniques, and derive and calculate meaningful measures for assessing the performance of different PUF constructions in these applications, based on the quality of their response statistics. Finally, as a proof of concept, we present a fully functional prototype implementation of a PUF-based cryptographic key generator, demonstrating the full benefit of using PUFs and the efficiency of the introduced processing techniques.

Acknowledgements

The origin of this book is the thesis I wrote as the conclusion of my Ph.D. degree, discussing the main research topics I worked on, and contributed to, between 2007 and 2012. It is evident that a Ph.D. can only be successfully completed with the help of many people and instances.

Before all others, I am grateful to my promoter Prof. Ingrid Verbauwhede, for the opportunities she created for me, for her advice on matters great and small, and for trusting me to find my own way. I am also much indebted to Dr. Pim Tuyls for introducing me to the exciting topic of this book, for guiding me through my first couple of years as a young researcher, and in general for taking the idea of PUFs to a whole new level. In addition, I want to thank the other members of my Ph.D. jury for their combined effort in reviewing the text of my thesis, the KU Leuven for offering such an inspiring academic environment, and the Agency for Innovation by Science and Technology (IWT) for funding the major part of my Ph.D. research.

Being an academic researcher is far from a solitary occupation, and I have had the pleasure and privilege of meeting and collaborating with many of my peers worldwide. I must acknowledge all of my appreciated coauthors over the years, for their guidance and contribution. A special thanks goes out to the partners of the European UNIQUE project, and the people behind them, with whom it was always a pleasure to meet and discuss things, and from whom I have learned a lot. I also greatly enjoyed the opportunities to get a taste of life as a researcher in industry, through internships at Philips and Intel; both were extremely challenging experiences which have had a significant positive impact on me.

It is hard to overestimate my gratitude for having been able to work for five years in an atmosphere as vibrant, yet warm and friendly as the COSIC research group. Over the years I have seen people come and go, but the helpfulness, sociability and plain fun were invariably present. One of the many special people responsible for this is P  la No  , COSIC's secretary and so much more, but I am grateful to all my colleagues who made COSIC such an enjoyable place to work.

Geel, Belgium
September 2013

Roel Maes

Physically Unclonable Functions
Constructions, Properties and Applications

Maes, R.

2013, XVII, 193 p. 28 illus., Hardcover

ISBN: 978-3-642-41394-0