Chapter 7
Conclusion and Future Work

7.1 Conclusions

PUFs are physical security primitives which enable trust in the context of digital hardware implementations of cryptographic constructions, in particular they are able to initiate physically unclonable and secure key generation and storage. In this book we have studied physically unclonable functions or PUFs, in particular: (i) their concept and constructions, (ii) their properties, and (iii) their applications as a physical root of trust, and the relations between these three.

In Chap. 2 we introduced the concept of a physically unclonable function in great detail through an extensive study and analysis of earlier work and existing constructions. Based on similar and distinguishing construction characteristics, we discussed strengths and weaknesses and possible classifications. The most noteworthy identified subclass is so-called *intrinsic PUFs*, i.e. PUF constructions which are based on internal evaluations of implicitly obtained random creation features, because they are particularly well-fit for integration in larger security systems. It is however difficult to compare the practical value of different proposals from the literature due to a wide variety of implementation technologies and experimental considerations. The lateral overview does present a good insight in recurring intrinsic PUF implementation techniques: (i) amplification of microscopic unique features through differential measurement, (ii) physical enhancement of PUF behavior through low-level (design-intensive) implementation control, and (iii) algorithmic behavioral improvement through adapted post-processing techniques.

In Chap. 3 we identified the most important usability and physical security properties attributed to PUFs and we introduced clear definitions pointing out what exactly each of these properties signify. Through a comparative analysis on a representative subset of PUF constructions and a number of important non-PUF reference cases, we discovered which properties are really *defining* for a PUF construction, and which are convenient additions but are in no way guaranteed for every PUF. As it turns out, the core defining property of a PUF is its *physical unclonability*. A second contribution of this chapter was the introduction of a formal framework

R. Maes, *Physically Unclonable Functions*, DOI 10.1007/978-3-642-41395-7_7,

for using PUFs, and more general physical security primitives, in theoretical security reductions at a higher level. We defined robustness, physical unclonability and unpredictability in this framework.

With the goal of testing their security and usability characteristics as accurately and as objectively as possible, we implemented and evaluated eight different intrinsic PUF constructions on a 65 nm CMOS silicon platform. The design process and the experimental results of this ASIC chip are described in detail in Chap. 4. The measurements of each of these eight constructions were tested for their reproducibility and their uniqueness through a characterization of their respective intra- and inter-distance distributions using well-chosen statistical parameters. The unpredictability of the studied PUFs is also estimated by proposing and evaluating a number of increasingly tighter upper bounds of the entropy density of their response bitstrings. The experiments in this chapter yielded the first-ever objective comparison between multiple different intrinsic PUF constructions on the same platform, and a quantitative representation of their primary characteristics which can be directly used to assess their efficiency and performance in the following physical security applications.

The first PUF-based security applications we considered in Chap. 5 were entity identification and authentication, as defined in Sect. 5.1.1. We first elaborated on the identifiability property of PUFs and demonstrated how a fuzzy identification scheme based on PUF responses can be set up, equivalent to biometric identification. Based on the measured characteristics of the eight intrinsic PUF construction studied in Chap. 4, we evaluated their identifying capabilities based on the typical fuzzy identification performance metrics of false acceptance and rejection rates which are combined in receiver-operating characteristics and equal error rates. Next, we proposed a new mutual authentication protocol for PUF-carrying entities with significantly relaxed security conditions for the used PUF such that it can deploy any intrinsic PUF construction. The primary innovative aspect of this protocol is an atypical use of an error-correction technique which results in a secure yet very lightweight authentication solution. Based on this scheme, the authentication performance and efficiency of the eight studied intrinsic PUFs was again compared.

Next, in Chap. 6, we discussed in detail the prerequisites and security considerations for PUF-based secure key generation and storage, and presented and evaluated practical constructions and implementations. We first studied existing techniques and constructions for enhancing the reliability of fuzzy data, so-called secure sketches, and for boosting the unpredictability of a derived key, either from an information-theoretic perspective, based on strong and fuzzy extractors, or from a practical perspective, based on entropy accumulators. The first main contribution of Chap. 6 was a new and significantly improved construction of a secure sketch based on the innovative idea of using available soft-decision information of the PUF's response bits. Secondly, we introduced a practical generalization of fuzzy extractors in which we traded information-theoretical security for a large gain in efficiency, while still retaining adequate security based on widely used best-practice entropy accumulation. Again, we tested the key generation capacity of the eight studied intrinsic PUFs, based on a proposed design of a practical fuzzy extractor. Lastly,

to demonstrate the feasibility and applicability of this design, we made a fully functional, efficient, yet flexible FPGA reference implementation of a PUF-based key generator, including a newly proposed ring-oscillator PUF with Lehmer-Gray response encoding, a practical secure sketch based on a new highly optimized BCH decoder, and entropy accumulation with a lightweight hash function.

7.2 Future Work

The generic concept of a physically unclonable function was presented little over a decade ago, but the major research contributions on this topic are situated in the last couple of years. PUFs are hence a relatively new subject in the field of physical security, and a number of interesting future research directions, as well as some encountered open problems can be identified.

PUF Constructions As pointed out a number of times in this book, one of the major open questions on the side of PUF constructions is if, and how, an efficient truly unclonable intrinsic PUF, also called a strong PUF by some authors, can be built. Some candidate circuits have been proposed, but they are currently lacking any convincing argumentation of being unpredictable which is required for achieving mathematical and true unclonability. Due to the difficulty of mathematically proving unpredictability based on physical arguments, it is more convenient to assess unpredictability in relation to the best known attack. This method has been applied successfully in recent decades to cryptographic symmetric-key primitives. However, to make independent analysis possible, Kerckhoffs' principle needs to be obeyed. For physical security primitives like PUFs, this entails that the full design *and* implementation details of a proposed construction need to be disclosed. A more practical alternative is to publish, in an easily accessible electronic format, extensive datasets of experimental PUF evaluations for public scrutiny. We hope that the practical performance evaluation methods proposed in this book can contribute to more meaningful and objective assessments of the value of different PUF constructions.

Another open issue is the construction of a physically reconfigurable PUF, as discussed in Sect. 2.5.3. Rather exotic suggestions were proposed but never tested. A logically reconfigurable PUF is a good emulation from the behavioral perspective, but does not achieve the same strong physical security qualities.

Finally, as with all hardware (security) primitives, continuing research effort is required to develop increasingly more efficient constructions which offer better trade-offs and enable applications in resource-constrained environments.

PUF Properties For PUF properties, we see the need for research effort on two levels. Firstly, on a practical level, more detailed methods and techniques need to be developed and investigated for assessing if, and to what extent, a proposed PUF construction meets a particular property. For some properties, this is based on an analysis of the inter- and intra-distance distributions of measured PUF responses, and a number of evaluation methods have been proposed in this book. Presenting detailed

and accurate statistics of these distributions is hence indispensable when proposing a new PUF construction. In-depth and independent analysis of a PUF's construction and experimental results is required to assess its unpredictability, e.g. by means of tighter response entropy bounds.

For other properties, an assessment is based on physical arguments and this is again difficult to approach from a mathematical perspective. Qualities like physical unclonability and tamper evidence can, and should only be assessed in a heuristic manner. Especially the core property of physical unclonability requires special attention in that regard. A PUF which, through improved physical insights or technological progress, is found to be no longer physically unclonable, ceases to be a PUF.

On a more theoretical level, it needs to be further investigated how PUFs can be deployed as formal primitives in a security system, i.e. allow theoretical designers to reason about PUFs in a formal way without having to worry about their physical aspects, which are often beyond their expertise. We have proposed such a formal framework for describing physical functions and have applied this to PUFs and their core properties. Extending this framework to other primitives and properties will be an interesting and fruitful exercise.

PUF Applications In this book, we have demonstrated how to achieve two primary PUF-based security objectives: entity authentication and secure key generation/storage. We see further developments possible, both in trying to achieve basic security objectives based on PUFs, as well as attempting to integrate PUFs and PUF-based primitives securely and efficiently into larger security systems. A noteworthy direction of the former which was not further discussed in this book is so-called *hardware-entangled cryptography*, i.e. designing basic cryptographic primitives which directly deploy a PUF as a building block. We introduced this approach in [2] and illustrated it with a secure design of a PUF-based block cipher.

To facilitate the further deployment of PUFs in security systems, we see the following interesting and essential future challenges:

- A greater insight and effort on the low-level silicon circuit design of intrinsic PUF constructions will result in increasingly more efficient (smaller, more robust, more random) structures.
- Both incremental and fundamental progress in the development and application of post-processing techniques required to use a PUF (reliability enhancement, randomness extraction, ...) is possible, e.g. the use of alternative error-correction techniques (non-binary codes, non-linear codes, ...) and more insight into entropy accumulation techniques.
- Other physical security qualities of PUFs need to be considered, in particular their resistance to side-channel attacks. Initial work on side-channel analysis of PUFs was recently introduced by Karakoyunlu and Sunar [62], Merli et al. [97], but more elaborate research efforts are required.

To conclude, we expect that the continuous improvements and better understanding of their practicality and of the physical as well as algorithmic security of PUFs will enable and accelerate their further transition into common and new security applications.