Risk Analysis of Physically Unclonable Functions

Andrea Kolberger, Ingrid Schaumüller-Bichl, Martin Deutschmann

Risk Analysis of Physically Unclonable Functions

Andrea Kolberger[1], Ingrid Schaumüller-Bichl[1], and Martin Deutschmann[2]

[1] University of Applied Sciences Upper Austria
{andrea.kolberger, ingrid.schaumueller-bichl}@fh-hagenberg.at
[2] Technikon Forschungs- und Planungsgesellschaft mbH
codes@technikon.com

Abstract. Physically unclonable functions (PUFs) are an emerging technology that have been proposed as central building blocks in a variety of cryptographic application areas. Keys are not stored permanently anymore, but generated as needed using unique "fingerprints" that are inherent in each device. Since PUFs are "noisy" functions responses generated by a certain PUF instantiation are error-prone and therefore highly sophisticated error correction is required to reliably reconstruct the respective PUF response. To be aware of potential threats and vulnerabilities concerning PUF-based security schemes a risk analysis on different use cases was performed in order to gain requirements for the development and implementation of effective error correction methods as well as requirements regarding the whole operational life cycle of such tokens.

Keywords: Physically Unclonable Function (PUF), Risk Analysis, Vulnerabilities and Threats, Authentication, HW/SW Binding, Key Generation, Error Correction, Fuzzy Extractor, Cryptographic Applications

1 Introduction

PUFs are inherently "noisy" which means that responses of a single PUF instantiation to one and the same challenge always slightly differ. Such responses cannot be directly used in cryptographic applications. Thus error correction processing is required in order to generate a reliable and stable PUF response. Also, the PUF's behaviour depends on environmental conditions like voltage supply, ambient temperature and ageing effects. All of these circumstances need to be taken into account when creating a PUF-based security scheme. Our risk analysis considers in addition to the error correction methods the whole operational life cycle of PUF-based security modules. We analysed different use cases and the related communication protocols. Considering the pre-operational phase (manufacturing, delivery, ...) as well as the usage of the token in the field we identified several threats and vulnerabilities due to either active attacks or the noisy, unstable behaviour of a PUF instantiation. The outcome of the analysis provided valuable input for defining requirements on the error correction mechanisms as well as requirements on the environment to ensure a reliable and secure usage of PUF-based devices. Furthermore the results formed the basis for the preparation of a Protection Profile for PUFs according to Common Criteria (CC) [1] that was presented at the IFIP SEC 2014 in Marrakech, Morocco [9].

2 Physically Unclonable Functions

A Physically Unclonable Function (PUF), i.e. a function embodied in a physical structure, contains random and unique information which originates from uncontrollable process variations during manufacturing in integrated circuits (IC). The basic idea is to use this "fingerprint" to serve as security anchor in various applications. The usage of PUFs enables the design of cryptographic applications without storing sensitive information such as keys in memory at all. For practical usability, PUFs should be easy to evaluate whereas they are considered unclonable because it is extremely difficult to make either a hardware clone, a mathematical model of the behaviour of the structure, or a software program that can compute the response to a challenge in a reasonable amount of time [4]. In [10] Maes and Verbauwhede present an extensive overview of PUFs and PUF-like proposals. One established technique are SRAM PUFs that make use of the fact that SRAM cells tend to have the same state after power up very consistently. Thus, a challenge consists of an address range and the response is the value of the respective SRAM cells after power up. Owing to time, temperature and voltage variations, some bits tend to flip [6]. Therefore so called fuzzy extractors are put in place, which take care that existing bit flips are corrected (e.g. by means of error correction codes). The basic principle of the so-called Arbiter PUFs [3] is to conduct a race on two paths on a chip. Therefore the challenges consist of a vector shaping the path of the "race" and an Arbiter circuit then decides, which path "won" the race, resulting in one bit response (0 or 1). Beside the noisy characteristic of PUFs, also ageing effects have to be taken into account, when developing PUF-based solutions. It is known that the response behaviour of a PUF instantiation is likely to slightly alter in the course of its lifespan. Therefore the noise levels would increase over time in the absence of anti-ageing protocols.

3 Risk Analysis

Performing the comprehensive risk analysis first different use cases were defined that cover a broad field of applications. Based on these use cases we identified several threats which were assessed in a further step. In doing so threats were not only considered as a malicious activity of an attacker. Even the PUF itself, because of its physical properties and noisy behaviour, might act in an undesired manner and therefore cause damage. The risk of the identified threats was calculated by the parameters "Risk Exposure" and "Impact". The ranges of these parameters were adapted to the specific terms of PUFs.

Use Cases. In the risk analysis we evaluated five different use cases. *One-Way Authentication* describes a very simple use case. PUF responses are used to authenticate the PUF-based token, but in this communication protocol no cryptographic actions are foreseen. Thus, a PUF-based token is accepted when the generated response is close enough to the reference response. As compared to *Mutual Authentication* [7], both entities in a protocol are authenticated using

cryptographic algorithms to reliably generate and reconstruct unique responses. Use case *Secret Key Generation and Session Key Exchange* applies PUF responses as a key to encrypt the session key used for further communication. Both use cases *Key Zeroization* and *Hardware/Software Binding* are based on the usage of logically reconfigurable PUFs (LR-PUFs), i.e. the behaviour of a PUF instantiation can be changed by adding some state information [2, 8].

Results of Risk Analysis. The results of the performed risk analysis and the assessment of threats and vulnerabilities were prioritised with respect to the calculated risk value in order to highlight the most important ones. The analysis showed that the usage of a weak fuzzy extractor and/or weak error correction as well as PUF failures cause the highest risks. This means that the fuzzy extractor as well as the error correction must not reveal any information regarding the PUF-individual response because helper data, generated by the fuzzy extractor, are public information. At the same time these methods have to ensure the reliable reconstruction of secrets/keys from an error-prone response even in case of ageing and variation of environmental conditions. Another security relevant function is the manipulation of state information used for LR-PUFs. State information is public too and it must not be changed by unauthorized entities. Some further risks concern the PUF's environment that cannot be treated by the PUF itself. Therefore requirements and assumptions on the (pre-)operational environment have to be defined considering the underlying PUF technology as well as the intended use case. For example each PUF-based token has to be enrolled with different, unpredictable and random challenges in order to prevent guessing of valid challenges. Further the exchange of the database (comprising challenge-response pairs) between the enrolment facility and the customer has to be performed in a secure way in order to ensure confidentiality and integrity. Also, the analysis showed that model building attacks strongly depend on the PUF type and thus must be discussed separately. Literature already provides numerous papers [5, 11–13] that might be considered.

4 Conclusion and Outlook

The results of the risk analysis formed the basis for the preparation of the security problem definition (SPD) and the security solution definition (SSD) in our Protection Profile for PUFs. These parts include potential threats, assumptions that are made on the TOE's environment as well as organizational security policies (OSPs). In order to achieve the security objectives several security functional requirements were derived including some extended components considering PUF specific needs. In the ongoing project the defined requirements are implemented in a prototype comprising PUFs and realizing mutual authentication and key generation. As a next step the prototype will be evaluated against these requirements in order to prove that the identified threats are countered and the security objectives are achieved.

Acknowledgements. This work is co-financed by the Austrian Research Promotion Agency (FFG) in the FIT-IT line within the project CODES (835932): Algorithmic extraction and error correction codes for lightweight security anchors with reconfigurable PUFs. The project partners are Technikon Forschungs- und Planungsgesellschaft mbH, Alpen-Adria Universität Klagenfurt and University of Applied Sciences Upper Austria - Campus Hagenberg.

References

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model. CCMB-2012-09-001, Version 3.1, Revision 4 (2012)
2. Eichhorn, I., Koeberl, P., van der Leest, V.: Logically reconfigurable PUFs: memory-based secure key storage. In Proceedings of the sixth ACM workshop on Scalable trusted computing, STC '11, 59-64, New York, USA (2011)
3. Fruhashi, K., Shiozaki M., Fukushima A., Murayama T., Fujino T.: The arbiter-PUF with high uniqueness utilizing novel arbiter circuit with Delay-Time Measurement. IEEE International Symposium on Circuits and Systems (ISCAS), 2325–2328 (2011)
4. Gassend, B., Clarke, D., van Dijk, M., Devadas, S.: Controlled Physical Random Functions, In IEEE, editor, Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC02), USA (2002)
5. Gassend, B., Lim, D., Clarke, D., van Dijk, M., Devadas, S.: Identification and authentication of integrated circuits. Concurrency and Computation: Practice and Experience, 16(11):10771098 (2004)
6. Handschuh, H.: Hardware-Anchored Security Based on SRAM PUFs, Part 1. Security Privacy, IEEE, 10(3):80–83 (2012)
7. Herrewege, A., Katzenbeisser, S., Maes, R., Peeters, R., Sadeghi, A.-R., Verbauwhede, I., Wachsmann, Ch.: Reverse Fuzzy Extractors: Enabling Lightweight Mutual Authentication for PUF-Enabled RFIDs. In AngelosD. Keromytis, editor, Financial Cryptography and Data Security. LNCS, vol. 7397, 374–389. Springer, Heidelberg (2012)
8. Katzenbeisser, S., Kocabas, U., van der Leest, V., Sadeghi, A.-R., Schrijen, G.-J., Schröder, H., Wachsmann, Ch.: Recycable PUFs: Logically Reconfigurable PUFs. (2007)
9. Kolberger, A., Schaumüller-Bichl, I., Brunner, V., Deutschmann, M.: Protection Profile for PUF-based Devices. In Proceedings of the 29th IFIP TC 11 International Conference on ICT Systems Security and Privacy Protection, IFIP SEC 2014, 91–98. Springer, Heidelberg (2014)
10. Maes, R., Verbauwhede, I.: Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. In Ahmad-Reza Sadeghi and David Naccache, editors, Towards Hardware-Intrinsic Security, Information Security and Cryptography, 3–37. Springer, Heidelberg (2010)
11. Majzoobi, M., Koushanfar, F., Potkonjak, M.: Testing Techniques for Hardware Security. In IEEE International Test Conference, ITC 2008, 1-10 (2008)
12. Rührmair, U., Sehnke, F., Sölter, J., Dror, G., Devadas, S., Schmidhuber, J.: Modeling attacks on physical unclonable functions. In Proceedings of the 17th ACM conference on Computer and communications security, CCS '10, 237-249, New York, NY, USA (2010)
13. Sölter, J.: Cryptanalysis of Electrical PUFs via Machine Learning Algorithms. Master's thesis, Technische Universität München (2009)