Advanced Reconfigurable Physical Unclonable Functions (AR-PUFs) and Their Security Applications

Manish Kumar[†], Nikolaos Athanasios Anagnostopoulos[†], Yufan Fan[*] & Stefan Katzenbeisser[†]

[†] Computer Science Department, Technische Universität Darmstadt, Hessen, Germany
[*] Department of Electrical Engineering and Information Technology, Technical University of Darmstadt, Hessen, Germany

Physical Unclonable Functions (PUFs) are novel lightweight security primitives that can potentially provide a high level of security with low power and area overhead, in comparison to other security solutions. A PUF provides a digital fingerprint which can be used as a unique identity for a particular device. PUFs can be utilized for cryptographic key generation and agreement [SD07], as well as identification and authentication. Therefore, they are increasingly used as a means of protection against identity theft, device cloning, and counterfeiting of merchandise.

However, recent publications regarding attacks against them have shed doubt on their potential as security mechanisms. Multiple vulnerabilities have been identified that can be exploited to attack computer systems that base their security on PUFs. A number of attacks based on these vulnerabilities, such as model building, machine learning, fault injection, physical and other known attacks, have been proposed in the relevant literature. Additionally, avoiding or detecting these attacks has become a challenging task in modern cryptographic research. Therefore, the role of PUFs as security mechanisms is currently under question.

In order to address the shortcomings of present PUF implementations, we investigate ways of increasing their entropy and, therefore, potentially enhance their security. Our research focuses on novel security solutions, which are based on the concept of Reconfigurable PUFs (R-PUFs) [EKvdL11, KKvdL$^+$11, KSS$^+$09], including Controlled PUFs [GCvDD02, GDC$^+$08], and on their applications. A PUF can be combined with another source of entropy, in order to increase its entropy and transform it into a reconfigurable security mechanism, whose output is not only dependent on the PUF itself, but also on the other source of entropy. By increasing the entropy of the final output of this composite security mechanism, the probability of a successful attack against it can be significantly reduced.

In particular, we examine and evaluate a number of different composite R-PUF implementations that appear to be promising regarding their security. A number of different components, such as non-volatile memory, hash functions, such data structures as trees, or, even, other PUFs can be used as sources of additional entropy, which can be combined with a PUF in order to (re)configure it. Additionally, such R-PUFs can potentially also allow for secure reconfiguration, by partial renewal of their components through the help of a semi-trusted party. Finally, by keeping a history of the inputs, such an R-PUF can also allow for both tamper evidence and restoration back to a legitimate state. We, therefore, come up with a family of novel R-PUFs that can offer advanced security applications, which we name *Advanced Reconfigurable PUFs* (AR-PUFs).

References

[EKvdL11] I. Eichhorn, P. Koeberl, and V. van der Leest. Logically reconfigurable PUFs: Memory-based secure key storage. In *Proceedings of the Sixth ACM Workshop on Scalable Trusted Computing*, STC '11, pages 59–64, New York, NY, USA, 2011. ACM.

[GCvDD02] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. Controlled physical random functions. In *Proceedings of the 18th Annual Computer Security Applications Conference*, ACSAC '02, pages 149–, Washington, DC, USA, 2002. IEEE Computer Society.

[GDC$^+$08] B. Gassend, M. V. Dijk, D. Clarke, E. Torlak, S. Devadas, and P. Tuyls. Controlled physical random functions and applications. *ACM Trans. Inf. Syst. Secur.*, 10(4):3:1–3:22, January 2008.

[KKvdL$^+$11] S. Katzenbeisser, Ü. Kocabaş, V. van der Leest, A.-R. Sadeghi, G.-J. Schrijen, and C. Wachsmann. Recyclable PUFs: Logically reconfigurable pufs. *Journal of Cryptographic Engineering*, 1(3):177, Sep 2011.

[KSS$^+$09] K. Kursawe, A. R. Sadeghi, D. Schellekens, B. Skoric, and P. Tuyls. Reconfigurable physical unclonable functions - Enabling technology for tamper-resistant storage. In *2009 IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 22–29, July 2009.

[SD07] G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *2007 44th ACM/IEEE Design Automation Conference*, pages 9–14, June 2007.

crypto day matters 28 (2018)
Beiträge vom 28. Kryptotag, 07.-08.06.2018, Kirchheim.
doi:10.18420/cdm-2018-28-22