XOR Arbiter PUFs: an Empirical Approach to Input Transformations

Nils Wisiol
Freie Universität Berlin

30th Crypto Day, 28/29 March 2019

Physically Unclonable Functions (PUFs) are identical-design integrated circuits that behave differently on different chips due to manufacturing imperfections. This device-specific behavior has been extensively studied and can be used as an authentication mechanism for embedded systems and other cryptographic applications (Gassend, Lim, Clarke, Dijk & Devadas (2004); Rührmair, Busch & Katzenbeisser (2010a); Armknecht, Maes, Sadeghi, Sunar & Tuyls (2010)).

One of the biggest challenges to PUFs is their vulnerability to machine learning attacks, where an attacker builds a prediction model based on collected examples of one PUF's behavior. Although some XOR Arbiter PUFs have been shown to be vulnerable to this kind of attack (Rührmair, Sehnke, Sölter, Dror, Devadas & Schmidhuber (2010b)), it remains unknown if the design can be improved to make such attacks harder or impossible.

One option to augment the design of XOR Arbiter PUFs is to modify the given challenge before it is fed into the individual arbiter chains of the XOR Arbiter PUF, a method that I call *input transformation.* PUF literature already contains some input transformations, most notably the Lightweight Secure XOR Arbiter PUF (Majzoobi, Koushanfar & Potkonjak (2008)).

In this talk, I show results of a novel attack on the Lightweight Secure input transformation and propose a new input transformation design. The presentation will also introduce pypuf, my most important tool for studying input transformations.

References

Frederik Armknecht, Roel Maes, Ahmad-Reza Sadeghi, Berk Sunar & Pim Tuyls (2010). Memory leakage-resilient encryption based on physically unclonable functions. In *Towards Hardware-Intrinsic Security*, 135–164. Springer.

Blaise Gassend, Daihyun Lim, Dwaine Clarke, Marten van Dijk & Srinivas Devadas (2004). Identification and authentication of integrated circuits. *Concurrency and Computation: Practice and Experience* **16**(11), 1077–1098. ISSN 1532-0634. URL `https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.805`.

crypto day matters 30 (2019)
Beiträge vom 30. Kryptotag, 28.-29.03.2019, Mozilla, Berlin.
doi:10.18420/cdm-2019-30-07

MEHRDAD MAJZOOBI, FARINAZ KOUSHANFAR & MIODRAG POTKONJAK (2008). Lightweight Secure PUFs. In *Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design*, ICCAD '08, 670–673. IEEE Press, Piscataway, NJ, USA. ISBN 978-1-4244-2820-5. URL http://dl.acm.org/citation.cfm?id=1509456.1509603.

ULRICH RÜHRMAIR, HEIKE BUSCH & STEFAN KATZENBEISSER (2010a). Strong PUFs: Models, Constructions, and Security Proofs. In *Towards Hardware-Intrinsic Security: Foundations and Practice*, AHMAD-REZA SADEGHI & DAVID NACCACHE, editors, Information Security and Cryptography, 79–96. Springer Berlin Heidelberg, Berlin, Heidelberg.

ULRICH RÜHRMAIR, FRANK SEHNKE, JAN SÖLTER, GIDEON DROR, SRINIVAS DEVADAS & JÜRGEN SCHMIDHUBER (2010b). Modeling Attacks on Physical Unclonable Functions. In *Proceedings of the 17th ACM Conference on Computer and Communications Security*, CCS '10, 237–249. ACM, New York, NY, USA. ISBN 978-1-4503-0245-6. URL http://doi.acm.org/10.1145/1866307.1866335.