Towards Secure Strong PUFs

Nils Wisiol
Chair for Security in Telecommunications,
Technische Universität Berlin, Germany

31th Crypto Day, 17/18 October 2019

Pioneered by Pappu *et al.* (2002), Physically Unclonable Functions (PUFs) have been studied in the last two decades as a possible replacement for secure memory of cryptographic keys. Gassend *et al.* (2004) were the first to electrically implemented a PUF, using integrated circuits (IC) with behavior depending on manufacturing imperfections. As a consequence, the ICs behavior, usually defined as the response to a given challenge, will be different on each chip, providing unclonability. PUFs that have (in their security parameter) an exponentially large challenge space are called strong PUFs. As first shown by Brzuska *et al.* (2011), Strong PUFs have the potential to serve as cryptographic primitive in many cryptographic applications, ranging from basic unidirectional authentication to oblivious transfer and bit commitment schemes (but see Badrinarayanan *et al.* (2017)). However, the design and implementation of strong PUFs is still an active area of research where often, designs are broken (see Rührmair *et al.* (2013); Wisiol *et al.* (2019)), revised (see Majzoobi *et al.* (2008); Herder *et al.* (2017)), and broken again.

Our contribution will give an overview over the past two decades in strong PUF research, cover important design and attack strategies, discuss difficulties, and historically motivate the current state of the art in strong PUF research and discuss the most recent design proposal of the Interpose PUF by Nguyen *et al.* (2018). We present an analysis of the Interpose PUF design, an approximation method and an attack that can break the design when parameters allow an approximation. Finally, we compare our results with other recently claimed attacks on the Interpose PUF by Santikellur *et al.* (2019).

References

Saikrishna Badrinarayanan, Dakshita Khurana, Rafail Ostrovsky & Ivan Visconti (2017). Unconditional UC-Secure Computation with (Stronger-Malicious) PUFs. In *Advances in Cryptology – EUROCRYPT 2017*, Jean-Sébastien Coron & Jesper Buus Nielsen, editors, volume 10210, 382–411. Springer International Publishing, Cham. ISBN 978-3-319-56619-1 978-3-319-56620-7. URL http://link.springer.com/10.1007/978-3-319-56620-7_14.

Christina Brzuska, Marc Fischlin, Heike Schröder & Stefan Katzenbeisser (2011). Physically Uncloneable Functions in the Universal Composition Framework. In *Advances in Cryptology – CRYPTO 2011*, David

crypto day matters 31 (2019)
Beiträge vom 31. Kryptotag, 17.-18.10.2019, Qualcomm, Berlin.
doi:10.18420/cdm-2019-31-05

Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell, Moni Naor, Oscar Nierstrasz, C. Pandu Rangan, Bernhard Steffen, Madhu Sudan, Demetri Terzopoulos, Doug Tygar, Moshe Y. Vardi, Gerhard Weikum & Phillip Rogaway, editors, volume 6841, 51–70. Springer Berlin Heidelberg, Berlin, Heidelberg. ISBN 978-3-642-22791-2 978-3-642-22792-9. URL http://link.springer.com/10.1007/978-3-642-22792-9_4.

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.

C. Herder, L. Ren, M. van Dijk, M. Yu & S. Devadas (2017). Trapdoor Computational Fuzzy Extractors and Stateless Cryptographically-Secure Physical Unclonable Functions. *IEEE Transactions on Dependable and Secure Computing* **14**(1), 65–82. ISSN 1545-5971.

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.

Phuong Ha Nguyen, Durga Prasad Sahoo, Chenglu Jin, Kaleel Mahmood & Ulrich Rührmair (2018). The Interpose PUF: Secure PUF Design against State-of-the-Art Machine Learning Attacks 48.

Ravikanth Pappu, Ben Recht, Jason Taylor & Neil Gershenfeld (2002). Physical One-Way Functions. *Science* **297**(5589), 2026–2030. ISSN 0036-8075, 1095-9203. URL http://science.sciencemag.org/content/297/5589/2026.

Ulrich Rührmair, Jan Sölter, Frank Sehnke, Xiaolin Xu, Ahmed Mahmoud, Vera Stoyanova, Gideon Dror, Jürgen Schmidhuber, Wayne Burleson & Srinivas Devadas (2013). PUF Modeling Attacks on Simulated and Silicon Data. *IEEE Transactions on Information Forensics and Security* **8**(11), 1876–1891.

Pranesh Santikellur, Aritra Bhattacharyay & Rajat Subhra Chakraborty (2019). Deep Learning Based Model Building Attacks on Arbiter PUF Compositions 10.

Nils Wisiol, Georg T Becker, Marian Margraf, Tudor A A Soroceanu, Johannes Tobisch & Benjamin Zengin (2019). Breaking the Lightweight Secure PUF: Understanding the Relation of Input Transformations and Machine Learning Resistance 9. Https://eprint.iacr.org/2019/799.