Special Session: How Secure Are PUFs Really? On the Reach and Limits of Recent PUF Attacks

Ulrich Rührmair
Technische Universität München
80333 München, Germany
E-mail: ruehrmair@ilo.de

Ulf Schlichtmann
Technische Universität München
80333 München, Germany
E-mail: ulf.schlichtmann@tum.de

Wayne Burleson
University of Massachusetts Amherst
Amherst, MA 01003, USA
E-mail: burleson@ecs.umass.edu

***Abstract*—Just over a decade ago, Physical Unclonable Functions (PUFs) have been introduced as a new cryptographic and security primitive in a number of seminal publications. Due to their assumed security and cost advantages, they have attracted substantial attention both from the security industry and the academic community, and are also gaining ground in commercial applications. Nevertheless, a number of recent works have presented successful attacks on PUF core properties, such as their digital and physical unclonability. How strong and relevant are these attacks, and how secure are PUFs really? This question is addressed in a dedicated hot topic session at DATE 2014. This paper provides a short and easily accessible overview of the session.**

***Index Terms*—Physical Unclonable Functions (PUFs), Weak PUFs, Strong PUFs, Security, Modeling Attacks, Invasive Attacks, Side Channel Attacks, Protocol Attacks**

I. Motivation and Overview

Embedded security plays an increasing role in overall lightweight systems design. Slightly over a decade ago, physical unclonable functions (PUFs) have been introduced in two seminal works by Pappu et al. in SCIENCE magazine 2002 [13] and by Gassend et al. at CCS 2002 [3]. Since then, the field has undergone an explosive development, with interdisciplinary contributions from EDA, VLSI, cryptanalysis, and embedded security. This progress was mainly driven by the promised security advantages of PUFs in comparison with classical techniques: Their assumed natural resilience against side channel and invasive attacks; their presumed digital and physical unclonability; and, most recently, their purported practical usability in advanced cryptographic protocols such as key exchange and oblivious transfer. In recent years, however, both PUFs and PUF protocols have been the subject of various classes of new attacks, some of which were tailored specifically for this new primitive. Several of these attacks have affected exactly the assumed security upsides that acted as drivers for the field. These attacks include the following:

- Machine-learning based modeling attacks on PUFs have been put forward by a number of researchers, including Majzoobi et al. at ITC 2008 [7] and Rührmair et al. at CCS 2010 [23] and IEEE T-IFS 2013 [25]. If successful, they allow adversaries to build a computer algorithm which can numerically emulate the challenge-response behavior of the PUF – a so called "digital clone" of the PUF. It can be used to break those protocols and applications that rest on the PUF's unpredictability and unclonability.
- At TRUST 2011, Merli et al. [8] carried out a side channel attack on the error correction module for PUF responses, which is an inherent part of several PUF designs. In the same year, EM analyses on PUFs have been carried out by Merli et al. at WESS 2011 [9]. Other side-channel attacks on PUFs are currently under investigation in several groups, including those of some of the proponents.
- At CHES 2012 [19], JCEN 2013 [20], and IEEE S&P 2013 [21], Rührmair and van Dijk reported practical attacks on several existing advanced PUF protocols, including those of Brzuska et al. from CRYPTO 2011 [1], which destroy their security in a large number of realistic use cases.
- Finally, at HOST 2013 and FDTC 2013, Helfmeier et al. [5] and Nedospasov et al. [11] carried out successful physical cloning and invasive attacks on SRAM PUFs. They firstly allow an adversary to read out the PUF responses – e.g., the values present in the SRAM PUFs after the cells have been powered up. Secondly, they enable adversaries to tune these start-up values to any given value, thereby effectively cloning the PUF. These attacks affect exactly the purported security advantages of PUFs: Their digital and physical unclonability; their security against unauthorized read-out; and the practical security of advanced PUF protocols.

This state of the art leaves several open questions, most notably: How secure are PUFs really? Are the recently discovered attacks part of a natural consolidation process, which will eventually lead to more secure, attack-resilient PUF designs? Or do the attacks point to the fact that the original PUF promise is already broken, meaning that this new primitive will be unable to fulfill its pledge in the long term?

These questions are pressing not only from an academic, but also from a practical perspective, since PUFs have witnessed some commercial breakthroughs just recently: For example, they will be part of NXP's top smart card line in the upcoming years [12], and will also be used in products of the Microsemi

978-3-9815370-2-4/DATE14/©2014 EDAA

corporation [10]. These topics are addressed in a dedicated session at DATE 2014, bringing together exactly those scientists who have been active in the abovementioned attacks over the last years. The aim of the presentations and associated papers of this session is to come to a thorough and fair evaluation of recent PUF attacks — on their reach just as well as on their limitations. We want to provide participants from industry and academia with a fair perspective of the field, its current healthiness, and, in particular, of its long-term perspectives.

II. Papers Associated to the Session

The session will comprise six talks. Each talk has one associated paper, which summarizes and extends the material of the talk, providing more details and in-depth discussions. The content of the papers and their function for the session is as follows (speakers of the associated talks have been put in italics):

- *U. Rührmair*, D. Holcomb: PUFs at a Glance [16].
  - The paper introduces PUFs and prepares the stage for the other papers of the session. It provides the necessary terminology, including the distinction between so-called Weak PUFs and Strong PUFs [1]. It also discusses other PUF basics, such as their security features, implementations, applications, and typical attacks.
- *U. Rührmair*, J. Sölter: PUF Modeling Attacks: An Introduction and Overview [24].
  - This paper summarizes and extends the talk on PUF modeling attacks. The latter are numeric cryptanalytic attacks, in which an adversary extrapolates the PUF behavior on all CRPs from a small fraction of CRPs that is known to him. The attacks are mostly applicable for one particular PUF type, so-called Strong PUFs. The paper discusses the latest modeling results from the literature and describes the machine learning algorithms that have been used in the most successful attacks.
- X. Xu, *W. Burleson*: Hybrid Side-Channel / Machine-Learning Attacks on PUFs: A New Threat? [26].
  - The paper describes the first dedicated hardware attacks within the session, namely side channel attacks. While PUFs were originally believed to be mostly side channel resilient, certain specific PUF side channels have emerged in the literature recently. The paper and the associated talk also cover the combination of side channels with other approaches, for example modeling attacks, which poses an additional threat to PUF security. A part of the attacks presented in the paper apply to Weak PUFs (namely the attacks on error correction modules or emanation analysis), another part mainly to Strong PUFs (namely the combined modeling and side channel attacks).
- C. Helfmeier, D. Nedospasov, S. Tajik, C. Boit, *J.-P. Seifert*: Physical Vulnerabilities of Physically Unclonable Functions [6].
  - The paper describes a second type of dedicated hardware attacks on PUFs within our session, namely invasive and PUF cloning attacks. It relates to some of the assumed core properties of PUFs, namely their physical unclonability. The attacks presented in this paper mainly apply to so-called "Weak PUFs", i.e., to SRAM PUFs and similar structures.
- *M. van Dijk*, U. Rührmair: Protocol Attacks on Advanced PUF Protocols and Countermeasures [2].
  - The special security features of Strong PUFs, for example their publicly accessible hardware interface, make them a novel protocol tool, which requires special protocol design. This paper investigates the secure use of Strong PUFs in various protocols, and shows that some proposed schemes are insecure under realistic attack models (the so-called *"bad PUF model"* and the *"PUF re-use model"*). It illustrates how these models work, and how countermeasures to restore security could look like.
- M. Rostami, J.B. Wendt, M. Potkonjak, *F. Koushanfar*: Quo Vadis, PUF? Trends and Challenges of Emerging Physical-Disorder based Security [14].
  - This paper concludes the session. It thereby provides readers with a short summary of the most important results and facts. Its focus lies on describing future directions in PUF research, though, and on highlighting interesting opportunities for the reader's own research, both on the sides of PUF attackers, PUF designers, and PUF users.

III. Conclusions

The session's aim is to provide a fair evaluation of PUF's security and long-term prospectives in the light of recent attacks. Three aspects should be mentioned explicitly.

Firstly, it must be stressed that the recent attacks are serious and pose a non-trivial challenge to the field. Some of them concern PUF core properties, namely their unclonability, or reveal unexpected vulnerabilities, for example in Strong PUF protocols. The attacks do show that security in certain PUF applications cannot be obtained as easily as had been envisaged originally. To name some examples, the use of Strong PUFs in advanced protocols is more intricate than assumed originally. The same holds for the employment of Weak PUFs/SRAM cells as unclonable systems in high end security applications, which is threatened by the recent cloning and invasive attacks. Furthermore, the existence of powerful modeling attacks makes the construction of secure and cost efficient electrical Strong PUFs more difficult than expected;

[1] We emphasize once more, as already done in earlier works, that this terminology is not to be misunderstood in a pejorative or judgemental manner. The terms Weak PUF and Strong PUF had originally been introduced by Guajardo, Kumar, Schrijen, and Tuyls in [4], and have been further developed and refined in [22], [23], [17], [18].

mostly linear structures like the Arbiter PUFs reach their limits quickly. Yet further examples are discussed throughout the session and papers (compare Section II).

At the same time, however, it is essential to also understand the limits of the existing attacks. None of them "kills" the field in its entirety. Most of them in fact create new research opportunities. Just to list the most prominent of them: Which additional features are required of Strong PUFs in order to restore their broad usability in advanced cryptographic protocols? How can these features (for example erasability or certifiability, see [2]) be implemented in hardware efficiently? How can Weak PUFs be made more secure against cloning and invasive attacks? How can they be made tamper sensitive at low costs? How must Strong PUFs be designed in order to be secure against modeling? In this sense, the existing attacks could even be seen positively: As drivers for future research in the field.

In sum, we thus believe that the attacks should be seen in a bigger context, and should be interpreted in a balanced fashion. They are part of a natural consolidation process in the PUF area, similar to the consolidation that classical security primitives have undergone already some time ago. This process indicates that the field is becoming increasingly mature. One typical byproduct is the insight that certain aspects of the area are not as simple as originally believed, which may be disappointing at first sight. Overall, however, a sound consolidation will eventually create more research opportunities than it destroys. It will likely lead to secure PUF constructions and applications in the end, sorting out those approaches that were overstated or misled.

IV. Short Bios of Speakers

Wayne Burleson is a senior fellow with AMD research and a professor at the University of Massachusetts Amherst. He has held visiting professorships at ENST Paris, LIRM Montpellier, and EPFL Switzerland. Wayne has published over 190 refereed publications and is a fellow of IEEE. He was one of the co-proponents of SRAM PUFs, one of the commercially most viable PUF types, in 2007.

Marten van Dijk is an associate professor at the University of Connecticut. He has worked as researcher at Philips Eindhoven, RSA Security, and MIT. Together with Srini Devadas, he is one of the co-founders of the field of PUFs. Recently, Marten has been particularly active on various PUF protocol attacks, e.g. at CHES 2012, JCEN 2013, or IEEE S&P 2013.

Farinaz Koushanfar is an associate professor at Rice University and director of the Adaptive Computing and Embedded Systems (ACES) lab at Rice. Farinaz holds a PhD from the University of California at Berkeley and a Presidential Early Career Award. She has published numerous works on PUFs and anti-counterfeiting techniques, e.g. at DAC, DATE, ICCAD, and IEEE T-IFS.

Ulrich Rührmair holds an MSc from Oxford University. He has founded and headed the physical cryptography project at TU Munich. His recent research has concentrated on PUFs and related concepts, where he has published around 30 papers. A large part of these concerns PUF attacks, including modeling and protocol attacks, e.g. at CHES 2012, JCEN 2013, IEEE S&P 2013, ACM CCS 2010, and IEEE T-IFS 2013.

Jean-Pierre Seifert is professor for security in telecommunications at TU Berlin, and head of the identically-named research laboratory of the Deutsche Telekom. He has been awarded Infineon's Inventor of the Year Award and two Intel Achievement Awards. He is the co-inventor of around 40 patents and co-author of numerous scientific publications. His group presented the first successful physical PUF cloning attacks at HOST 2013 and the first invasive attacks on PUFs at FDTC 2013.

References

[1] C. Brzuska, M. Fischlin, H. Schröder, S. Katzenbeisser: *Physically Unclonable Functions in the Universal Composition Framework*. Advances in Cryptology (CRYPTO'11), 2011.

[2] M. van Dijk, U. Rührmair: *Protocol Attacks on Advanced PUF Protocols and Countermeasures*. Design, Automation and Test in Europe (DATE'14), 2014.

[3] B. Gassend, D. Clarke, M. van Dijk, S. Devadas: *Silicon physical random functions*. 9th ACM conference on Computer and communications security (CCS'02), 2002.

[4] Jorge Guajardo, Sandeep S. Kumar, Geert Jan Schrijen, Pim Tuyls: *FPGA Intrinsic PUFs and Their Use for IP Protection*. CHES 2007: 63-80

[5] C. Helfmeier, D. Nedospasov, C. Boit, J.P. Seifert: *Cloning Physically Unclonable Functions*. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'13), 2013.

[6] C. Helfmeier, D. Nedospasov, S. Tajik, C. Boit, J.-P. Seifert: *Physical Vulnerabilities of Physically Unclonable Functions.* Design, Automation and Test in Europe (DATE'14), 2014.

[7] M. Majzoobi, F. Koushanfar, M. Potkonjak: *Testing Techniques for Hardware Security*. IEEE International Test Conference (ITC'08), 2008.

[8] D. Merli, D. Schuster, F. Stumpf, G. Sigl: *Side-channel analysis of PUFs and fuzzy extractors*. Int. Conference on Trust and Trustworthy Computing (TRUST'11), 2011.

[9] D. Merli, D. Schuster, F. Stumpf, G. Sigl: *Semi-invasive EM attack on FPGA RO PUFs and countermeasures*. ACM Workshop on Embedded Systems Security (WESS'11), 2011.

[10] http://investor.microsemi.com/releasedetail.cfm?releaseid=596301

[11] D. Nedospasov, C. Helfmeier, J.P. Seifert, C. Boit: *Invasive PUF Analysis*. Fault Diagnonsis and Tolerance in Cryptography (FDTC'13), 2013.

[12] NXP Semiconductors, http://www.nxp.com/news/press-releases/2013/02/nxp-strengthens-smartmx2-security-chips-with-puf-anti-cloning-technology.html

[13] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld: *Physical one-way functions*. Science, 2002.

[14] M. Rostami, J.B. Wendt, M. Potkonjak, F. Koushanfar: *Quo Vadis, PUF? Trends and Challenges of Emerging Physical-Disorder based Security*. Design, Automation and Test in Europe (DATE'14), 2014.

[15] U. Rührmair: *Oblivious Transfer based on Physical Unclonable Functions*. International Conference on Trust and Trustworthy Computing (TRUST'10), 2010.

[16] U. Rührmair, D. Holcomb: *PUFs at a Glance*. Design, Automation and Test in Europe (DATE'14), 2014.

[17] U. Rührmair, H. Busch, S. Katzenbeisser: Strong PUFs: Models, Constructions and Security Proofs. In A.-R. Sadeghi, P. Tuyls (Editors): *Towards Hardware Intrinsic Security: Foundation and Practice.* Springer, 2010.

[18] U. Rührmair, S. Devadas, F. Koushanfar: *Security based on Physical Unclonability and Disorder*. In M. Tehranipoor and C. Wang (Editors): Introduction to Hardware Security and Trust. Springer, 2011.
[19] U. Rührmair, M. van Dijk: *Practical Security Analysis of PUF-based Two-Player Protocols*. CHES 2012.
[20] U. Rührmair, M. van Dijk: *On the Practical Use of Physical Unclonable Functions in Oblivious Transfer and Bit Commitment Protocols*. Journal of Cryptographic Engineering (JCEN), 2013.
[21] U. Rührmair, M. van Dijk: *PUFs in Security Protocols: Attack Models and Security Evaluations*. IEEE Symposium on Security and Privacy (IEEE S&P '13), 2013.
[22] U. Rührmair, J. Sölter, F. Sehnke. *On the Foundations of Physical Unclonable Functions*. Cryptology ePrint Archive, Report 2009/277, 2009.
[23] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, J. Schmidhuber: *Modeling Attacks on Physical Unclonable Functions*. ACM Conference on Computer and Communications Security (CCS'10), 2010.
[24] U. Rührmair, J. Sölter: *PUF Modeling Attacks: An Introduction and Overview*. Design, Automation and Test in Europe (DATE'14), 2014.
[25] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, S. Devadas: *PUF Modeling Attacks on Simulated and Silicon Data*. IEEE Transactions on Information Forensics and Security (IEEE T-IFS), 2013.
[26] X. Xu, W. Burleson: *Hybrid Side-Channel / Machine- Learning Attacks on PUFs: A New Threat?* Design, Automation and Test in Europe (DATE'14), 2014.