Addressing the Effects of Temperature Variations on Intrinsic Memory-Based Physical Unclonable Functions

Nikolaos Athanasios Anagnostopoulos[1], Tolga Arul[1], Yufan Fan[2], Christian Hatzfeld[2], Fatemeh Tehranipoor[3] and Stefan Katzenbeisser[1]

[1] Computer Science Department, Technical University of Darmstadt, Germany
[2] Department of Electrical Engineering and Information Technology, Technical University of Darmstadt, Germany
[3] School of Engineering, San Francisco State University, United States of America

Physical Unclonable Functions (PUFs) ideally act as functions encoded in hardware, which produce a unique output, being referred to as a response, for a specific input, being called a challenge. PUFs are often implemented using inherent components of a system, such as memory modules, in order to be practical and cost-efficient. Such PUFs are called intrinsic, as they do not require the addition of hardware for their construction and operation. Intrinsic PUFs can be used in low-end resource-constrained devices in order to implement flexible and low-weight cryptographic protocols. Well-known examples of memory-based intrinsic PUFs include SRAM-based and DRAM-based PUFs.

However, recent publications have revealed that temperature can have a dramatic effect on the performance of such intrinsic memory-based PUFs. Low temperatures can lead to data remanence in both DRAM and SRAM modules [HSH+09, AAF+18], significantly affecting their ability to serve as PUFs [AKR+16]. Additionally, high temperatures can speed up the aging of such modules and, therefore, potentially also affect their performance [TKYC17]. Finally, a number of recent works [SXA+17, SXA+18, AKCT18, KPHM18, AAF+18] have proven that DRAM retention-based PUFs, which can be accessed at runtime and provide multiple challenge-response pairs, are significantly affected by common temperature variations, such as those normally occuring through a day.

Our work addresses these issues through the usage of temperature sensors, which are inherent in most contemporary DRAM modules. We combine temperature readings obtained from such a sensor with the responses of the relevant PUF, in order to establish an authentication protocol that can be used at different temperatures, even if the PUF is highly dependent on temperature. Additionally, our protocol also disallows access to the PUF response, if the relevant temperature readings indicate that the performance of the PUF operation may have been afflicted by temperature-related effects, such as data remanence.

References

[AAF+18] N. A. Anagnostopoulos, T. Arul, Y. Fan, C. Hatzfeld, A. Schaller, W. Xiong, M. Jain, M. U. Saleem, J. Lotichius, S. Gabmeyer, J. Szefer, and S. Katzenbeisser. Intrinsic run-time row hammer PUFs: Leveraging the row hammer effect for run-time cryptography and improved security. *Preprints*, Apr 2018.

[AKCT18] N. A. Anagnostopoulos, S. Katzenbeisser, J. Chandy, and F. Tehranipoor. An overview of DRAM-based security primitives. *Cryptography*, 2(2), 2018.

[AKR+16] N. A. Anagnostopoulos, S. Katzenbeisser, M. Rosenstihl, A. Schaller, S. Gabmeyer, and T. Arul. Low-temperature data remanence attacks against intrinsic SRAM PUFs. Cryptology ePrint Archive, Report 2016/769, 2016. `https://eprint.iacr.org/2016/769`.

[HSH+09] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten. Lest we remember: Cold-boot attacks on encryption keys. *Commun. ACM*, 52(5):91–98, May 2009.

[KPHM18] J. S. Kim, M. Patel, H. Hassan, and O. Mutlu. The DRAM latency PUF: Quickly evaluating physical unclonable functions by exploiting the latency-reliability tradeoff in modern commodity dram devices. In *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)*, pages 194–207, Feb 2018.

[SXA+17] A. Schaller, W. Xiong, N. A. Anagnostopoulos, M. U. Saleem, S. Gabmeyer, S. Katzenbeisser, and J. Szefer. Intrinsic rowhammer PUFs: Leveraging the rowhammer effect for improved security. In *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 2017.

[SXA+18] A. Schaller, W. Xiong, N. A. Anagnostopoulos, M. U. Saleem, S. Gabmeyer, B. Skoric, S. Katzenbeisser, and J. Szefer. Decay-based DRAM PUFs in commodity devices. *IEEE Transactions on Dependable and Secure Computing*, 2018.

[TKYC17] F. Tehranipoor, N. Karimian, W. Yan, and J. A. Chandy. Dram-based intrinsic physically unclonable functions for system-level security and authentication. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 25(3):1085–1097, March 2017.

crypto day matters 28 (2018)
Beiträge vom 28. Kryptotag, 07.-08.06.2018, Kirchheim.
doi:10.18420/cdm-2018-28-23