Associate Professorship of Coding and Cryptography
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Seminar

Authentification based on DRAM PUFs

Physically Unclonable Functions (PUFs) are proved to be an effective and low-cost measure against counterfeiting by probiding device authentication and secure key storage services. PUFs based on Dynamic Random Access Memory (DRAM) are particularly advantageous due to their large address space and multiple controllable parameters during respnse generations [1].

The security of an authentification protocol based on PUF devices comes from the intrisinc uniqueness of PUF devices.

Several works (e.g. [2,3]) have been done in characterising DRAM PUFs and designing the authentification protocol for decay-based DRAM PUFs.

This task is to do further literature research on the characterization and cryptographic applications of DRAM PUFs.

References:

[1] Sutar, S., Raha, A., Kulkarni, D., Shorey, R., Tew, J., and Raghunathan, V. (2017). D-PUF: An intrinsically reconfigurable DRAM PUF for device authentication and random number generation. ACM Transactions on Embedded Computing Systems (TECS), 17(1), 1-31.

[2] Xiong, W., Schaller, A., Anagnostopoulos, N. A., Saleem, M. U., Gabmeyer, S., Katzenbeisser, S., and Szefer, J. (2016, August). Run-time accessible DRAM PUFs in commodity devices. In International Conference on Cryptographic Hardware and Embedded Systems (pp. 432-453). Springer, Berlin, Heidelberg.

[3] Schaller, A., Xiong, W., Anagnostopoulos, N. A., Saleem, M. U., Gabmeyer, S., Škorić, B., Katzenbeisser, S. and Szefer, J. (2018). Decay-based DRAM PUFs in commodity devices. IEEE Transactions on Dependable and Secure Computing, 16(3), 462-475.

Prerequisites

Information theory

Digital Circuit

Channel Coding

Contact

lia.liu@tum.de

Advisors

Hedongliang Liu