DRAM-Based Physically Unclonable Functions and the Need for Proper Evaluation

Pascal Ahr, Christoph Lipps and Hans Dieter Schotten
German Research Center for Artificial Intelligence, Kaiserslautern, Germany
Pascal.Ahr@dfki.de
Christoph.Lipps@dfki.de
Hans_Dieter.Schotten@dfki.de

Abstract: Dynamic Random-Access Memory (DRAM)-based Physically Unclonable Functions (PUFs) are a part of the Physical Layer Security (PhySec) domain. Those electrical PUFs are memory based and exhibit a high availability, Shannon Entropy, low energy consumption and high amount of Challenge Response Pairs (CRPs). Because of those properties, the DRAM PUF is a promising approach for security applications in the Industrial Internet of Things (IIoT) context as well as securing the Sixth-Generation (6G) Wireless Systems and edge computing. DRAM, with its most common one-Transistor one-Capacitor (1T1C) architecture, and as a volatile memory is embedded in almost every modern computing unit. Regarding the PUF security applications, four main types of applications are currently distinguished in the scientific community: *Retention Error*, *Row Hammer*, *Startup* and *Latency* PUFs. Thereby these differ in their procedure in how responses are generated as well as by the physical mechanisms. Each of them with varying properties in terms of availability, reliability, uniqueness and uniformity. To examine this, and to obtain comparable results, this work proposes to compare the four different DRAM-PUF types i) with the same metrics of evaluation and ii) implemented on the same DRAM cells. This represents both the difference with regard to the work done in the literature and the added value of this work presented. As far as known, there is no work to date that performs the intended evaluations using the same evaluation platform under the identical conditions. However, this is required for comparable results. This consistent comparison is ensured by a self-developed and implemented evaluation platform, which is accordingly equipped with a significant number of DRAMs. By an appropriate high volume of measurements, a corresponding resolution will be given. Monitoring the environmental conditions prevents from wrong interpretations caused by environmental influences but also provides useful context information. Furthermore, a detailed technical and physical background will be described. The results of this approach will assist by the consideration of which DRAM-PUF is appropriate in which (environmental) conditions and thereby provide a guideline for practitioners.

Keywords: physical layer security, physically unclonable functions, dynamic random-access memory, DRAM PUFs, secure 6G, secure edge computing

1. Physically Unclonable Functions as hardware security anchors

Interconnectivity, as one of the drivers and core technologies of the fourth industrial revolution, overcomes the limitations of local computers. Concepts like the Industrial Internet of Things (IIoT), edge computing and Next Generation Wireless Systems, such as in particular the development of the Sixth-Generation (6G) are leading to a high increase of low complexity and Reduced Capacity (RedCap) devices (Lipps, et al., 2021). The challenge facing the systems, however, is secure communication and the doubtless identification and authentication of the participants. But, according to the computing power, size and energy constrains of IIoT devices, “traditional” cryptographic methods like the Rivest-Shamir-Adleman (RSA) algorithm are not sufficient and therefore new and appropriate approaches are required.

One promising approach are Physically Unclonable Functions (PUFs), a “physical entity whose behaviour is a function of its structure and the intrinsic variation of its manufacturing process“ (Halak, 2018). Due to manufacturing related and uninfluenceable influences are those variations unique for every physical entity and can be considered as a technical fingerprint of the semiconductor device. An additional benefit is their Non-Volatile Memory (NVM): A PUF response can be regenerated the time needed (Lipps, et al., 2018). Furthermore, Random-Access Memory (RAM) is intergraded in almost every computing unit and thus inherently existing in many systems. Now that the Static RAM (SRAM) variant has been discussed in detail in the scientific community, the focus is currently shifting to the Dynamic RAM (DRAM) one (Ahr, Noushinfar & Lipps, 2021). But, although there is work available (Anagnostopoulos, et al., 2018), these merely compare different approaches, whereas the present work calls for a unified and standardized approach.

Therefore, this work in progress paper focusses to close the lack of consistency over the four DRAM PUF types: *Retention Error*, *Row Hammer*, *Startup* and *Latency* PUFs; and to provide a sound comparison. This is structured as follows: Section 2 explains the DRAM and its PUF types while Section 3 describes the test setup. Afterwards in Section 4 metrics to compare the different types are introduced. Finally, Section 5 summarizes the work.

2. Dynamic-RAM based Physically Unclonable Functions

Dynamic Random-Access Memory is a volatile memory with its most common architecture, the one-transistor one-capacitor (1T1C) structure. As depicted in **Figure** 1, the storage capacitor (C_S) is connected to the bitline (BL) via a Metal-Oxide-Semiconductor Field Effect Transistor (MOSFET) (M1) and "stores" the content of the cell. A DRAM is built of many such cells, while a specific word can be accessed via the wordline (WL). This in turn is connected to the gate of the MOSFET (M1). Due to its dimensions, the BL has a capacitance much higher than C_S, which leads to a very small exchange of electrons and therefore a very small change of the bitline voltage V_{BL}, while connected. To "detect" the voltage change, a sense amplifier (SensAmp) is used. These are two cross coupled inverters in a feedback loop and thereby build a bistable system with the two states *logical zero* and *logical one*.

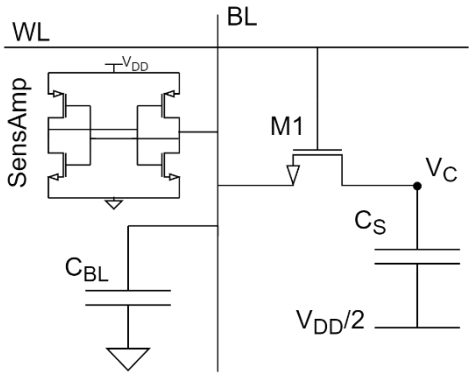

Figure 1: 1T1C DRAM Cell

During a read out process the BL is pre-charged to the tipping point of the SensAmp. Afterwards the C_S is connected and according to its content, the bistable system will adopt one of the two possible states. To reduce the stress caused by the electrical field, one plate of the C_S is biased to $V_{DD}/2$ (Tehranipoor , et al., 2017). But, as the storage capacitor and MOSFET are not ideal they exhibit leakage effects leading to discharging of C_S and therefore to the loss of the stored data. To avoid this, a refreshing of the system is done periodically.

The semiconductors are influenced by manufacturing process fluctuations and can be used to build four different DRAM PUF types: *Retention Error*, *Row Hammer*, *Startup* and *Latency* PUFs.

2.1 Retention Error

The Retention Error PUF uses the leakage effect of the non-ideal components of the DRAM cell. This leakage effect is individual for every cell and influenced by the manufacturing fluctuations. C_S is charged to V_{DD} by writing and reading out after a predefined time while disabling the refreshing mechanism. Either the cell will remain enough electrons to charge the BL over the tipping point of the SensAmp and will read out as logical one or not and will read out as logical zero. This pattern is used to form the PUF response (Keller, et al., 2014).

2.2 Row Hammer

The hammer procedure, a rapidly access to a DRAM row, so called Hammer Rows, causes a quick leakage in cells of adjacent rows, called PUF rows. The quantity of this effect is influenced by manufacturing related fluctuations of the Integrated Circuit (IC). The response is generated by pre-charging C_S, performing the hammer procedure and read the remaining content of the DRAM (Schaller, et al., 2017).

2.3 Latency

A DRAM cell needs some time to store or read data correctly. If this time is violated the operation failed. Manufacturing fluctuations causes an individual time for each cell. The procedure is to write known data in a specific memory region normally and read those with reduced time. Some cells will read correctly while others not. This pattern forms the response of the latency PUF and is possible with reduced write time as well (Hashemian , et al., 2015) (Kim , et al., 2018).

2.4 Startup

After the Startup of a discharged DRAM, all cells are in an undefined state. Due to the pre-charging of one plate of the C_S, point V_C in Figure 1 has got a potential different from GND. By reading out the Sartup state, either point V_C is charged enough to cause the SensAmp to adopt a logical one or not and a logical zero is read (Tehranipoor , et al., 2017).

3. Evaluation platform

To provide the required consistency, all four different DRAM-PUF types shall be integrated successively on the same DRAM modules. Only this enables a DRAM independent proper comparison. In order to consider the environmental conditions as influencing factors in the evaluation, the analysis will be performed in a climatic chamber in which, among other things, the temperature as well as the humidity can be adjusted. The respective conditions are recorded via a corresponding sensor system and taken into account in the evaluation with respect to possible correlations of the PUF responses.

As basis for the evaluation platform a Xilinx EK-U1-ZCU 104G Field Programmable Gate Array (FPGA) development board with a connection from FPGA to embedded DRAM Small Outline Dual Inline Memory Module (SODIMM) is considered. This enables the usage of the Double Data Rate (DDR) interface of the DRAM modules. Besides, by using the interface, it is possible to control the DRAM sufficiently. The read out of the PUF responses will be send from the FPGA board via ethernet or via Peripheral Component Interconnect (PCI) BUS to a conventional computer. This is enabled by an onboard processor and installed LINUX Operating System (OS) and provide a sufficient transfer of the measured data.

4. Metrices

As already mentioned, a uniformity of evaluation is mandatory for an adequate scientific exploitation of the results. This also includes working with appropriately standardized matrices. According to *Basel Halak* the uniqueness, reliability and uniformity are the most important metrics to classify the quality of a PUF (Halak, 2018). The calculations are based on the Hamming Distance (HD) and the Hamming Weight (HW).

In addition, factors and parameters such as the implement-ability in already existing devices, temperature dependency, time to generate PUF response, time when the PUF is available and the correlation with environmental conditions are considered as well.

4.1 Uniqueness

This metric indicates how unique a specific PUF chip is and its distinguishability form other chips. If two chips are completely nonidentical the value is 50%. The uniqueness is calculated by

$$\mathrm{HD}_{\mathrm{inter}} = \frac{2}{k \cdot (k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{\mathrm{HD}\left(R_i(n), R_j(n)\right)}{n} \cdot 100\% \tag{1}$$

With the same challenge and $\mathrm{R_i(n)}$ as the response of chip i and $\mathrm{R_j(n)}$ as the response of chip j out of k chips.

4.2 Reliability

The ability of a PUF to generate a consistent response to a given challenge is given by the Reliability and the best possible value is 100%. The reliability is calculated as follows

$$\mathrm{HD}_{\mathrm{intra}} = \frac{1}{k} \sum_{i=1}^{k} \frac{\mathrm{HD}\left(R_i(n), R_i'(n)\right)}{n} \cdot 100\% \tag{2}$$

$$\mathrm{reliability} = 100\% - \mathrm{HD}_{\mathrm{intra}} \tag{3}$$

With different condition for the same challenge and $R_i'(n)$ as the response of the same chip.

4.3 Uniformity

How unpredictable a specific response of a PUF is, is given by the uniformity, whereby a value of 50% indicates true randomness.

$$\text{Uniformity} = \frac{1}{k}\sum_{i=1}^{k} r_i \cdot 100\% \tag{4}$$

With the same chip and r_i as the HW of the ith out of k PUF responses.

5. Conclusion

Physically Unclonable Functions, especially in their application as arbiter, flip-flop, and SRAM-based approaches are well researched applications. However, there is a growing trend towards DRAM-based approaches as well. Unfortunately, the four common derivatives *Retention Error, Row Hammer, Latency and Startup* have not yet been examined uniformly or have merely been considered separately from one another, leading to not fully comparable results.

This work in progress proposes to examine all methods uniformly on a common evaluation platform using the same metrics. By considering additional information like implement-ability in already existing devices, temperature dependency, time to generate the PUF response, time when the PUF is available and correlation with the environmental conditions, a database is created which allows to select a suitable DRAM for a specific application and thus to give the reader a concrete assistance. The next step will be the implementation of the proposed evaluation platform and the collection of the corresponding data in order to make them available in a clearly structured way.

Acknowledgements

This work has been supported by the Federal Ministry of Education and Research of the Federal Republic of Germany (Förderkennzeichen 16KIS1283, AI-NET PROTECT). The authors alone are responsible for the content of the paper.

References

Ahr, P., Noushinfar, M. & Lipps, C., "RAM-Based PUFs: Comparing Static- and Dynamic Random Access Memory", *Workshop on Next Generation Networks and Application*, Kaiserslautern, Germany, 2021.

Anagnostopoulos, N., Katzenbeisser, S., Chandy, J. & Tehranipoor, F., "An Overview of DRAM-Based Security Primitives", *Cryptography*, DOI:10.3390/cryptography202007, 2018.

Halak, B., "Physically Unclonable Functions - From Basic Design Principles to Advanced Hardware Security Applicaitons", Springer International Publishing, ISBN: 978-3-319-76804-5, 2018.

Hashemian, M.S., Singh, B., Wolff, F., Weyer, D., Clay, S & Papachristou, C., "A Robust Authentication Methodology using Physically Unclonable Functions in DRAM Arrays", *Design, Automation Test in Europe Conference Exhibition (DATE)*, Grenoble, France, DOI: 10.7873/DATE.2015.0308, 2015.

Keller , C., Gurkaynak , F., Kaeslin , H. & Felber, N., "Dynamic memory-based physically unclonable function for the generation of unique identifiers and true random numbers", *IEEE International Symposium on Circuits and Systems (ISCAS)*, Melbourne, VIC, Australia, DOI: 10.1109/ISCAS.2014.6865740, 2014.

Kim , J. S., Patel , M., Hassan , H. & Mutlu, O., "The DRAM Latency PUF: Quickly Evaluating Physical Unclonable Functions by Exploiting the Latency-Reliability Tradeoff in Modern Commodity DRAM Devices", *IEEE International Symposium on High Performance Computer Architecture (HPCA)*, Vienna, Austria, DOI: 10.1109/hpca.2018.00026, 2018.

Lipps, C., Weinand, A., Krummacker, D., Fischer, C. & Schotten, H.D., "Proof of Concept for IoT Device Authentication Based on SRAM PUFs Using ATMEGA 2560-MCU", *1st International Conference on Data Intelligence and Security (ICDIS)*, South Padre Island, TX, USA, DOI: 10.1109/ICDIS.2018.00013, 2018.

Lipps, C., Baradie, S., Noushinfar, M., Herbst, J., Weinand, A. & Schotten, H.D., "Towards the Sixth Generation (6G) Wireless Systems: Thoughts on Physical Layer Security", *Mobile Communication - Technologies and Applications - 25. VDE/ITG Fachtagung Mobilkommunikation*, Osnabrück, Germany, 2021.

Schaller, A., Xiong, W., Anagnostopoulos, N.A., Saleem, M.U., Gabmeyer, S., Katzenbeiser, S. & Szefer, J., "Intrinsic Rowhammer PUFs: Leveraging the Rowhammer effect for improved security", *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, Mclean, VA, USA, DOI: 10.1109/HST.2017.7951729, 2017.

Tehranipoor , F., Karimian , N., Yan , W. & Chandy, J.A., "DRAM-Based Intrinsic Physically Unclonable Functions for System-Level Security and Authentication", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 3, DOI:10.1109/TVLSI.2016.2606658, 2017.