# Comparative Analysis of Latency Based Physically Unclonable Functions

Pratik Baishnav
*Dept. of Computer Science and Mathematics*
*University of Passau*
email address : baishn01@ads.uni-passau.de

***Abstract*—Physical/Physically unclonable functions are digital fingerprints of the electronic devices which serve as unique identifiers to authenticate and secure devices. Two latency-based PUFs are compared in this work to build a research basis for read-based and write-based latency PUFs, which is the targeted PUF. Various important properties of PUF like uniqueness, randomness, reliability, low latency, and low interference is discussed. The PreLatPUF surpasses DRAM latency PUF in every aspect of different metrics evaluated with concrete evidence. This research aims to help and evaluate the performance of the desired read/write latency based PUFs for generating robust and reliable digital signatures at the present time as well as in the future.**

***Index Terms*—PUF, latency, PreLatPUF, DRAM-latencyPUF**

## I. Introduction

Physically unclonable functions (PUFs) are regarded as an important mechanism for electronic devices which for generating digital fingerprints which serve as unique identifiers to authenticate and secure wide range of security-related applications. Integrated circuit(IC) designers are always required to acknowledge various security issues which includes reverse engineering, cloning, side-channel attacks, counterfeiting, overbuilidng, tampering attacks, etc. [18] [2]. Due to the random variations like propagation delay, transistor drive strength, metal resistance, mismatches between complementary transistors and in physical properties, PUFs can help to distinguish from one device (or chips) to another as they are designed in such a way that they are practically burdensome or unfeasible to duplicate, even by the manufacturer [1]. The extensive studies and thorough researches conducted for PUFs has made it a dynamic security initiative choice for ICs because of it's appealing functionality in variety of applications, such as intellectual property (IP) counter-plagiarism, chip authentication, and embedded system security [10]. The random variations can be measured and evaluated but are impossible to replicate or simulate. A PUF measures these variations and equates them to generate a response. The quality of the bitstrings generated by a PUF is evaluated using several analytical metrics and the specific varying properties utilized by the PUF which can vary from one PUF design to another. PUF structures lead to the generation of unique and random challenge-response pairs (CRPs) for a chip [18]. A digital input as challenge is triggered, which gives a digital response from the PUF. The unclonability of PUFs originates from the random, irreplicable, and unpredictable variations in device structure during manufacturing.

The concept of PUFs can be applied to various physical systems, mobile devices, IoT applications and smart systems, sensor nodes, smart grids etc [2]. Although there are various different kinds of PUFs available according to the need but the significant amount of the PUF designs according to the popularity and functionality are based on memory as well as delay variation systems. The read/write latency PUF's idea is to utilize fundamental principle of both (delay and memory based) and provide a better result. The fundamental principle implemented in these memory-based designs is to utilize ubiquitous presence of memory in the embedded device as they require minimal(or no) additional hardware, unlike other PUF implementations [12] where as delay-based design's principle is to compare a pair of inherently symmetric/identical circuit elements(composed of logic and interconnect), and evaluate any delay mismatch that is instigated by the manufacturing process variation, and not by the design [10]. In delay-based systems there are specified timing constraints to schedule these delay-based operations and in memory-based, operation depends on single memory component based on single entropy source. Altering these parameters can affect the reliability of information produced by the PUF and results in data leakage, that is where an idea of read/write latency based structures can be introduced to construct a PUF where a filtering mechanism can be applied to eliminate unstable response in different iterations to enhance the PUF's robustness and reliability.

This paper presents comparison of ideas of different latency-based PUF designs that transform the inherent random variations in device parameters from basic physical constraints in manufacturing process to variations in circuit-level parameters for random digital signature generation.

The rest of the paper is organized as follows. Section II presents the background of DRAM architecture, read/write operation, properties of desirable PUFs, properties of run-time accessible PUFs, common different kind of PUFs. Related Work in Section III. Result and Analysis is present in Section IV. Followed by Evaluation of experiments conducted in two papers in Section V. And at last the paper concludes in Section VI.

## II. Background

In one-way (irreversible) physical unclonable function, a PUF is designed with numerous n-binary inputs, known as the input challenges [2]. An input challenge is necessary for the

generation of a binary response bits. For a PUF to be effective for applications such as encryption, the three requirements must be fulfilled: 1) Uniqueness: the generated response for each device/chip must be adequately unique to distinguish each chip from every other, 2) Robust and Randomness: it should be difficult for any adversary to design and predict the bitstrings thus, must be compulsorily random, and 3) Uniform and Reliable: according to different environmental background, the bitstring must be reliable and stable over time [1]. Likewise, for fast processing or working of PUF they must possess two key properties i.e. 1) Low Latency: Evaluation of PUF's application requesting authentication must be fast and should always opt for the smallest possible amount of time, 2) Low System Interference: Concurrently-running applications must not be hindered (slow down) by PUF evaluation [5]. There are two major sources of system interference: a) requiring exclusive DRAM rank/bank access during entire PUF evaluation and b) using a region in a separate DRAM rank to count latency failures. First, other access to the PUF memory segment should be blocked, as timing parameters could only be manipulated for the coarse granularity of DRAM rank and if allocation of other access to the same rank is permitted then it results in increasing the reduced timing parameters (more time is requried) and corrupts the data. Because of this evaluation requires exclusive access to a full DRAM rank for the entire duration of PUF evaluation. Secondly, the DRAM latency PUF algorithm requires a small counter buffer which stores counters for each bit of the PUF memory segment. But it is possible by compensating both DRAM capacity overhead and additional memory traffic penalty because of which the counter buffer can be insignificant.

Following these properties there are various types of PUFs following different methodologies, some of them are as follows: i) Arbiter PUFs(APUFs) are one of the famous delay-based PUFs. A switch-box construction is used by APUFs to produce a relay between two delay paths with an edge triggered flip-flop or D-latch known as arbiter at the end [2]. Two identical paths are formed to create one response bit based on the delay of these paths using challenge inputs. Using the designated paths whichever signal reaches the arbiter first, that signal is transmitted.

ii) Ring-Oscillator PUFs(RO-PUFs) consists of an odd number of reversing stages which are connected sequentially to maintain continuous oscillation. The frequencies of two ROs are compared to generate 1 bit output [6]. RO-PUF output generation mechanism generates a number of output bits, where a certain number of ROs are constructed and two of them are selected. For each bit generation, the selected ROs's frequencies are compared with identical counters.

iii) SRAM PUF is a six transistor circuit where four of the tranistors are used as two cross-coupled inverters which holds the value at their outputs and two transistors are used as the load transistors to steer the value applied from outside to the cross-coupled inverters [6]. SRAM causes each cell to derive one of two states (start-up values) to be 0 or 1, depending upon the relative strengths (minor voltage) differences and

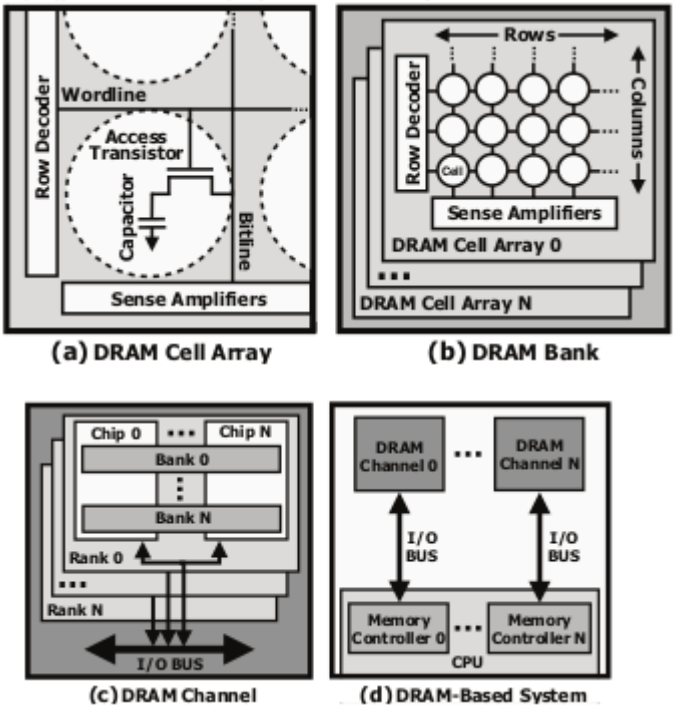


Fig. 1. DRAM Organization [5]

mismatches between two inverters as well as noise [12].

For the read/write latency based PUF, examples of DRAM Latency PUFs is considered because DRAM latency PUFs can be operated at a wide range of operating temperatures (0°C-70°C) which contributes to low evaluation time and during manufacture, the latency failures introduces inherent alteration related to chip-specific random method which enables for each DRAM chip to use the failures as unique identifiers [12]. The logic behind DRAM latency PUF is to provide unique device signatures using the error pattern derived from accessing DRAM with reduced timing parameters. Also, they deal with proper memory segment allocation/management which is relevant to read/write latency based PUFs and its memory management. The Fig.1 shows the DRAM organization.

## III. Related Work

Secret Unknown Ciphers (SUC) has been discussed by Mars et al. in [8] which acts as an ultra-low latency robust digital PUF coined as SRAM-SUC. Here SRAM-SUC focuses on downsides, mainly inconsistency of PUFs because of their analog nature establishing itself as a worthy mechanism which can outrank well-known PUF-based authentication methods by generating a faster response and appealing as an ideal solution for Ultra Reliable Low Latency Commnunication (URLLC).

Sutar et al. in [12] proposed a new memory-based combination PUF that intelligently combines two memory technologies, SRAM and DRAM to overcome their shortcomings which showed substantial improvements over current memory-based PUFs including ability to resist various attacks by not

depending on complex error correction and high operational latency.

Many PUFs have been proposed based on other substrates having different memory technologies and customized hardware designs. Some of them are as follows: Arbiter PUFs [14] [10] [4] [2] [9], Ring-Oscillator PUFs [14] [2] [16] [7] [6] [17], SRAM PUFs [12] [15], Butterfly PUFs [10], Neuron-PUF [3] [11] etc.

### *A. **DRAM Latency PUF: Evaluating PUFs by Exploiting the Latency-Reliability Tradeoff***

The traditional DRAM based PUFs were not up to the marks to be considered runtime-accessible as they had major drawbacks shown by Kim et al. (2018) in the paper [5]. So, they introduced a new class of DRAM PUF which intentionally violated manufacturer-specified DRAM latency parameters. The main goal of this research was to develop a new runtime-accessible PUF that i) uses existing commodity DRAM devices, 2) satisfy all characteristics of an effective runtime-accessible PUF, and 3) provide low-latency evaluation with low system interference across all operating conditions. The key idea of the DRAM latency PUF was to provide unique device signatures using the error pattern resulting from accessing DRAM with reduced timing parameters. These latency failures were essentially related to chip-specific random process variation introduced during manufacturing, which allowed the usage of failures as unique identifiers for each DRAM chip. For the evaluation of DRAM latency PUF, known data were written into a fixed-size memory segment (e.g., 4 DRAM rows = 8KiB in LPDDR4 DRAM chips) and were read it back with reduced timing parameters where the resulting failures formed a pattern of bits unique to the tested device. Using the data from 223 real LPDDR4 DRAM chips, it was evident that introduced DRAM latency PUF not only satisfies the requirements of an effective PUF but also runtime-accessible PUF. The Jaccard index, is a statistic used for gauging the similarity and diversity of sample sets so, Kim et al. used the Jaccard index as a metric for evaluation of similarity between PUF responses where index value closer to 1 indicates high similarity between the two PUF responses and a value closer to 0 indicates uniqueness. Thus, a unique PUF should have Jaccard index values close to 0 across all pairs of distinct memory segments. Intra-Jaccard represented the Jaccard index of two PUF responses from the same memory segments where Inter-Jaccard referred to the index of two PUF responses from different memory segments.

### *B. **PreLatPUF: Exploiting DRAM Latency Variations for generating Robust Signatures***

In the paper [13] Talukder et al.(2019) proposed a DRAM-based PUF that exploits the precharge-latency variations in DRAM cells for generating robust device signatures. Here, the latency was defined as the time required to move charge during read/write operation where the DRAM vendor provided the minimum required timing latency to perform a reliable read/write operation. If the minimum timing latency was not maintained, erroneous read/write operation was observed. Six memory banks from two commercial DDR3 memory modules of two major memory vendors (namely A and B) were experimented, which led to the results that the proposed scheme and algorithm (PreLatPUF) generates robust, unique and random signatures by satisfying the PUF's effectiveness and accessibility surpassing existing DRAM PUF's by providing outputs at a much faster rate.The motivation behind this research was: i) improve the DRAM Power Cycle's waste, ii) reduce large evaluation time, iii) designing a PUF which is less destructive and, iv) introducing a PUF which is less disruptive. Hamming Distance measures the minimum number of substitutions required to change one string into the other, or the minimum number of errors that could have transformed one string into the other. Therefore, Talukder et al. used Hamming Distance as a metric for evaluation to test three major properties of PUF performance metrics to quantify and compare it's proposed PreLatPUF. Minimum Hamming distance was set 0.25 and maximum Hamming distance was set 0.75 as input parameters. The Hamming distance of 0.5 was considered ideal where Hamming distance of 0 represented that the PUF was not unique meaning that Hamming distances close to 0 are sufficient to imply that the PUF is not unique whilst a value of 0 means that the two PUFs are completely identical. Inter-HD represented the distance of PUF responses from different memory segments where Intra-HD represented the distance of responses from the same memory segments.

## IV. Result and Analysis

In this section the two most influential research would be discussed i.e. done by Kim et al.(2018) [5] and Talukder et al.(2019) [13]. The conducted experiments to fulfill the important properties of a desirable PUF and metrics runtime-accessible PUF were tested and is mentioned below:

**i)Uniqueness and Uniform Randomness:** In [5],three 223 LPDDR4 DRAM chip's large number of different segments were studied where each memory segment were evaluated 50 times at 70°C. To ensure the proposed PUF exhibit uniqueness and uniform randomness across any memory segment from any device from any manufacturer, it was ensured that the distribution of Inter-Jaccard indices were distributed near 0 [5]. To prove two things: one was that the error patterns were unique such that no two distinct memory segments generated PUF responses with high similarity and other was the error patterns were distributed uniform randomly across the DRAM chips such that the likelihood of two chips generated the same error pattern was exceedingly low. The experiment showed that the distribution of the Inter-Jaccard indices was multimodal, but the Inter-Jaccard index always stayed below 0.25 for any pair of distinct memory segments meaning that DRAM latency PUFs from different memory segments had low similarity thus concluding that latency related error patterns satisfies the behaviour of a desirable PUF with regard to both uniqueness and uniform randomness which can be seen in Fig. 2

In comparison to [5] Talukder et al to check randomness, inter Hamming distance (interHD) was measured from each

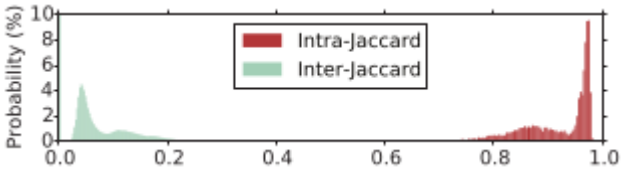


Fig. 2. Distributions of Jaccard indices calculated across every possible pair of PUF responses across all tested PUF memory segments from each of 223 LPDDR4 DRAM chips. [5]

| Vendor | Memory Bank ID | #Qualified row (%) | Average Hamming Distance (%) | Average Hamming weight (%) |
|---|---|---|---|---|
| A | a | 100.00 | 48.87 | 54.23 |
| | b | 92.31 | 49.35 | 53.29 |
| | c | 92.30 | 49.24 | 49.24 |
| | d | 67.82 | 28.97 | 53.98 |
| B | a | 74.84 | 42.28 | 68.19 |
| | b | 63.99 | 38.06 | 70.31 |

Fig. 3. Table of Average Hamming weight and average Hamming distance among the keys generated from each bank. [13]

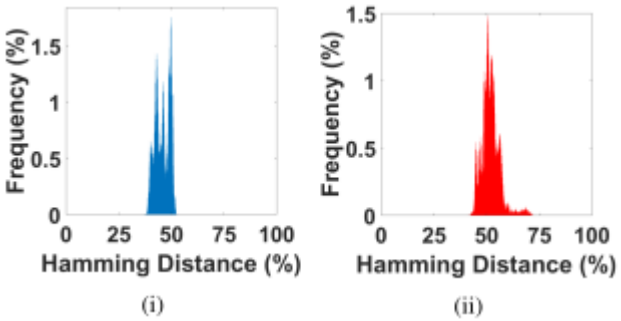


Fig. 4. Inter Hamming distance for the worst case from (i) vendor A (Micron) and (ii) vendor B (Samsung). [13]

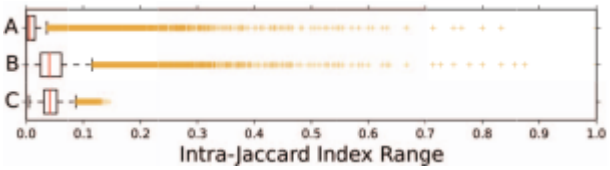


Fig. 5. Distribution of the Intra-Jaccard index range values calculated between many PUF responses that a PUF memory segment generates over a 30-day period. [5]

bank of the two vendor 'A' (Micron) and 'B' (Samsung). 50% of interHD signified that unique key can be generated from the tested bank and the average Hamming weight of 50% represented that keys were random. There were seven banks in total which were tested, vendor 'A' Micron had 4 banks and 'B' Samsung had 2 banks which were tested and found that vendor A's best average Hamming distance and average Hamming weight was 49.24% where vendor B's best average Hamming distance was 42.28%. Though the average HD and Hamming weight were not exactly 50% and chips deviate from 50%, the results from all chips showed that (From Fig. 3, 'A' deviated from 0.65% minimum to 21.03% maximum and B's minimum deviation 7.72%, maximum deviation 11.94%), the keys generated from the same memory bank were not repetitive. For uniqueness, the inter Hamming Distance (interHD) of the generated key from different memory banks was used. Following scenarios were considered for accessing uniqueness: 1) A different pair of banks which were from the same module. 2) A different pair of banks that were from different modules but from the same vendor. 3) A different pair of banks, from two different vendors. As a result worst case were shown (i.e., the largest deviation from 50% inter HD). Fig. 4 shows that for the vendor A, the average (mean), minimum and maximum inter HD were 45.78%, 37.05% and 52.5% respectively whereas, For the vendor B, 51.91% was the mean, 40.92% the minimum, and 72.23% the maximum. Every worst case was considered and it is safe to say that the best results did not deviated that far from the desired inter HD hence concluding that proposed PreLatPUF's key generation is unique.

**ii) Reliability:** In order to show that the DRAM latency PUF [5] exhibits reliability, multiple times different memory segments of PUF were evaluated and Intra-Jaccard indices were generated, as highly-repeatable PUF generates very similar PUF responses during each evaluation. Therefore, the Intra-Jaccard indices was expected to be tightly distributed near a value of 1. It was observed that the Intra-Jaccard indices were clustered very close to 1.0 and never dropped below 0.65. Also, the repeatability of DRAM latency PUFs on a subset of chips over a 30day period was studied to show that the repeatability property hold for longer period of time or not. More than a million 8KiB memory segments across many chips were examined and it was evident that the Intra-Jaccard index ranges are quite low i.e, less than 0.1 (shown in Fig. 5). Thus, it was evident that the DRAM latency PUF not only exhibited very high repeatability but also for longer period of time.

In contrast in order to test PreLatPUF's [13] reliability worst results from each vendor were presented (i.e., memory bank with the most significant deviation from 0%). At four different conditions the PUF was tested to prove it's reliability to work in extreme operating environment: 1) Nominal voltage and room temperature (NVRT), 2) low-voltage and room temperature (LVRT), 3) high-voltage and room temperature (HVRT), and 4) nominal voltage and high temperature (NVHT). From Fig. 6, we can observe that the bank d from the vendor A produced slightly robust output with the change in voltage (increased or decreased) because this bank produced noisier cells than other banks. The intra HD $\mu$ of bank d of vendor A's NVRT,LVRT,HVRT, and NVHT was 1.54%, 1.69'%, 1.47% and 4.72% respectively where as intra HD $\sigma$ was 9.02%, 8.87%, 8.73 % and 8.36% respectively.

**iii) Low latency:** In [5],for the PUF's evaluation time, the expected final evaluation time was estimated approximately 87ms. To experiment this, at 55°C 10000 evaluations across several chips from three manufacturers (A, B and C) were

| Vendor | Memory Bank ID | Operating Codition | $\Delta V$ (mV) | $\Delta T$ (° C) | Intra HD | | Key with Intra HD | |
|---|---|---|---|---|---|---|---|---|
| | | | | | $\mu$ | $\sigma$ | $> 1\%$ | $> 30\%$ |
| A | a | NVRT | 0 | 0 | 0.48 | 0.07 | 0.00 | 0.00 |
| | | LVRT | −20 | 0 | 0.05 | 0.08 | 0.00 | 0.00 |
| | | HVRT | +55 | 0 | 0.07 | 0.09 | 0.00 | 0.00 |
| | | NVHT | 0 | +20 | 0.06 | 0.09 | 0.00 | 0.00 |
| | b | NVRT | 0 | 0 | 0.47 | 3.17 | 1.57 | 0.00 |
| | | LVRT | −20 | 0 | 2.94 | 10.55 | 7.81 | 2.91 |
| | | HVRT | +55 | 0 | 0.09 | 0.10 | 0.00 | 0.00 |
| | | NVHT | 0 | +20 | 0.67 | 3.84 | 2.34 | 0.01 |
| | c | NVRT | 0 | 0 | 0.49 | 3.34 | 1.54 | 0.03 |
| | | LVRT | −20 | 0 | 7.77 | 12.38 | 27.95 | 0.46 |
| | | HVRT | +55 | 0 | 0.09 | 0.12 | 0.01 | 0.00 |
| | | NVHT | 0 | +20 | 0.52 | 3.38 | 1.54 | 0.02 |
| | d | NVRT | 0 | 0 | 1.54 | 9.02 | 4.37 | 2.74 |
| | | LVRT | −20 | 0 | 1.69 | 8.87 | 8.87 | 2.66 |
| | | HVRT | +55 | 0 | 1.47 | 8.73 | 4.29 | 2.64 |
| | | NVHT | 0 | +20 | 4.72 | 8.36 | 9.35 | 2.62 |
| B | a | NVRT | 0 | 0 | 1.97 | 10.25 | 3.37 | 3.25 |
| | | LVRT | −55 | 0 | 2.11 | 10.19 | 3.36 | 3.17 |
| | | HVRT | +55 | 0 | 1.92 | 10.02 | 3.53 | 3.17 |
| | | NVHT | 0 | +20 | 2.13 | 10.23 | 3.76 | 3.26 |
| | b | NVRT | 0 | 0 | 1.93 | 10.55 | 3.24 | 2.62 |
| | | LVRT | −55 | 0 | 2.22 | 10.30 | 5.68 | 2.52 |
| | | HVRT | +55 | 0 | 1.95 | 10.35 | 3.18 | 2.53 |
| | | NVHT | 0 | +20 | 1.99 | 10.55 | 3.39 | 2.74 |

Fig. 6. Table of Intra HD at different operating conditions. [13]

performed to measure the evaluation time of the DRAM latency PUF. According to the experiment manufacturer A's chips average computation speed was ($\mu$) 89.1ms, B's average computation speed was 88.2ms, and 'C' had computation speed of ($\mu$) 87.2ms, which showed that the evaluation times had similar means and were extremely tightly distributed close to 87ms which was the desired evaluation time. Also, mixture of several chips from all three manufacturer had the following result 'ABC'($\mu$ = 88.2ms) and found that the estimated 87ms from the experiment resulted in only 1.4 percent error. Also, from the experiment it was evident that DRAM latency PUFs were minimally affected by changes in temperature and importantly since the proposed method does not change with temperature, DRAM latency PUF evaluation time remains reliably short across all operating temperatures.

Likewise, in [13] for time evaluation, the original proposed method was not used but another method was used which was slower than the proposed method. Several memory segments of vendor A (Micron) and B (Samsung) were tested and worse average speed was calculated. From Fig.7, vendor A was very fast in generating keys compared to vendor B. Average time key generation for vendor A was 0.58ms where vendor B's average time was 1.46ms. In particular A's memory bank b was the fastest of all with average speed of 0.41ms. Even the worse timing was way faster than prior methodologies so it can be safely assured that proposed method is way faster.

| Vendor | Memory Bank ID | #Required Burst (mean) | Mean Evaluation time (ms) |
|---|---|---|---|
| A | a | 9.00 | 0.51 |
| | b | 6.43 | 0.41 |
| | c | 7.19 | 0.47 |
| | d | 16.10 | 0.93 |
| B | a | 28.15 | 1.59 |
| | b | 24.18 | 1.34 |

Fig. 7. Table of Average PreLatPUF evaluation time [13]

## V. Evaluation

Though the evaluation metric for both the researches conducted by Kim et al. [5] and Talukder et al. [13] were different but their results of their important properties can be compared to determine which was better in general. In terms of number of experimented chips, in [5] more number of several chips were tested compared to [13]. Regarding uniqueness and randomness, PreLatPUF generates unique keys better than DRAM latency based PUF(inter-Jaccard index below 0.25) because in PreLatPUF the worst case scenario was used and even results of the worst case scenarios(A's average 45.78% and B's average 51.91%) did not deviated that far from the desired or predetermined metric value. In the matter of reliability, though DRAM latency based PUFs were tested at more extreme temperatures(0°C-70°C) than PreLatPUFs but it was found that the deviation value was high from the pre-established value in DRAM latency based PUF(intra-Jaccard below 0.65, but 0.65 to 1 is high) than PreLatPUF (1.54%, 1.69'%, 1.47% and 4.72% under different circumstances and temperature). Likewise, in terms of speed even though original proposed method was not used but the worse average speed was still better in PreLatPUF (0.41ms) than DRAM latency based PUF' best average speed (87.2ms).

## VI. Conclusion

In this work, we have analyzed and compared different papers of latency based PUF. Despite producing outstanding results by the DRAM latency PUF prior to their predecessor, it could not surpass the results achieved by PreLatPUF for generating robust device signatures. There is still room to grow as further research can be done using other metric variables and development of future technologies can also play a huge role. Future work would include further improvement on read-based and write-based latency PUF's involvement in generating exemplary digital signatures which can be used for authentication and secure communication.

## References


[1] Jim Aarestad, Philip Ortiz, Dhruva Acharyya, and Jim Plusquellic. Help: A hardware-embedded delay puf. *IEEE Design Test*, 30(2):17–25, 2013.

[2] Fathi Amsaad, Mohammed Niamat, Amer Dawoud, and Selcuk Kose. Reliable delay based algorithm to boost puf security against modeling attacks. *Information*, 9(9):224, 2018.

[3] Mohamed Elshamy and Haralampos-G Stratigopoulos. Neuron-puf: Physical unclonable function based on a single spiking neuron. In *27th IEEE International Symposium on On-Line Testing and Robust System Design*, 2021.

[4] Miaoqing Huang and Shiming Li. A delay-based puf design using multiplexer chains. In *2013 International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, pages 1–6. IEEE, 2013.

[5] Jeremie S Kim, Minesh Patel, Hasan Hassan, and Onur 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. IEEE, 2018.

[6] Giray Kömürcü, Ali Pusane, and Günhan Dündar. A ring oscillator based puf implementation on fpga. *IU-Journal of Electrical & Electronics Engineering*, 13(2):1647–1652, 2013.

[7] Abhranil Maiti and Patrick Schaumont. Improved ring oscillator puf: An fpga-friendly secure primitive. *Journal of cryptology*, 24(2):375–397, 2011.

[8] Ayoub Mars, Hussam Ghandour, and Wael Adi. Sram-suc: Ultra-low latency robust digital puf. *arXiv preprint arXiv:2106.07105*, 2021.

[9] Sergey Morozov, Abhranil Maiti, and Patrick Schaumont. A comparative analysis of delay based puf implementations on fpga. *IACR Cryptol. ePrint Arch.*, 2009:629, 2009.

[10] Sergey Morozov, Abhranil Maiti, and Patrick Schaumont. An analysis of delay based puf implementations on fpga. In *International Symposium on Applied Reconfigurable Computing*, pages 382–387. Springer, 2010.

[11] Fatemeh Najafi, Masoud Kaveh, Diego Martín, and Mohammad Reza Mosavi. Deep puf: A highly reliable dram puf-based authentication for iot networks using deep convolutional neural networks. *Sensors*, 21(6):2009, 2021.

[12] Soubhagya Sutar, Arnab Raha, and Vijay Raghunathan. Memory-based combination pufs for device authentication in embedded systems. *IEEE Transactions on Multi-Scale Computing Systems*, 4(4):793–810, 2018.

[13] BMS Bahar Talukder, Biswajit Ray, Domenic Forte, and Md Tauhidur Rahman. Prelatpuf: Exploiting dram latency variations for generating robust device signatures. *IEEE Access*, 7:81106–81120, 2019.

[14] Yale Wang, Chenghua Wang, Chongyan Gu, Yijun Cui, Maire O'Neill, and Weiqiang Liu. Theoretical analysis of delay-based pufs and design strategies for improvement. In *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1–5, 2019.

[15] Fengchao Zhang, Shuo Yang, Jim Plusquellic, and Swarup Bhunia. Current based puf exploiting random variations in sram cells. In *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 277–280. IEEE, 2016.

[16] Ji-Liang Zhang, Gang Qu, Yong-Qiang Lv, and Qiang Zhou. A survey on silicon pufs and recent advances in ring oscillator pufs. *Journal of computer science and technology*, 29(4):664–678, 2014.

[17] Qinglong Zhang, Zongbin Liu, Cunqing Ma, Changting Li, and Lingchen Zhang. Fropuf: how to extract more entropy from two ring oscillators in fpga-based pufs. In *International Conference on Security and Privacy in Communication Systems*, pages 675–693. Springer, 2016.

[18] Yu Zheng, Fengchao Zhang, and Swarup Bhunia. Dscanpuf: A delay-based physical unclonable function built into scan chain. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 24(3):1059–1070, 2015.