Practical Experiments to Evaluate Quality Metrics of MRAM-Based Physical Unclonable Functions

ARASH NEJAT\textsuperscript{1}, FREDERIC OUATTARA\textsuperscript{1}, MOHAMMAD MOHAMMADINODOUSHAN\textsuperscript{2}, BERTRAND CAMBOU\textsuperscript{2}, KEN MACKAY\textsuperscript{3}, AND LIONEL TORRES\textsuperscript{1}

\textsuperscript{1}LIRMM, University of Montpellier, CNRS, 34095 Montpellier, France
\textsuperscript{2}School of Informatics, Computing, and Cyber Systems, Northern Arizona University, Flagstaff, AZ 86011, USA
\textsuperscript{3}Crocus Technology Grenoble, 38025 Grenoble, France

Corresponding author: Arash Nejat (arash.nejat@lirmm.fr)

This work was supported by the French Government BPI (Banque Publique d’Investissement) under Grant FUI AAP N° 18 MultiSmart.

\section*{ABSTRACT} Process variations in the manufacturing of digital circuits can be leveraged to design Physical Unclonable Functions (PUFs) that are extensively employed in hardware-based security. Different PUFs based on Magnetic Random-Access-Memory (MRAM) devices have been studied and proposed in the literature. However, most of these studies have been simulation-based, which do not fully capture the physical reality. We present experimental results on a PUF implemented on dies fabricated with a type of the MRAM technology namely Thermally-Assisted-Switching MRAM (TAS-MRAM). To the best of our knowledge, this is the first experimental validation of a TAS-MRAM-based PUF. We demonstrate how voltage values used for writing in the TAS-MRAM cells can make stochastic behaviors required for PUF design. The analysis of the obtained results provides some preliminary findings on the practical application of TAS-MRAM-based PUFs in authentication protocols. Besides, the results show that for key-generation protocols, one of the standard error correction methods should be employed if the proposed PUF is used.

\section*{INDEX TERMS} Physical unclonable functions, magnetic RAM, thermally assisted switching MRAM.

\section*{I. INTRODUCTION} Physical unclonable functions (PUFs) are primitive and essential circuitry components for hardware-based security. They are cost-effective to generate trustworthy signatures and high-quality random numbers for different security protocols, such as anti-counterfeiting, identification, authentication, key generation, etc., [1], [2]. Also, PUFs are low-power so they have received significant attention for addressing security issues of the Internet-of-Things (IoT) devices [2], [3].

The word unclonable in the term PUF refers to the most important property of such circuits. It suggests the difficulty of fabricating a circuit or developing an algorithm able to generate the same inputs/outputs of PUF. For this purpose, designers can leverage process variations (PVs) that happen during circuit manufacturing. PVs can make unique electrical characteristics for each instance of manufactured circuits [1].

Different PUFs have been reviewed in previous studies [4]. A well-known class of PUFs in digital circuits/systems is Memory-PUF in which memory cells are employed to design and implement PUFs. This class has received much interest because memories and state elements are embedded in today’s System on Chips (SoCs) [1], [3]. Memory-PUFs can be realized using different memory technologies. Two widespread memory technologies that have been largely studied for PUF design are Static RAM (SRAM) and Dynamic RAM (DRAM). However, PUFs based on these technologies have security issues since they are based on using digital information of “0” or “1” [7]. In such PUFs, for the first response, “0” or “1” is read in some specific cells. The response for those cells is the same for the next response queries. As a result, such PUFs can be broken when the hacker accesses them [7]. Contrariwise, PUFs based on technologies such as Resistive RAM (ReRAM) and Magnetoresistive RAM (MRAM) use the resistance value of memory cells. Thus, a given cell can be either ‘0’, ‘1’, ‘Z’ depending on its resistance value and the resistance ranges being considered as ‘0’, ‘1’, or ‘Z’ [7].

The non-obviousness of ReRAM or MRAM PUFs compared to SRAM or DRAM PUFs makes them more
encouraging [7]. However, ReRAM cells are susceptible to environmental and voltage fluctuations, which results in a 5-20% error rate [7].

MRAM is one of several new emerging technologies aiming to become a “universal” memory device. This technology has the potential to gain importance for non-volatile memories because of promising properties such as non-volatility, low fabrication cost, high speed, low power consumption, and high reliability [9].

In MRAM devices the electron spin is used to store information. Different types of MRAM devices have been realized, such asToggle MRAM (T-MRAM), Spin-Transfer Torque MRAM (STT-MRAM), Thermally-Assisted-Switching MRAM (TAS-MRAM), etc. In each type, a unique method is used to change the electron spin.

Different PUFs based on different MRAM types have been studied and proposed [8]–[11]. However, most of the studied MRAM-based PUFs have been conducted on simulation environments. Despite the valuable knowledge obtained in such studies, the lack of practical experiments is very tangible. However, there are a few experimental studies based on STT-MRAM devices. Research on designing other types of MRAM-PUFs is limited and to the best of our knowledge, this is the first experimental validation of TAS-MRAM-based PUF.

In this work, we present experiments, results, and analyses on the stochastic switching behavior of an MRAM-based PUF using some fabricated TAS-MRAM dies. These dies are designed and fabricated by Crocus Technology [12]. The measured quality metrics and analysis results in this study provide some preliminary findings showing that TAS-MRAM can be used in authentication or key-generation protocols instead of SRAM PUFs. This is due to 1) higher speed and lower power of TAS-MRAM rather than that of SRAM, 2) the acceptable error rate of the proposed PUF, which is more or less like the SRAM-PUFs error rate. The error rate results in this study show that the proposed PUF like SRAM-PUFs can be employed in key-generation protocols if one of the common error correction methods is used in that protocol. This is because even a 1-bit mismatch between two keys is not acceptable.

The remainder of the paper is organized as follows: Section II represents a necessary background on PUFs and MRAM devices. Section III presents the proposed PUF design in this work. Section IV explains the experiments and exhibits obtained results. Some discussions are prepared in Section V about different MRAM-PUFs. Finally, Section VI provides concluding remarks.

II. BACKGROUND

A. PHYSICAL UNCLONABLE FUNCTIONS

As mentioned before, in order to design PUFs, designers can leverage PVs that happen during circuit manufacturing [1]–[3]. PVs cause fluctuations in physical dimensions and materials density of transistors and interconnections, and thus in their magnetic and electrical characteristics in each instance of a fabricated circuit layout [1].

PUFs can be categorized into two classes: weak PUFs and strong PUFs [1], [8]. Weak PUFs have one or few practical and valid inputs, the so-called challenge in literature [1], [8]. On the contrary, strong PUFs have a large number of challenges [1], [8]. Weak PUFs employed within IoT devices have at least one uncloneable output, the so-called response, which is unique per each fabricated device (PUF instance) while applying an identical challenge [2], [3]. Therefore, they can be utilized as the device ID, secret authentication signature, or secret cryptographic key [13]. As a result, there is no need to store the keys, which can be stolen, into untrustworthy Flash or One-Time-Programmable memories. A large number of challenge-response pairs (CRPs) in strong PUFs have enough entropy to be able to replace Hardware Security Modules in Public Key Infrastructure [8], [14].

In order to introduce some properties of PUFs in this section and Section IV, we employ a notation as follows:

- $\mathcal{P}$: the structure or layout of a PUF
- $\Pi$: a fabricated instance of $\mathcal{P}$
- $|\Pi|$: the number of all the fabricated $\Pi$s
- $C\leftarrow\{0,1\}^N$: a valid challenge for each $\Pi$ with $N$ bits
- $\tilde{C}$: the set of all valid challenges
- $|\tilde{C}|$: the number of challenges in $\tilde{C}$
- $R\leftarrow\{0,1\}^M$: response for each $\Pi$ with $M$ bits
- $R_{ij} = \Pi_i(C_j)$, $i \leq j \leq |\tilde{C}|$: a response obtained by applying $C_j$, the jth $C$ of $\tilde{C}$, to $\Pi_i$, to the ith $\Pi$.

The quality of a PUF is measured according to different parameters. The three most important ones are explained in the following:

1) INTER-PUF VARIATION, OR UNIQUENESS (UQ)

For a weak PUF, $UQ$ shows the average difference between the responses corresponding to one identical valid challenge applied to every instance of the PUF. For a strong PUF, all or several valid challenges are applied to every instance of the PUF. This parameter is shown in (1). For the ideal PUF, $UQ$ is 50% [1], [8].

$$UQ = \frac{1}{|\Pi| |\tilde{C}|} \sum_{i=1}^{|\Pi|-1} \sum_{j=1}^{|\tilde{C}|} \Pi_i(C_j) - \Pi_{i+1}(C_j) \quad (1)$$

2) INTRA-PUF VARIATION, OR REPRODUCIBILITY (RE)

RE is the variation of the responses of an instance PUF over time. For a weak PUF, $RE$ shows the average difference between the responses corresponding to one identical challenge repeatedly applied to each instance of a PUF, e.g., for $T = 1000$ times. For a strong PUF, instead of one challenge, all or several challenges are applied to all the instances. $RE$ is shown in (2). If a PUF is ideal, its responses are stable and robust for environmental conditions and multiple reading; thus, $RE$ is 0% for the ideal PUF [1], [8]. Actually, an RE less than 10% is acceptable [8], and one can employ error

The measured quality metrics and analysis results in this study provide some preliminary findings showing that TAS-MRAM can be used in authentication or key-generation protocols instead of SRAM PUFs. This is due to 1) higher speed and lower power of TAS-MRAM rather than that of SRAM, 2) the acceptable error rate of the proposed PUF, which is more or less like the SRAM-PUFs error rate. The error rate results in this study show that the proposed PUF like SRAM-PUFs can be employed in key-generation protocols if one of the common error correction methods is used in that protocol. This is because even a 1-bit mismatch between two keys is not acceptable.
correction methods to decrease \( RE \) to the order of magnitude of \(-6\) or even \(-9\) [15].

\[
RE = \frac{1}{T \cdot |\Pi| \cdot |\bar{C}|} \sum_{i=1}^{\Pi} \sum_{j=1}^{|\bar{C}|} \sum_{t=1}^{T-1} T_1 (\Pi_t (C_j)) - T_{t+1} (\Pi_t (C_j))
\]  

(2)

3) UNIFORMITY (UF)

One can easily calculate the fraction exists in the number of ‘0’ to the number ‘1’ in the responses corresponding to an identical challenge applied to every instance of a weak PUF. UF is the average of this fraction among all the instances. Like the previous parameters, all or several challenges are utilized for strong PUFs. UF is shown in (3). For the ideal PUF, UF is 1 [1], [8].

\[
UF = \frac{1}{|\Pi| \cdot |\bar{C}|} \sum_{i=1}^{\Pi} \sum_{j=1}^{|\bar{C}|} \frac{\text{No. of zeroes in } r_i^{(j)}}{\text{No. of ones in } r_i^{(j)}} \tag{3}
\]

These parameters are employed in this work to show the quality of the proposed PUF.

B. MRAM TECHNOLOGY AND TAS-MRAM DEVICES

MRAM exploits the Tunnel magnetoresistance (TMR) effects due to Magnetic tunnel junctions (MTJs). In Fig. 1a, a simplified schematic of an MTJ is presented. It consists of one insulator, the so-called tunnel barrier, interpolated between two ferromagnetic layers. The tunnel barrier is thin enough such that electrons can tunnel from one ferromagnetic layer into the other one. The TMR phenomenon is impossible in classical physics, but it is explicable in quantum physics.

Another point about MTJs is that their resistances significantly differ when their ferromagnetic layers have a parallel (P) or anti-parallel (AP) magnetic orientation [16]. These two resistances are denoted by \( R_p \) and \( R_{ap} \) in Fig. 1a. An MTJ resistance is low when the two ferromagnetic layers have a parallel magnetic orientation; otherwise, in the antiparallel configuration, the resistance is high [17]. This can be interpreted that MTJs operate like a switch.

One of the two ferromagnetic layers in each MTJ has a fixed magnetic orientation. This layer is called the “pinned layer” (PL). On the contrary, the magnetic orientation of the other layer, the so-called free-layer (FL), is easily changeable. Different methods have been designed to change the magnetic orientation of FL. For example, in STT-MRAM devices, a polarized current is applied to change the magnetic orientation of FL [18].

In TAS-MRAM devices, increasing temperature through MTJ while applying an external magnetic field can change the magnetic orientation of FL [19]. Fig. 1b shows the schematic of an MTJ device fabricated with TAS-MRAM. As can be seen in this figure, the MTJ has two antiferromagnetic layers of AFML\(_1\) and AFML\(_2\), correspond to the PL and FL, respectively. AFML\(_1\) and AFML\(_2\) have the blocking temperatures of TB\(_1\) = 300° and TB\(_2\) = 160°, respectively. The magnetic orientation of the FL and PL remains fixed and insensitive to external magnetic fields for temperatures below the blocking temperatures, also called the “temperature of Neel.” To change the magnetic orientation of the FL in Fig. 1b, one must heat AFML\(_2\) up to 160°. For this purpose, a parameter called “heating voltage” is employed [20].

The writing process in a TAS-MRAM MTJ is depicted in Fig. 2. At first, the MTJ heats up and when it is warm enough, its FL becomes ready to store ‘0’ or ‘1’. Afterward, a field line current is applied to the MTJ. The direction of this current determines the direction of the FL. Finally, a short time-space is required to cool down the MTJ by stopping the heating while maintaining the field line current.

C. PROCESS VARIATION EFFECTS ON TAS-MRAM

Due to PVs physical attributes of TAS-MRAM MTJs, such as the thickness and materials density of the ferromagnetic/insulator layers, are slightly different in every MTJ. One important feature of each MTJ affected by PVs is the heating voltage threshold (HV\(_{th}\)) of the MTJ, which is the minimum voltage required to sufficient heat up the AFML\(_2\) to change the magnetic direction of the FL [21]. To reliably set/reset an MTJ in TAS-MRAM devices, one needs to employ a value for the heating voltage more than the HV\(_{th}\).

The HV\(_{th}\) variability causes stochastic switching behavior in each MTJ while applying a voltage equal to the theoretically calculated HV\(_{th}\). In other words, some MTJs heat up enough to switch using the HV\(_{th}\) and some MTJs do not. As a result, employing a voltage equal to the HV\(_{th}\) may cause failures in the set/reset operations [20]. Finding a value that causes a failure probability of 50% allows for designing PUF. However, having exactly 50% is not practically feasible.
III. PROPOSED PUF DESIGN

In this work, we aimed to explore an MRAM-PUF implemented on TAS-MRAM dies. It leverages PV effects on the write operations. The dies are designed and fabricated by Crocus Technology [12]. Each die includes 1 kbit arranged in a 32 × 32 array such that each bit is individually addressable and accessible. A microscopic picture of the dies and its holding package (QFN44) are shown in Fig. 3.

![QFN44 package (left) and microscopic picture of the TAS-MRAM die in QFN44 (right).](image)

The architecture of the dies is presented in Fig. 4. Here, IOF, IOM, and IOR are sense pads employed during the read operation. As seen in this figure, IOF is the pad connected to the top of the MTJ of each memory cell. It enables applying the intended voltages, during the read/write operations. IOM is connected right below the MTJ, and IOR is between a poly 500Ω resistance and a Select transistor. This transistor in each cell is derived by one of the outputs of the decoder, which converts the data of the address pines. The impedance of an MTJ holding ‘0’ is changed from \( R_{\text{min}} = 2k\Omega \) to \( R_{\text{max}} = 4k\Omega \) by the write ‘1’ operation (W1). Likewise, the write ‘0’ operation (W0) changes the MTJ impedance from \( R_{\text{max}} \) to \( R_{\text{min}} \). Both the operations require three voltages: \( V_{\text{Heat}} \), \( V_{\text{Field 1}} \), and \( V_{\text{Field 2}} \). The first one is needed to heat the selected MTJ, whereas the second and third ones allow changing the magnetic orientation of FL in the desired state after heating.

To have a certain MTJ holding ‘0’ is changed from \( R_{\text{max}} \) to \( R_{\text{min}} \). Both the operations require three voltages: \( V_{\text{Heat}} \), \( V_{\text{Field 1}} \), and \( V_{\text{Field 2}} \). The first one is needed to heat the selected MTJ, whereas the second and third ones allow changing the magnetic orientation of FL in the desired state after heating. To have a certain MTJ holding ‘0’, one needs to apply 2.2 V to \( V_{\text{Heat}} \) and then \( V_{\text{Field 1}} \) and \( V_{\text{Field 2}} \). The duration of these three signals, \( T_{\text{Heat}} \), \( T_{\text{Field 1}} \), and \( T_{\text{Field 2}} \), must be 30 ns. In these cases, one can be sure that the write operations are done without any failure. We call these operations “Certain Write 0” (CW0) and “Certain Write 1” (CW1). The requirement of the read operation are \( V_{\text{Field 1}} = V_{\text{Field 2}} = 0 \) V, \( V_{\text{Heat}} = 0.3 \) V, and \( T_{\text{Heat}} = 30 \) ns.

In the proposed PUF, we use CW1 and then “Uncertain Write 0” (UW0) in which a voltage in the range of \( 1 \) V to \( 1.8 \) V is selected for applying to \( V_{\text{Heat}} \). In this case, the probability that a cell has the logic ‘0’ after performing the sequence of CW1-UW0 depends on \( 1 \) the selected voltage for \( V_{\text{Heat}} \). 2) PVs that affect the MTJ. To have an efficient PUF, one must select a value from the mentioned range such that it results in a failure probability of 50%.

It is noteworthy that if the CW0 and CW1 operation does not affect the resistance value of an MTJ, it can be broken or defective. Broken MTJs are the ones whose resistance and voltage value are sensibly lower than normal MTJs. The resistance and voltage of broken MTJs in our dies are always less than \( 400 \) Ω and \( 100 \) mV, respectively. There are also some defective MTJs, not broken or shorted; they are always in either of the P or AP states. In fact, the magnetic direction of the FL is always fixed in the defective MTJs. Therefore, the resistance of an MTJ does not change even if the CW0/CW1 operations repeated several times, that MTJ is defective.

IV. EXPERIMENTS AND RESULTS

In our experiments, we employ a Xilinx NEXYS2 FPGA board [22] [Bea, 2000 #14] and a National Instrument acquisition board [23] for writing in and reading from the dies, shown in Fig. 5. As seen in this figure, a PCB is designed and fabricated to route the address and read/write pins of the die to the FPGA board. It includes 3 digital potentiometers that can be controlled and set up through I2C protocol. The FPGA sets up addresses and commands these potentiometers to regulate the necessary voltages for writing in or reading from the cells of a die under test. The acquisition board is employed to read the voltage value of the addressed cells during the reading operation. Three pads are shown in Fig. 4 and used to read the voltage of the MTJ at the three different points.
The flow of the experiments starts by distinguishing broken and defective cells from intact ones. Figs. 6a and 6b illustrate the cells of a die by applying CW₁ and CW₀, respectively. As seen in Fig. 6a, there is one broken cell (blue) in the die under test. Six always-P-state cells (yellow) with a voltage value between 220 mV and 260 mV are also seen in Fig. 6a. Moreover, 21 always-AP-state cells (dark red) with a value of more than 300 mV are seen from Fig. 6b. In Fig. 6b there are some (around 45) light red cells with a voltage between 270 mV and 290 mV. Some of them are fixed, but some of them usually get a value in this range. One can consider wider voltage ranges to interpret the P and AP states and use such cells.

The probability of the voltage range corresponding to Fig. 6 is shown in Fig. 7. The common part between the two diagrams of this figure corresponds to the light red cells in Fig. 6. These two diagrams are almost the same as all the other dies. The values in this diagram indicate that there is more variation in the P state. Therefore, in the next step, we run the sequence of CW₁-UW₀-Read.

The second step in our experiments is to analyze different heating voltages to find out a proper one, by which 50% Hamming distance is obtained for inter-PUF variation. For this purpose, experiments begin from a heating voltage equal to 1.8 V. The sequence of CW₁-UW₀-Read is applied to all the cells of 26 dies. Then, 0.1 V is deducted from the heating voltage and the sequence is repeated. This procedure is continued until the heating voltage reaches 1 V.

Figure 8 illustrates the inter-PUF variation obtained by (1) for each of 26 dies in different heating voltages. The dashed lines in this figure show that for the heating voltages in the range of 1.4 V-1.6 V, For these three heating voltages the inter-PUF variations among all the dies are almost 40%-50%, which is an acceptable range. Fig. 9 shows the average of the inter-PUF variations among all the dies for the employed heating voltages. According to the green (dashed) bar in the figure, the best inter-PUF variation result is 49.8% for 1.4 V.

The third step in our experiments is to measure intra-PUF variation. For this purpose, the sequence of CW₁-UW₀-Read is run 1000 times on all the cells of the 26 dies. Like the previous step, nine heating voltages varying from 1.8 V to 1 V are analyzed. The results are reported in Fig. 10 and Fig. 11. Figure 10 shows the intra-PUF variations corresponding to each die for different heating voltages. Figure 11 presents the average of the intra-PUF variations among all the dies for different heating voltages.

![FIGURE 6. 32 × 32 cells in a die, a) applied CW₁ and b) applied CW₀.](image-url)
different heating voltages. In these figures, the lines and bars corresponding to the heating voltage 1.4 V are dashed (green). For this voltage, the intra-PUF variation obtained by (2) is 7.7%. This rate is acceptable and can be easily corrected using error correction methods like those proposed in [10], [15].

As mentioned in Section II, uniformity is an important parameter for PUFs. Fig. 12 shows the average of the uniformity among all the dies for the different heating voltages. As shown in this figure, the best result (i.e., 0.93) is obtained using the heating voltage of 1.4 V.

V. DISCUSSION

Although MRAM devices have many advantages over other types of NVMs, there are still existing issues regarding their reliability and security. One of the main concerns about MRAM devices is their vulnerability to magnetic fields and temperature. Different methods have been used to solve these issues. For example, in T-MRAM, designing a magnetic shield or heat shield around the device can be a possible solution [29], [30], but due to its cost, it may not be practical or useful for applications such as IoT. Moreover, MRAM devices can face an intentional magnetic field and temperature, which may not be protected by the packaging. For example, Everspin lists the maximum magnetic tolerance for their MRAM chips during write/read/standby to be only 100Oe [24].

STT-MRAM offers high density and consumes almost zero leakage power. This MRAM type is quite mature [9]. The unique characteristics of STT-MRAM make it a suitable candidate for several applications such as replacing conventional memories. However, its high and asymmetric read/write current introduces new challenges. For example, similar to the write current, the read current passes through the MTJ might affect the free-layer magnetization. Therefore, one of the problems with STT-MRAM is the induced disturbance of the free-layer state during reading [8]. More importantly, different kinds of security attacks have been reported on STT-MRAM-PUFs. For example, in [9], a correlation power analysis on the write operations of an STT-MRAM-PUF is performed successfully.

TAS-MRAM requires a single magnetic field and lower field values compared to T-MRAM, and thus it consumes less power than T-MRAM. Also, TAS-MRAM solves the limitation of conventional MRAM devices for PUF applications. First, addressing errors are reduced since the selection at write
operation is driven by temperature. Second, TAS-MRAM has better reliability and less vulnerability than STT-MRAM to field disturbance [25]. Although external fields change the resistance state of a cell, the state after the field disturbance goes back to its first state [8], [25].

| TABLE 1. Based PUF designs comparison. |
|---------------------------------------|
| MRAM Type   | RE  | U/Q  | Ref. # | Simulation |
|-------------|-----|------|--------|------------|
| STT         | 5.0% | 45.83% | [26]   | Simulation |
| STT         | 2.25% | 47%   | [27]   | Simulation |
| STT         | 1%–10% | ~50.1% | [28]   | Simulation |
| STT         | 0%   | ~50%  | [9]    | Experimental |
| TAS         | 7.7% | 49.8% | This work | Experimental |

The results of some of the previous publications on MRAM-PUFs are provided in Table 1. The studies are selected since the quality metrics of their designed MRAM-PUFs have also been reported without any post-processing method. However, they are not necessarily the most recent. In [26]–[28], promising MRAM-based PUF results are reported. However, the reported results are based on simulation studies, which do not fully capture the physical reality. In comparison, our results are based on experiments on the fabricated TAS-MRAM dies. In [9], the results are based on small-scale experiments on STT-MRAM while our results are based on larger-scale analyses. The use of the MRAM-based PUFs in key generation protocols [26]–[28] necessitate employing some error reduction/correction methods to enhance PUF reliability. Our results show 49.8% of the inter-PUF between different TAS-MRAM-based PUF dies. Nevertheless, our findings show 7.7% of the intra-PUF, which is more satisfactory compared to one reported in the previous studies [26]–[28]. Therefore, a method for handling the error is necessary for key generation using the TAS-MRAM-based PUF. However, our results show that the proposed PUF can be used instead of SRAM PUFs for key-generation or authentication protocols, which are considered as future research. This is because the inter-PUF distances are near to the maximum and the intra-PUF (error rate) is in an acceptable range. This can reduce False Rejection Rate (FRR) and False Acceptance Rate (FAR) in authentication protocols. Numerical evaluation of FAR and FRR in key-generation protocols is also, considered as future research.

VI. CONCLUSION

In this work, practical experiments are performed on fabricated TAS-MRAM dies. The experiments include analyzing the efficiency of an implemented PUF on these dies. The major objective of this work is to investigate the stochastic switching behavior in the MTJ cells of the dies as a source of randomness. The experimental results of this work show the possibility of obtaining a PUF on TAS-MRAM devices with almost 50% inter-PUF variation, 0.94 uniformity by accepting 7.7% intra-PUF variation, without using any extra hardware overhead. To realize this goal, we need to run the sequence of the certain-writing-1 and uncertain-writing-0 operations by applying 2.2 V and 1.4 V for the heating voltage required in the writing operations in the 1 kbit TAS-MRAM dies. The main conclusion is that our suggested circuits can be used to design resilient PUFs with TAS-MRAM.

VII. ACKNOWLEDGMENT

The authors would like to thank Dr. Bernard Dieny (CEA-Grenoble) for useful discussions.

REFERENCES

[1] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, “Physical unclonable functions and applications: A tutorial,”Proc. IEEE, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[2] B. Halak, M. Zwolinski, and M. S. Mispan, “Overview of PUF-based hardware security solutions for the Internet of Things,” inProc. IEEE 59th Int. Midwest Symp. Circuits Syst. (MWSCAS), Oct. 2016, pp. 1–4.

[3] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, “A PUF-based secure communication protocol for IoT,”ACM Trans. Embedded Comput. Syst., vol. 16, no. 3, pp. 1–25, Jul. 2017.

[4] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, “A PUF taxonomy,”Appl. Phys. Rev., vol. 6, no. 1, Mar. 2019, Art. no. 011303.

[5] A. Garg and T. T. Kim, “Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect,” inProc. IEEE Int. Symp. Circuits Syst. (ISCAS) Jun. 2014, pp. 1941–1944.

[6] C. Keller, F. Girkaynak, H. Kaeslin, and N. Felber, “Dynamic memory-based physically unclonable function for the generation of unique identifiers and true random numbers,” inProc. IEEE Int. Symp. Circuits Syst. (ISCAS), Jun. 2014, pp. 2740–2743.

[7] B. Cambou and M. Orlowski, “PUF designed with resistive RAM and ternary states,” inProc. 11th Annu. Cyber Secur. Res. Conf. CISRC Apr. 2016, pp. 1–8.

[8] E. I. Vatapulu, G. D. Natale, M. Barbaresechi, L. Torres, M. Indaco, and P. Proni, “STT-MRAM-Based PUF architecture exploiting magnetic tunnel junction fabrication-induced variability,”ACM J. Emerg. Technol. Comput. Syst., vol. 13, no. 1, pp. i–21, Dec. 2016.

[9] Y.-S. Chen, D.-Y. Wang, Y.-C. Hsin, K.-Y. Lee, G.-L. Chen, S.-Y. Yang, H.-H. Lee, Y.-J. Chang, I.-J. Wang, P.-H. Wang, C.-I. Wu, and D. D. Tang, “On the hardware implementation of MRAM physically unclonable function,”IEEE Trans. Electron Devices, vol. 64, no. 11, pp. 4492–4495, Nov. 2017.

[10] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, “Emerging physical unclonable functions with nanotechnology,”IEEE Access, vol. 4, pp. 61–80, 2016.

[11] G. Finocchio, T. Moriya, R. De Rose, G. Siracusano, M. Lanuzza, V. Puliafito, S. Chiappini, F. Crupi, Z. Zeng, T. Ono, and M. Carpentieri, “Spin-orbit torque based physical unclonable function,” J. Appl. Phys., vol. 128, no. 3, 2020, Art. no. 033904.

[12] C. T. Accessed: 2020. [Online]. Available: https://circus-techology.com

[13] G. E. Suh and S. Devadas, “Physical unclonable functions and applications: A tutorial,”Proc. IEEE 59th Int. Midwest Symp. Circuits Syst. (MWSCAS), Oct. 2016, pp. 1–4.

[14] W. Che, F. Saqib, and J. Plusquellic, “PUF-based authentication,” inProc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD), Nov. 2015, pp. 337–344.

[15] B. Colombier, L. Bossuet, D. Hély, and V. Fischer, “Key reconciliation protocols for error correction of silicon PUF responses,”IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1988–2002, Aug. 2017.

[16] C.-Y. You and H. Kim, “Effect of finite tunneling magnetoresistance for the switching dynamics in the spin transfer torque magnetic tunneling junctions,”IEEE Trans. Magn., vol. 53, no. 11, pp. 1–4, 2017.
Mohammad Mohammadinodoushan received the M.Sc. degree in electrical engineering from Northern Arizona University, where he is currently pursuing the Ph.D. degree in informatics and computing. His research interests include renewable energy power systems, including data mining, machine learning, intelligent control, and power electronics, and cyber engineering for cybersecurity, including statics to circuits of memory PUFs, very novel password managers utilizing PUFs, as well as key generation, keyless encryption, and key exchange using PUFs.

Bertrand Cambou received the Ph.D. degree from Paris-South (XI) University. He is currently a Professor of Practice with Northern Arizona University (NAU). He worked in smartcards/secure microcontrollers at GEMPLUS (now Gemalto) and in the POS/secure payment at Ingenico. He spent 15 years at Motorola Semiconductors (now NXP-Freescale), where he served in multiple capacities including the CTO, and was named a “Distinguished Innovator” and a Scientific Advisor of the BOD. In the last five years, he worked as the CEO in Silicon Valley in a high-tech industry, where his organization won a contract with the DARPA with applications related to quantum cryptography. He authored or coauthored 42 patents in microelectronics and cybersecurity. His primary research interests include cyber-security, and how to apply microelectronics to strengthen hardware security, the design of novel secure elements, physically unclonable functions (PUF), true random generators (TRNG), and the usage of nanotechnologies such as the ReRAM.

Ken Mackay received the Ph.D. degree in physics from the University of Cambridge, U.K. He is currently the Vice President of Technology Development with Crousé Technology Grenoble, Grenoble, France. He was previously with Hitachi GST, IBM, San Jose, CA, USA, and the National Center for Scientific Research, Grenoble. He has more than 20 years of extensive research and development expertise in magnetoresistive materials.

Frederic Ouattara received the M.Sc. degree in microelectronics from Polytech Marseille, France, in 2015. He is currently pursuing the Ph.D. degree with the Montpellier Laboratory of Informatics, Robotics, and Microelectronics, a joint research laboratory between the University of Montpellier and the French National Center for Scientific Research (CNRS). His research interest includes HW security primitives.