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

Lionel Torres, Arash Nejat, Bertrand Cambou, Frédéric Martial Ouattara, Ken Mackay, Mohammad Mohammadinodoushan

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier

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

Arash Nejat[1], Frederic Ouattara[1], Mohammad Mohammadinodoushan[2], Bertrand Cambou[2], Ken Mackay[3], and Lionel Torres[1]

[1]LIRMM, University of Montpellier, CNRS, Montpellier, France
[2]School of Informatics, Computing and Cyber Systems, Northern Arizona University, Flagstaff, US
[3]Crocus Technology Grenoble, 4 place Robert Schuman, 38025 Grenoble Codex, France

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

The French Government (BPI) under grant FUI AAP N ° 18 MultiSmart has funded this project. We thank Dr. Bernard Dieny (CEA-Grenoble) for useful discussions.

ABSTRACT: Process variations in the manufacturing of digital circuits can be leveraged to design Physical Unclonable Functions (PUFs) extensively employed in hardware-based security. Different PUFs based on Magnetic Random-Access-Memory (MRAM) devices have been studied and proposed. However, most of such research has 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. In addition, the results show that for key-generation protocols one of the standard error correction methods should be employed if the proposed PUF is used.

INDEX TERMS: Physical Unclonable Functions, magnetic RAM, Thermally Assisted Switching MRAM

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, disgners can leverage process variations (PVs) that happen during circuit manufacturing. PVs can make electrical characteristics of manufactured circuits unique in each instance [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 memorys and state elements are embedded in todays' System on Chips (SoCs) [1, 3]. Memory-PUFs can be realized using different memory technologies. Two widespread memory technoogies 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 technlogies 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 nonobviousness of ReRAM or MRAM PUFs compared with SRAM or DRAM PUF makes them more encouraging [7]. However, ReRAM cells are susceptible to environmental and voltage fluctuations, which results in a 5-*20%* error rate [8].

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 [10].

In MRAM devices the electron spin is used to store information. Different types of MRAM devices have been realized, such as Toggle 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 [9-12]. 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 but they are done 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 [13]. 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 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 used 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 presents a necessary background on PUFs and MRAM devices. Section III represents 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, in order to desing PUFs designers can leverage PVs that happen during circuit manufacturing [1-3]. PVs cause fluctuations in physical dimensions 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, 9]. Weak PUFs have one or few practical and valid inputs, the so-called *challenge* in literature [1, 9]. On the contrary, strong PUFs have a large number of challenges within a finite timeframe [1, 9]. Weak PUFs employed within IoT devices have at least one unclonable 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 [14]. As a result, there is no need for storing 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 (PKI) [9, 15]

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

- Ƥ: the structure or layout of a PUF
- Π: a fabricated instance of Ƥ;
- |Π|: the number of all the fabricated Πs
- C←{0,1}N: a valid challenge for each Π with N bits
- Č: the set of all valid challenges
- |Č|: the number of challenges in Č
- R←{0,1}M: response for each Π with M bits
- Rij = Πi (Cj) ($1 \leq i \leq |\Pi|$, $1 \leq j \leq |\check{C}|$}: a response obtained by applying Cj, the jth C of Č, to Πi, to the ith Π.

The quality of a PUF is measured according to different parameters. 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, 9].

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

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 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, 9]. In real words, less than *10% RE* is acceptable [9], and one can employ error correction methods to decrease *RE* to the order of magnitude of -6 or even -9 [16].

$$RE = \frac{1}{T.|\Pi|.|\check{C}|}\sum_{i=1}^{|\Pi|}\sum_{j=1}^{|\check{C}|}\sum_{t=1}^{T-1} T_t\left(\Pi_i(C_j)\right) - T_{t+1}\left(\Pi_i(C_j)\right) \quad (2)$$

3) UNIFORMITY (UF)

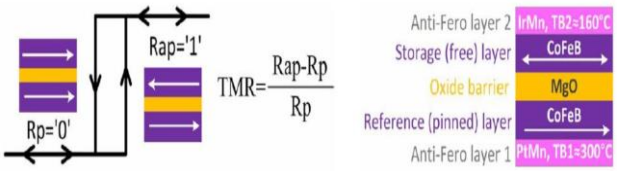
One can easily calculate the fraction exists in the number of '0' to the number '1' in the responses corresponding to an identical challenge applied to every instance of a weak PUF. *UF* is the average of this fraction among all the instances. Similar to the previous parameters, all or several challenges are utilized for strong PUFs. UF is shown in (3). For the ideal PUF, *UF* is 1 [1, 9].

$$UF = \frac{1}{|\Pi|.|\check{C}|}\sum_{i=1}^{|\Pi|}\sum_{j=1}^{|\check{C}|}\frac{No.\,of\ zeroes\ in\ r_i^{c_j}}{No.\,of\ ones\ in\ r_i^{c_j}} \quad (3)$$

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.



(a) (b)

FIGURE1. a) An MTJ in the parallel and antiparallel state, b) general schematic of an MTJ in TAS-MRAM devices [18]

Another point about MTJs is that their resistances significantly differ when their ferromagnetic layers have a parallel (P) or anti-parallel (AP) magnetic orientation [17]. These two resistances are denoted by *Rp* and *Rap* 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 [18]. 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 *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 [19].

In TAS-MRAM devices, increasing temperature through MTJ while applying an external magnetic field can change the magnetic orientation of FL [20]. 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°C and TB_2 = 160°C, 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°C. For this purpose, a parameter called "heating voltage" is employed [21].

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.

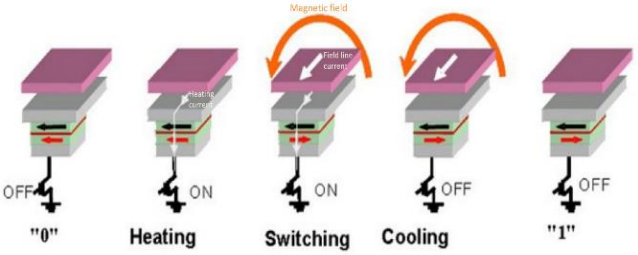


FIGURE2. The procedure of writing in a TAS-MRAM MTJ [17]

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 PV is the heating voltage threshold (HVth) of the MTJ, which is the minimum voltage required to sufficient heat up the $AFML_2$ to change the magnetic direction of the FL [22]. To set/reset a TAS-MRAM MTJ reliably, one needs to employ a value for the heating voltage more than the HVth.

The HVth variability causes stochastic switching behavior in each MTJ while applying a voltage equal to the theoretically calculated HVth. In other words, using the HVth, some MTJs heat up enough to switch and some MTJs do not. As a result, employing a value near to the HVth may cause failures in the set/reset operations [21]. Finding a value that causes a failure

probability of 50% allows 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 write operations. The dies are designed and fabricated by Crocus Technology [13]. Each die includes 1 *kbits* 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.

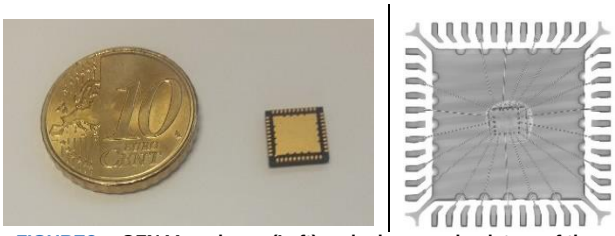


FIGURE3. **QFN44 package (Left) and microscopic picture of the TAS-MRAM die in QFN44 (right)**

The architecture of the dies is presented in Fig. 4. Here, IOF, IOM, and IOR are sense pads employed during the read (R) operation. As seen in thid 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 drived by one of the outputs of the decoder, which converts the dada of the address pines. The total impedance of an MTJ holding '0' is changed from R_{min} = *2k*Ω to R_{max} = *4k*Ω by the write '1' operation (W_1). Likewise, the write '0' operation (W_0) changes the MTJ impedance from Rmax to Rmin. Both the operations require three voltages: V_{Heat}, V_{Field1}, and V_{Field2}. The first one is needed to heat locally 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 certian W_0, one needs to apply *2.2 V* to V_{Heat} and then V_{Field1} and V_{Field2} *3.3 V* and *0 V*, respectively. Likewise, a certain W_1 needs to apply *3.3 V*, *0 V*, and *2.2 V* to V_{Heat}, V_{Field1}, and V_{Field2}, respectively. The duration of these three signals, T_{Heat}, T_{Field1}, and T_{Field2} 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" (CW_0) and "Certain Write 1" (CW_1). The requirement of the read (R) operation are $V_{Field1} = V_{Field2} = 0\ V$, $V_{Heat} = 0.3\ V$, and $T_{Heat} = 30\ ns$.

In the proposed PUF, we use CW_1 and then the "Uncertain Write 0" (UW_0) in which a voltage in the range of *1 V* to *1.8 V* is selected for applying to V_{Heat}. In this case, the probability that a cell has the logic '0' after performing the sequence of CW_1-UW_0 depends on: 1) the selected voltage for Vh_{eat}, 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%*.

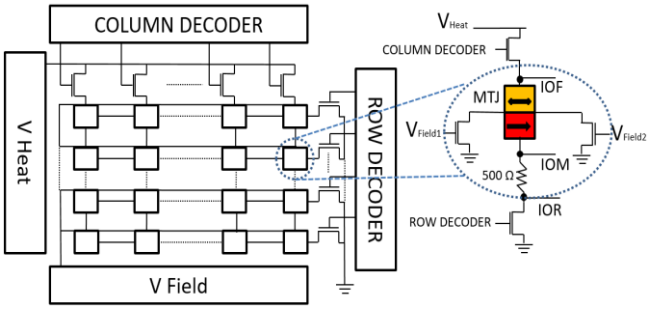


FIGURE4. **The architecture of the employed TAS-MRAM dies, and a memory cell including an MTJ and select transistor**

It is noteworthy that if the CW_0 and CW_1 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 in either of of the P or AP states 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 CW_0/CW_1 operations repeated several times, that MTJ is defective.

IV. EXPERIMENTS AND RESULTS

In our experiments, we employ a Xilinx NEXYS2 FPGA board [23] and a National Instrument acquisition board [24] 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 I^2C protocol. The FPGA sets up adrresses 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 process. Three pads are shown in Fig. 4 and used to read the voltage of the MTJ at the three different points.

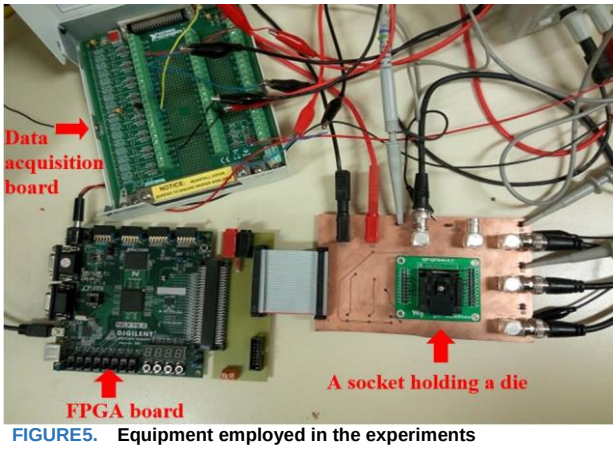


FIGURE5. **Equipment employed in the experiments**

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 CW_1 and CW_0, respectively. As seen in Fig. 6.a, 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. 6.b 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.

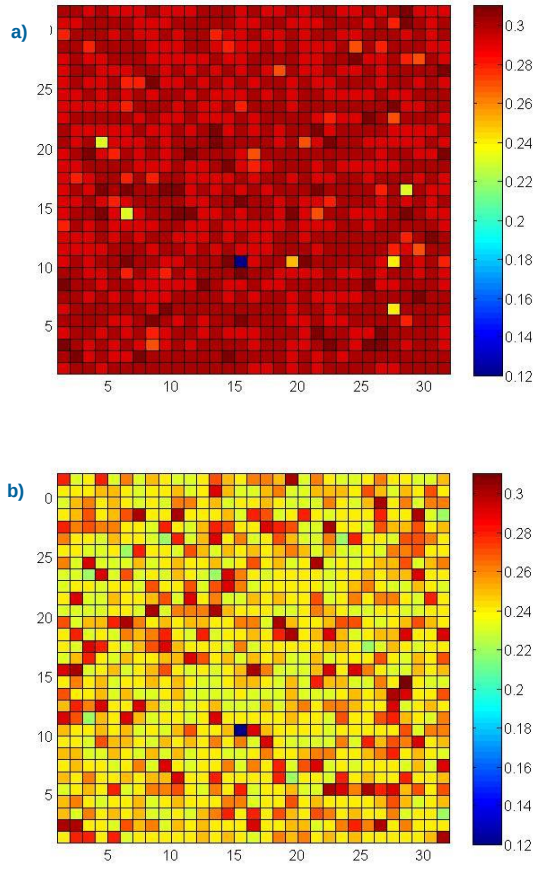


FIGURE6. 32×32 cells in a die, a) applied CW_1 and b) applied CW_0

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 is correspondent 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 CW_1-UW_0.

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 CW_1-UW_0-R is applied to all the cells of 26 dies. Then, *0.1 V* is deduced from the heating voltage and the sequence is repeated. This procedure is continued until the heating voltage reaches 1 V.

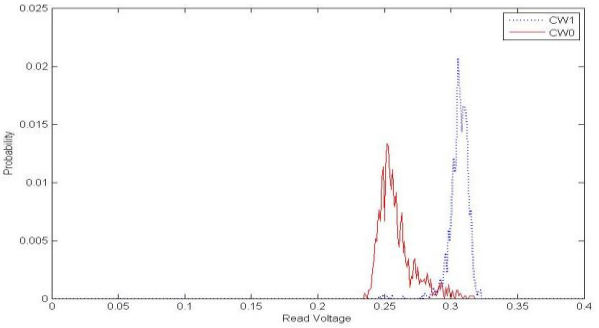


FIGURE7. Probability of the voltage range corresponding to Fig. 6

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 for all the dies are almost *40%-50%*, which is an acceptable range. Fig. 9 shows the average of the inter-PUF variations among the all 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.

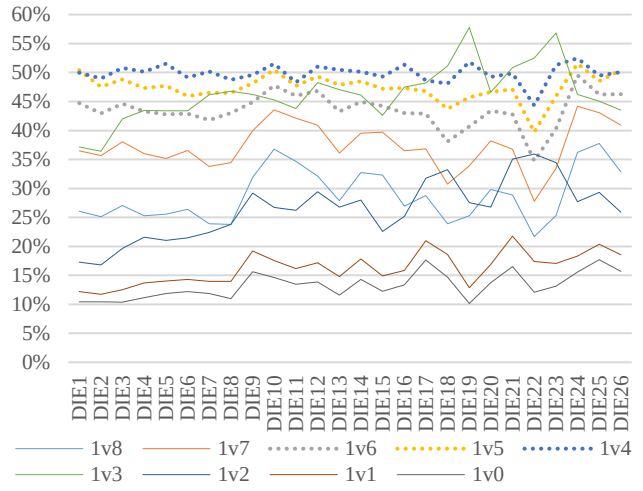


FIGURE8. Inter-PUF variations corresponding to each die for different heating voltages

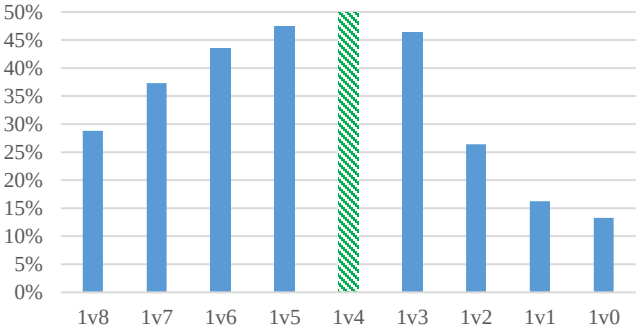


FIGURE9. Average of the inter-PUF variations among all the dies for different heating voltages

The third step in our experiments is to measure intra-PUF variation. For this purpose, the sequence of CW_1-UW_0-R was 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* were 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. Fig. 11 presents the average of the intra-PUF variations among all the dies for 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 [11, 16].

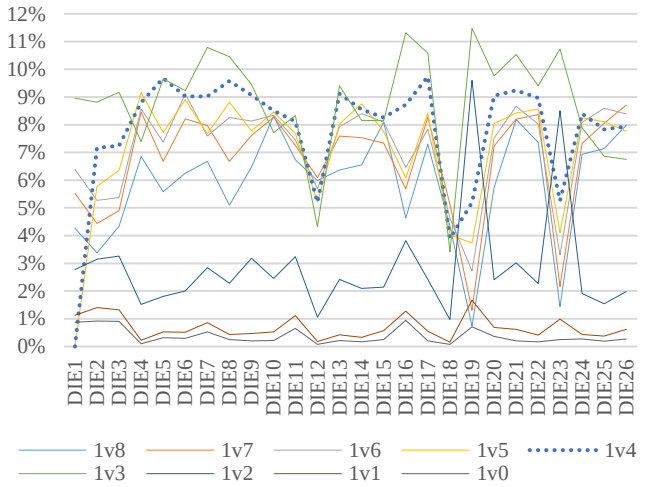


FIGURE10. Intra-PUF variation corresponding to each die for different heating voltages

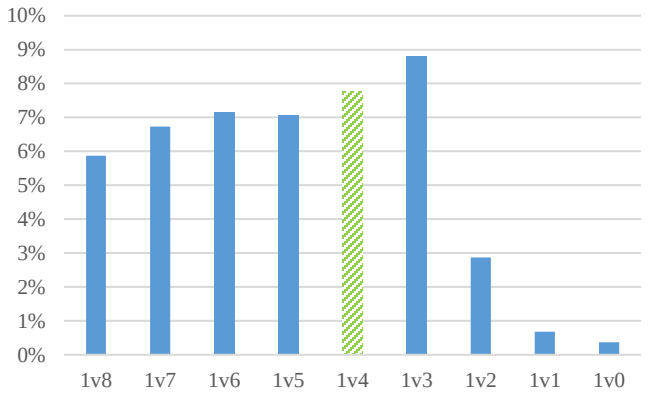


FIGURE11. Average of the intra-PUF variations among all the dies for different heating voltages

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 the figure, the best result (i.e., 0.93) is obtained using the heating voltage of 1.4 V.

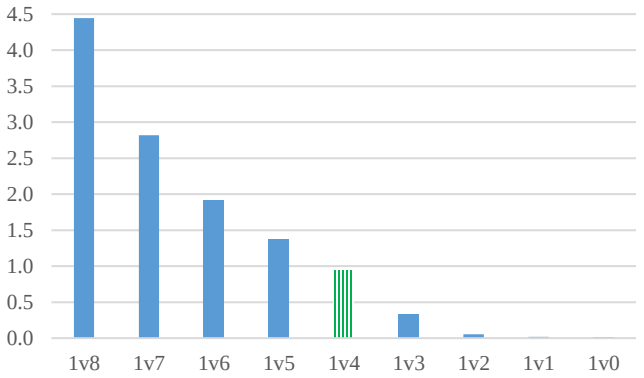


FIGURE12. Average of the uniformity among all the dies for the different heating voltages

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 MRAMs 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 [31-32], but due to its cost it may not be practical or useful for applications such as IoTs. 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 [25].

STT-MRAM offers high density, and consumes almost zero leakage power. This MRAM type is quite mature [26]. 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, applying a spin-transfer torque effect on the storage-(free-)layer magnetization. Therefore, one of the problems with STT-MRAM is the induced disturbance of the storage layer magnetic state during reading [9]. More importantly, different kinds of security attacks have been reported on STT-MRAM-PUFs. For example, in [10], a Correlation Power Analysis on the write operations of an STT-MRAM-PUF was 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 vulnerablilty than STT-MRAM to field disturbance [27]. Although external fields change the resistance state of a cell, the state after the field disturbance goes back to its first state [9, 27].

The results of some of the previous publications on MRAM-PUFs are provided in Table I. The studies were 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 [28-30], 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 [10], the results are based on small-scale experiments on STT-MRAM while our results are based on larger-scale analyses. For using the MRAM-based PUFs in key generation protocols [28-30], it is necessary to employ some error reduction/correction methods for enhancing the 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 [28-30]. 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 propotocls, which are considered as future research. This is because the inter-PUF distances are neer 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 considered as future work.

TABLE I
BASED PUF DESIGNS COMPARISON

MRAM Type	RE	UQ	Ref. #	Simulation Experimental
STT	5.0%	45.83%	[28]	Simulation
STT	2.25%	47 %	[29]	Simulation
STT	1%~10%	~50.1%	[30]	Simulation
STT	0%	~50%	[10]	Experimental
TAS	7.7%	49.8%	This work	Experimental

VI. CONCLUSION

In this work, practical experiments were performed on fabricated TAS-MRAM dies. The experiments included analyzing the efficiency of an implemented PUF on these dies. The major objective of this work was to investigate the stochastic switching behavior in the MTJ cells of the dies as a source of randomness. The experimental results of this work showed 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 on 1 *kbits* 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 TAS-MRAM. The main conclusion is that our suggested circuits can be used to design resilient PUFs with TAS-MRAM.

REFERENCES

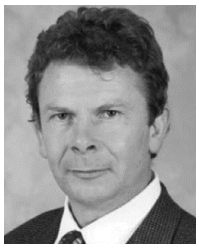
[1] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126-1141, 2014.
[2] Halak, B., Zwolinski, M., & Mispan, M. S. (2016, October). *"Overview of PUF-based hardware security solutions for the Internet of Things,"* In 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS) (pp. 1-4). IEEE.
[3] U. Chatterjee, R. S. Chakraborty, and D. Mukhopadhyay, *"A PUF-based secure communication protocol for IoT,"* ACM Transactions on Embedded Computing Systems (TECS), vol. 16, no. 3, pp. 1-25, 2017.
[4] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, *"A puf taxonomy,"* Applied Physics Reviews, vol. 6, no. 1, p. 011303, 2019.
[5] Garg, A., & Kim, T. T. (2014, June). *"Design of SRAM PUF with improved uniformity and reliability utilizing device aging effec,"*. In 2014 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 1941-1944). IEEE.
[6] Keller, C., Gürkaynak, F., Kaeslin, H., & Felber, N. (2014, June). *"Dynamic memory-based physically unclonable function for the generation of unique identifiers and true random numbers,"* In 2014 IEEE International Symposium on Circuits and Systems (ISCAS) (pp. 2740-2743). IEEE.
[7] Cambou, B., & Orlowski, M. (2016, April). *"PUF designed with Resistive RAM and Ternary States,"* In Proceedings of the 11th Annual Cyber and Information Security Research Conference (pp. 1-8).
[8] Cambou, B., & Orlowski, M. (2016, April). *"PUF designed with Resistive RAM and Ternary States*," In Proceedings of the 11th Annual Cyber and Information Security Research Conference (pp. 1-8).
[9] E. I. Vatajelu, G. D. Natale, M. Barbareschi, L. Torres, M. Indaco, and P. Prinetto, *"STT-MRAM-based PUF architecture exploiting magnetic tunnel junction fabrication-induced variability,"* ACM Journal on Emerging Technologies in Computing Systems (JETC), vol. 13, no. 1, pp. 1-21, 2016.
[10] Y.-S. Chen et al., *"On the hardware implementation of MRAM physically unclonable function,"* IEEE Transactions on Electron Devices, vol. 64, no. 11, pp. 4492-4495, 2017.
[11] 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.
[12] G. Finocchio et al., *"Spin–orbit torque based physical unclonable function,"* Journal of Applied Physics, vol. 128, no. 3, p. 033904, 2020.
[13] C. T. https://crocus-technology.com/. Available: https://crocus-technology.com/
[14] G. E. Suh and S. Devadas, *"Physical unclonable functions for device authentication and secret key generation,"* in 2007 44th ACM/IEEE Design Automation Conference, 2007, pp. 9-14: IEEE.
[15] Che, W., Saqib, F., & Plusquellic, J. (2015, November). *"PUF-based authentication,"* In 2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD) (pp. 337-344). IEEE.
[16] B. Colombier, L. Bossuet, V. Fischer, and D. Hély, *"Key reconciliation protocols for error correction of silicon PUF responses,"* IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1988-2002, 2017.
[17] C.-Y. You and H. Kim, *"Effect of finite tunneling magnetoresistance for the switching dynamics in the spin transfer torque magnetic tunneling junctions,"* IEEE Transactions on Magnetics, vol. 53, no. 11, pp. 1-4, 2017.
[18] B. Jovanović, R. M. Brum, and L. Torres, *"Comparative analysis of MTJ/CMOS hybrid cells based on TAS and in-plane STT magnetic tunnel junctions,"* IEEE Transactions on Magnetics, vol. 51, no. 2, pp. 1-11, 2014.
[19] A. Khvalkovskiy et al., *"Basic principles of STT-MRAM cell operation in memory arrays,"* Journal of Physics D: Applied Physics, vol. 46, no. 7, p. 074001, 2013.
[20] M. El Baraji, V. Javerliac, W. Guo, G. Prenat, and B. Dieny, *"Dynamic compact model of thermally assisted switching magnetic*

tunnel junctions," Journal of Applied Physics, vol. 106, no. 12, p. 123906, 2009.
[21] A. Jaiswal, X. Fong, and K. Roy, *"Comprehensive scaling analysis of current induced switching in magnetic memories based on in-plane and perpendicular anisotropies,"* IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 6, no. 2, pp. 120-133, 2016.
[22] F. Ouattara, A. Nejat, L. Torres, and K. Mackay, *"Practical Experiments on Fabricated TAS-MRAM Dies to Evaluate the Stochastic Behavior of Voltage-Controlled TRNGs,"* IEEE Access, vol. 7, pp. 59271-59277, 2019.
[23] Xilinx: https://www.xilinx.com/products/silicon-devices/fpga.html
[24] National Instrument: https://www.ni.com/fr-fr.html
[25] S. Ghosh, R. V. Joshi, D. Somasekhar, and X. Li, *"Guest Editorial Emerging Memories—Technology, Architecture, and Applications (First Issue),"* IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 6, no. 2, pp. 105-108, 2016.
[26] Y. Chen et al., *"On the Hardware Implementation of MRAM Physically Unclonable Function,"* IEEE Transactions on Electron Devices, vol. 64, no. 11, pp. 4492-4495, 2017.
[27] Senni, S., Torres, L., Sassatelli, G., Gamatie, A., & Mussard, B. (2016). *"Exploring MRAM technologies for energy efficient systems-on-chip,"* IEEE Journal on emerging and selected topics in circuits and systems, 6(3), 279-292.
[28]A. Kumar, S. Sahay, and M. Suri, *"Switching-time dependent PUF using STT-MRAM,"* in 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), 2018, pp. 434-438: IEEE.
[29] J. Das, K. Scott, S. Rajaram, D. Burgett, and S. Bhanja, *"MRAM PUF: A novel geometry based magnetic PUF with integrated CMOS,"* IEEE Transactions on Nanotechnology, vol. 14, no. 3, pp. 436-443, 2015.
[30] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, *"Highly reliable memory-based physical unclonable function using spin-transfer torque MRAM,"* in 2014 IEEE International Symposium on Circuits and Systems (ISCAS), 2014, pp. 2169-2172: IEEE.
[31] Tehrani, S. (2006, December). Status and outlook of MRAM memory technology. In 2006 International Electron Devices Meeting (pp. 1-4). IEEE.
[32] Wu, L., Taouil, M., Rao, S., Marinissen, E. J., & Hamdioui, S. (2020). Survey on STT-MRAM Testing: Failure Mechanisms, Fault Models, and Tests. arXiv preprint arXiv:2001.05463.

ARASH NEJAT received the M.Sc. in computer engineering from Amirkabir University, Iran, in 2012, and the Ph.D. in Nanoelectronic and technologies from Université Grenoble Alpes (UGA), France, in 2019. He is currently doing research as a postdoc at LIRMM, a joint research laboratory between the University of Montpellier and CNRS (French National Center for Scientific Research). His research interests are hardware security; MRAM technologies; and ASIC/FPGA design.

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

MOHAMMAD MOHAMMADINODOUSHAN received the M.Sc. in Electrical Engineering and is currently pursuing his Ph.D. in Informatics and Computing at Northern Arizona University. His past research emphasis was on Renewable Energy Power Systems, including data mining and machine learning, intelligent control, and Power Electronics. His current research emphasis is on Cyber Engineering for Cyber Security, 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.



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

BERTRAND CAMBOU received the Ph.D. from Paris-South (XI) University. Now, he is is a Professor of Practice at Northern Arizona University (NAU). His primary research interests are in cyber-security, and how to apply microelectronics to strengthen hardware security. This includes the design of novel secure elements, Physically Unclonable Functions (PUF), True Random Generators (TRNG), and the usage of nanotechnologies such as ReRAM. He worked in the smartcard/secure microcontroller industry at Gemplus (now Gemalto), and in the POS/secure payment industry at Ingenico. He spent 15 years at Motorola Semiconductor (now NXP-Freescale) where he served in multiple capacities including CTO and was named "Distinguished Innovator" and scientific advisor of the BOD. In the last 5 years, he worked as CEO in Silicon Valley in the high tech industry where his organization won a contract with IARPA with applications related to quantum cryptography. He is the author and co-author of 42 patents in microelectronics and cybersecurity.

LIONEL TORRES received the M.Sc. and Ph.D. from the University of Montpellier, in 1993 and 1996, respectively. From 1996 to 1997, he was an IP Core Methodology Research and Development Engineer with ATMEL. From 1997 to 2004, he was an Assistant Professor with Polytech Montpellier and Microelectronics (LIRMM), University of Montpellier. From 2007 to 2010, he was the Head of the Microelectronic Department, LIRMM, where he has been a Full Professor, since 2004. He is currently the Deputy Head of Polytech Montpellier, where he is in charge of research, industrial, and international relationship. Since 2015, he has been the Head of the Cluster of Excellence NUMEV (Digital and Hardware Solutions and Modeling for the Environment and Life Sciences). He has co-authored over 50 journal papers and 150 conference publications. He holds 10 patents. His research interests include system level architecture, with a specific focus on the security and cryptographic applications and nonvolatile computing based on emerging technologies. He leads several European, national, and industrial projects in these fields.