Exploring the impact of functional test programs re-used for power-aware testing

Aymen Touati, Alberto Bosio, Luigi Dilillo, Patrick Girard, Arnaud Virazel, Paolo Bernardi, Matteo Sonza Reorda

STT MRAM-Based PUFs

Elena Ioana Vatajelu[1], Giorgio Di Natale[2], Marco Indaco[1], Paolo Prinetto[1]
[1]Politecnico di Torino, Dip. di Automatica e Informatica, Turin, Italy
[2]LIRMM, Montpellier, France

Abstract — **Physical Unclonable Functions are emerging cryptographic primitives used to implement low-cost device authentication and secure secret key generation. In this paper we propose an innovative design based on STT-MRAM memory. We exploit the high variability affecting the electrical resistance of the MTJ device in anti-parallel magnetization. We will show that the proposed solution is robust, unclonable and unpredictable.**

***Index Terms*—Physical Unclonable Functions PUFs, MRAMs, Emerging Memory Technology, Security**

I. INTRODUCTION

Physical Unclonable Functions (PUFs) are emerging cryptographic primitives, used to implement low-cost device authentication and secure secret key generation. PUFs exploit intrinsic manufacturing variability of the CMOS fabrication process to generate a signature unique to each single device. In order to rely on this signature, the generated value for the same device must be robust with respect to aging and environmental variations (temperature, voltage noise, electromagnetic interferences). To guarantee the stability of the signature, existing solutions exploit fuzzy extractors and error correction codes.

One of the most investigated solutions uses SRAMs, since they provide high security (i.e., high inter-chip variation) and high stability (i.e., low intra-chip variation). Commercial devices and state-of-the-art studies exist for current SRAM CMOS technologies. Nevertheless, very few studies exist for PUFs based on emerging memory technologies. While there are some proposals exploiting resistive memories [1][2][3], only one solution has been so far proposed for magnetic memories [4]. However, this solution uses a non-standard memory design, where 2 storage cells are used for one bit.

In this paper we propose a PUF design based on the Spin-Transfer-Torque Magnetic memories (STT-MRAMs). The proposed PUF solution is robust, unclonable and unpredictable. To prove the robustness of our proposed PUF, we show that the signature generated for a same device under different conditions (temperature and voltage variations) matches with a high probability. Our PUF solution is unclonable and unpredictable since it is based on fabrication-induced variability (which cannot be controlled, not even by the manufacturer, hence resulting in unclonable devices) and we show that the PUFs generated for different devices exhibit high mismatch probability.

This paper is organized as follows. In Section II, we present the basic characteristics and operation principles of the STT-MRAM memory. In Sections III and IV, we present the principle underlying the PUF architecture and some simulation results, respectively. Section V concludes the paper.

II. STT-MRAM TECHNOLOGY

In Spin-Transfer Torque Random Access Memories (STT-MRAMs), information is stored into devices called Magnetic Tunneling Junction (MTJ). An MTJ is usually composed of two ferromagnetic layers separated by one oxide barrier. One ferromagnetic layer has a pinned magnetization direction (*fixed ferromagnetic* layer). The magnetization direction of the second ferromagnetic layer is unpinned (*free ferromagnetic* layer) and can be flipped by forcing a sufficiently large spin polarized current through the device. The relative Magnetization Directions (MDs) of the two ferromagnetic layers determine the electrical resistance of the MTJ device. When the magnetization directions of the two layers are parallel, the MTJ device exhibits low electrical resistance (R_L), while when they are anti-parallel, the MTJ device exhibits high electrical resistance (R_H) [5]. As depicted in Fig. 1(a), the parallel and the anti-parallel magnetizations are conventionally used to represent the logic states '0' and '1', respectively.

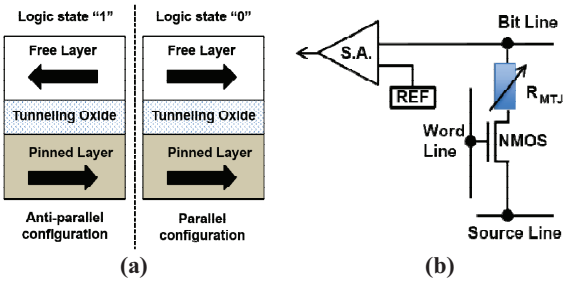

Fig. 1. The STT-MRAM Memory cell: a) MTJ configurations; b) Electric circuit of 1T1MTJ structure

Several STT-MRAM cell implementations have been proposed. In this work we target the popular 1T1MTJ structure. In this topology, the memory cell consists of one MTJ device connected to one NMOS transistor in series. The cell is accessed by the corresponding control lines, i.e., Bit Line (BL), Source Line (SL) and Word Line (WL). The MTJ is modeled as a variable resistor. The equivalent electric circuit is provided in Fig. 1(b).

The magnetic state of the MTJ device can be changed by applying a current (I_{MTJ}) able to switch the magnetic orientation of the free-layer. The value of such a current depends on the physical dimensions of the cell and the materials used, the temperature of the device while the operation is performed, and the duration of the applied voltage signal. For a write '0' operation (W0), the Bit Line (BL) is charged to V_{DD} (power supply voltage) while the Source Line (SL) is grounded. The voltage between BL and SL generates a current flow through the MTJ device (I_{MTJ}). If this current is larger than the threshold switching current I_{HL}, the cell

switches to the parallel state. For a write '1' operation (W1), interchanging voltages between BL and SL forces the cell to switch to the anti-parallel state. Manufacturing process parameter variations and non-uniformity of materials introduce cell-to-cell electrical parameter variations. Therefore, in the case of a memory array, the write current is statistically distributed around its nominal value, as shown in Fig. 2.

To perform a read operation, a small voltage (for instance 20% of V_{DD}) is applied to the BL, while the SL is grounded. The bias during read should be small enough not to disturb the data stored in the cell, and large enough for correct sensing. When the voltage is applied, a current proportional to its electrical resistance flows through the MTJ device (I_R), . If the cell stores '0' (resp. '1'), i.e., the MTJ is in parallel (resp. anti-parallel) magnetization, its electrical resistance is low (resp. high), hence the current (I_{R0}) is high (resp. low). Manufacturing process parameter variations introduce variability in the values of both resistance low (R_L) and high (R_H) and also in the access transistor, resulting in read current variation from cell to cell (as shown in Fig. 2).

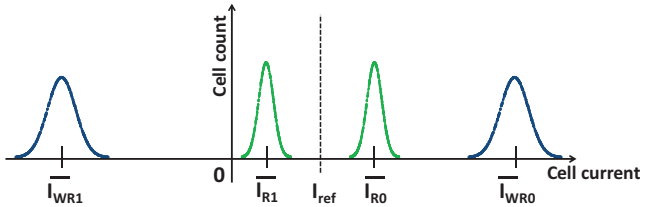

Fig. 2. Distribution of characteristic currents in STT-MRAM array (green/blue curves for reading/writing operations).

Read operations are performed by using a Sense Amplifier (Fig. 1(b)) where the reading current (I_R) is compared against a reference value (I_{ref}). Fig. 2. illustrates the distribution of the currents generated during read operations in case of stored '0' (with average $\overline{I_{R0}}$) or '1' (with average $\overline{I_{R1}}$). The I_{ref} current indicates the discriminating reference current that separates the two states. For a reliable read operation, the reference current is set to be equally apart from the nominal values of I_{R0} and I_{R1} (i.e., $I_{ref}=(\overline{I_{R1}}+\overline{I_{R0}})/2$) to assure maximum sensing margins for both logic states. If $I_R > I_{ref}$, this translates in a read '0' operation (R0), while if $I_R < I_{ref}$ it translates in a read '1' operation (R1).

The reference current can be obtained by using reference cells whose MTJ elements are identical to the ones of the cells to be read (therefore affected by the same fabrication variability), as shown in Fig. 3 [6]. The equivalent reference resistance is obtained by averaging the low and the high resistances of the MTJ devices. In order to reduce the effect of variability on I_{ref}, a larger number of reference cells are used. These cells are spatially distributed and interleaved with the active cells to capture the variability profile of the memory array, thus maximizing the probability that the reference current (I_{ref}) is equally apart from the read currents $\overline{I_{R0}}$ and $\overline{I_{R1}}$, respectively.

In the next section, we describe a novel solution for STT MRAM-based PUF.

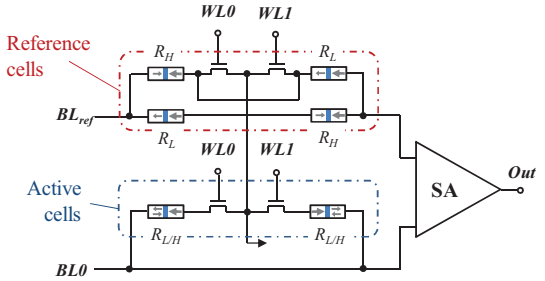

Fig. 3. - STT-MRAM differential reading schemes: the reference current is provided by averaging the current passing through standard MTJ devices in both parallel and anti-parallel configuration

III. Proposed Methodology

The electrical characteristics of an STT-MRAM bit-cell are strongly affected by the fabrication process, having a direct effect on the value of the MTJ resistance.

In our solution we resort to a memory array consisting of *N active cells* (to generate the PUF value), and *M reference cells* (to generate the reference current for read operations). Since the active and the reference cells have the same design characteristics and are fabricated in the same way, they are similarly affected by variability. Also, the references cells are interleaved with the active cells to further assure similar variability under stated environmental conditions. Our solution exploits the differential sensing during read operation, based on read current comparison against a reference value. The proposed solution is implemented as follows (see Fig. 4):

1. *Write all cells to '1':* all cells (active and reference) are set to anti-parallel magnetization. As a result, due to fabrication variability, both the active and the reference cells are characterized by high electrical resistance, with random values distributed around the nominal, resulting in random values for the read current (I_R). The reference current (I_{ref}) is generated by averaging the current flowing through the reference cells during the read operation. Since also reference cells are set all to '1', its value will be close to $\overline{I_{R1}}$.
2. *Read each cell*: all active cells are read. This operation is performed the same way a standard differential read operation is performed, i.e., by comparing the current passing through the active cell (active current: I_R) with the reference current (I_{ref}). Even if all cells are set to '1', (statistically) half of them will be read as '0' since the reference current is approximately equal to $\overline{I_{R1}}$.
3. *Get the PUF value:* the PUF value is read at the output of the sense amplifiers.

A PUF solution is considered *robust* if, after each run of the algorithm on a same device, the obtained result matches with high probability. Since the MTJ and access transistor parameter values are set by fabrication, the read current distribution (I_R) and the reference current (I_{ref}) are the same for one device operated under the same conditions at each run. However, due to the unavoidable and unpredictable noise in the circuit, there is an uncertain sensing zone for the sense amplifier. The bits falling in this zone, i.e. the bits for which

$|I_R-I_{ref}|$ is smaller than the sensing margin of the SA, can induce a meta-stable state, which will be randomly stabilized to '0' or '1' depending on the noise in the circuit. These cells can be read randomly as '1' or '0' at different runs of the algorithm, and are denoted as nondeterministic active cells in Fig 4. To reduce the probability of such occurrences, we use a 3-stage sense amplifier (first stage for current sensing and the other two for voltage sensing), which is designed to counteract the effect of fabrication variability.

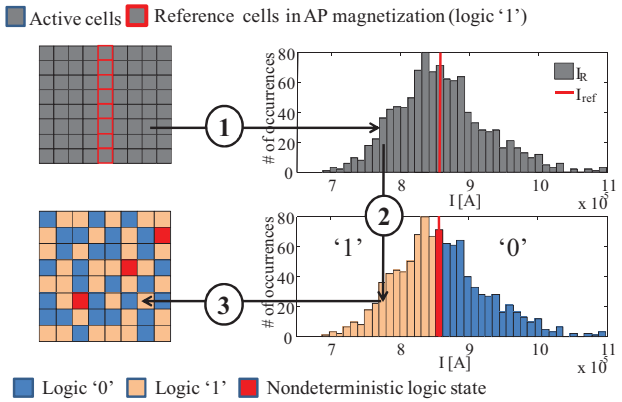

Fig. 4. The implementation strategy of the proposed PUF solution: 1) Write all cells to '1'; 2) Read each cell; 3) Use the read value

In the next section we describe statistical simulation results, which demonstrate the robustness and the unpredictability of the proposed PUF solution.

IV. Results

The relevant geometrical and electrical parameters of an STT-MRAM bit-cell are extracted from literature [7][8][9]. Our solution has been implemented and simulated in SPICE, using Matlab for statistical data generation and data processing. The robustness and the unpredictability of the PUF solution are extracted from these simulations.

The robustness of the PUF is measured by computing the *Hamming Distance* between the signatures obtained after different runs of the *same* PUF. Ideally, the *Hamming Distance* for robustness (HD_R) should be *0*; however, small numbers (*fractional* HD_R*<10%* in the case of SRAM-based PUFs) are accepted since error-correcting codes can be implemented at low cost.

We evaluated the unpredictability of the PUF by computing the *Hamming Weight* (*HW*) and the *Hamming Distance* between the signatures obtained from *different* PUFs. Ideally the PUF should exhibit bias neither towards 0 nor 1, i.e., the *fractional Hamming Weight* of one response should be *0.5*. The *fractional Hamming Distance* (HD_U) between two responses should be *0.5*, since this value allows for the maximum number of different responses.

For the robustness estimation, we run the same STT-MRAM-based PUF 100 times with different noise seeds; for the unpredictability estimation we evaluated 5000 samples of our STT-MRAM-based PUF. These statistical analyses yield statistically distributed Hamming metrics. Therefore, our robust and unpredictable STT-MRAM-based PUF has to meet the following specifications:

- *Fractional Hamming distance* for *robustness:*
  $\mu(fHD_U)$ *very small;* $max(fHD_R)<10\%$
- *Fractional Hamming weight*
  $\mu(fHW)\simeq 0.5$, $\sigma(fHW)$ *very small*
- *Fractional Hamming distance* for *unpredictability:*
  $\mu(fHD_U)\simeq 0.5$, $\sigma(fHD_U)$ *very small*
  $min(fHD_U)> max(fHD_R)$

where μ(.) represents the mean value of the distribution and σ(.) its standard deviation.

Simulation results show that the number of active and reference cells have a strong impact on the resulting PUF characteristics, as depicted in Fig. 5. We have evaluated the three fractional Hamming metrics for different combinations of *N* (number of active cell) and *M* (number of reference cells) values. The resulting *box-and-whiskers plots* of the statistically distributed fractional Hamming metrics show significant differences between the different PUFs, both in robustness and unpredictability.

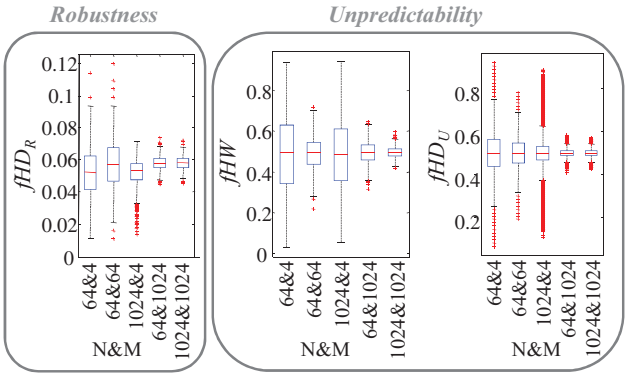

Fig. 5. Box-plots of the hamming metrics distributions for PUF robustness and unpredictability evaluation for different circuit sizing (with N the number of active cells and M the number of reference cells).

The mean value of the fractional Hamming distance for robustness (fHD_R) is affected primarily by the number of reference cells, while its standard deviation is affected by the number of both active and reference cells. The mean values of the fractional Hamming distance for unpredictability (fHD_U) and fractional Hamming Weight (*fHW*) are approximately constant, while their variances are affected by the number of both active and reference cells.

We have performed an analysis to identify the minimum array size that guarantees the robustness and unpredictability of our PUF solution. Several combinations of active & reference bit-cells have been simulated and the appropriate combination identified, as presented in the next subsections.

A. Optimum Memory Array Size

Table II summarizes the results obtained for the different array sizes. The minimum array size for which the conditions for reliable and unclonable weak PUF are met is *N=64*, *M=64* (marked in blue in Table I). However, this design would be very sensitive to any additional noise that may affect its operation, since there is just a small distance between $max(fHD_R)$ and $min(fHD_U)$. A better option, relies on designing the PUF using *N=256* active cells and *M=64*

reference cells (marked in green in Table I). This solution guarantees the reliability and the unpredictability of the PUF with sufficient margins for additional noise and relatively low percentage of bits to be corrected to assure signature uniqueness.

TABLE I. SELECTED RESULTS FOR PUF ROBUSNTESS AND UNPREDICTABILITY

N	M	fHD_R [%]			fHD_U [%]			fHW [%]	
		μ	σ	max	μ	σ	min	μ	σ
16	4	5.16	2.95	***12.5***	49.98	13.9	***0***	48.94	21.4
16	16	5.69	3.01	***18.7***	49.97	12.6	***0***	48.98	15.4
64	4	5.18	1.7	***11.5***	50.01	9.2	***6.25***	49.38	19.3
64	64	5.69	1.6	12	49.99	6.3	15.6	49.62	8.2
256	4	5.19	1.11	***8.6***	49.99	7.1	***6.64***	49.27	18.1
256	16	5.67	0.87	8.1	50.01	3.7	33.6	49.37	10.5
256	64	5.77	0.81	7.6	50.01	3.2	33.6	49.45	6.2
256	256	5.77	0.79	8.9	50.01	3.1	35.6	49.66	4.4
512	64	5.77	0.57	7.7	50.01	2.3	39.5	49.6	5.51
512	256	5.78	0.58	7.7	50.01	2.2	39.8	49.7	3.65

B. *Impact of environmental variations*

While the environmental variations have little effect on the unpredictability of the PUF solution, they can have an important effect on its robustness. One of the main features of our PUF solution consists in generating the reference current for read operation using reference cells interleaved with the active cells. This has the great advantage of having the reference cells affected by environmental variations in the same way as the active cells.

1) *Supply voltage variation*

A supply voltage variation of ±10% while writing the STT-MRAM cell has little effect on the electrical characteristics of the MTJ, since the duration of the write pulse is sufficiently large to guarantee that the MTJ acquires enough energy for switching the magnetization direction of the free ferromagnetic layer.

On the other hand, variations of the supply voltage affect the read operation from two directions. First, the read current (I_R) and the reference current (I_{ref}) are directly proportional with the Bit Line voltage ($20\%V_{DD}$). Therefore, decreasing the supply voltage causes a drop of the resulting currents. Since the active and reference cells are interleaved, they are equally affected by this variation. Consequently, the distributions of both I_R and I_{ref} change in the same way, resulting in similar differential current to be fed to the sense amplifier. Second, the supply voltage directly affects the behavior of the sense amplifier, more specifically its sensing margin decreases when the supply voltage decreases. This directly affects the number of nondeterministic bits during read operation, hence the PUF robustness.

The results show that under $\pm 10\%V_{DD}$ variation, the distributions of fractional Hamming weight (fHW) and Hamming distance for unpredictability (fHW_U), remain practically unchanged, whereas the distribution of the fractional Hamming distance for robustness (fHD_R) experience some variations (as illustrated in Fig. 6).

2) *Temperature variation*

Temperature (T) variation during write operation leads to variations of MTJ device electrical resistance in anti-parallel state (R_H). The R_H-T dependence is linear (R_H decreases with increasing T) [10] and it is the same for all the cells in the circuit. This causes the distributions of both R_H and R_{ref} to change in the same way, resulting in similar differential current to be fed to the sense amplifier.

We have evaluated the robustness metrics under threshold voltage variation and different temperature conditions for two designs: (*N=64 & M=64*) and (*N=256 & M=64*). The results are summarized in Fig. 6. We observe that the effect of supply voltage variations on the PUF robustness is larger than that of temperature variations. This is due to the fact that the main source of non-robustness is the number of nondeterministic bits, which is strongly affected by voltage variations.

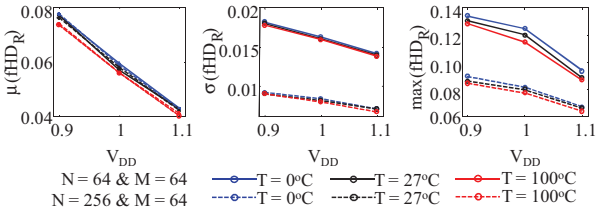

Fig. 6. PUF robustness metrics estimated for 2 circuit configurations operating under various conditions of temperature and supply voltage variation.

V. CONCLUSION

In this work we proposed a novel PUF solution based on the emerging STT MRAM memory. Our solution takes advantage of the high variability affecting the electrical resistance of the MTJ device in anti-parallel magnetization and the peculiarity of the reading operation. We show that the STT-MARM-based PUF is a promising solution for secret key generation since statistical simulations demonstrate high robustness, unpredictability, and limited sensitiveness to environmental variations.

REFERENCES

[1] P. Koeberl, Ü, et al., "Memristor PUFs: a new generation of memory-based physically unclonable functions", In Proceedings of the Conference on Design, Automation and Test in Europe (DATE '13). Dresden, Germany, pp. 428-431.

[2] G. S. Rose, et al., "Foundations of Memristor Based PUF Architectures," NANOARCH, July 2013.

[3] W. Che, J. Plusquellic, S. Bhunia, "A Non-Volatile Memory Based Physically Unclonable Function without Helper Data", ICCAD'14

[4] Le Zhang, et al. "Highly reliable memory-based Physical Unclonable Function using Spin-Transfer Torque MRAM". ISCAS 2014:2169-2172, June 2014.

[5] M. Hosomi, et al., "A novel nonvolatile memory with spin torque transfer magnetization switching: spin-ram," in IEEE International Electron Devices Meeting IEDM Technical Digest 2005, pp. 459–462.

[6] M. Durlam, et al., "A 1-Mbit MRAM based on 1T1MTJ bit cell integrated with copper interconnects," IEEE Journal of Solid-State Circuits, 2003, vol.38, no.5, pp.769-773.

[7] R. Ubal, J. Sahuquillo, S. Petit, H. Hassan, P. Lopez, "Leakage Current Reduction in Data Caches on Embedded Systems," Intelligent Pervasive Computing Conference (IPC), 2007, pp.45-50

[8] L. Jing, L. Haixin, S. Salahuddin, K. Roy, "Variation-tolerant Spin-Torque Transfer (STT) MRAM array for yield enhancement," IEEE Custom Integrated Circuits Conference (CICC), 2008, pp.193-196.

[9] S. Zhenyu, L. Hai, C. Yiran, W. Xiaobin, "Variation tolerant sensing scheme of Spin-Transfer Torque Memory for yield improvement," IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2010, pp.432-437.

[10] X. Bi, H. Li, X. Wang, "STT-RAM Cell Design Considering CMOS and MTJ Temperature Dependence, " IEEE Transactions on Magnetics, 2012, vol.48, no.11, pp.3821-3824.