Practical Experiments on Fabricated TAS-MRAM Dies to Evaluate the Stochastic Behavior of Voltage-controlled TRNGs

Frédéric Martial Ouattara, Arash Nejat, Lionel Torres, Ken Mackay

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 4, 2019, accepted March 6, 2019, date of current version May 17, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2907186

Practical Experiments on Fabricated TAS-MRAM Dies to Evaluate the Stochastic Behavior of Voltage-Controlled TRNGs

FREDERIC OUATTARA[1], ARASH NEJAT[1], LIONEL TORRES[1], AND KEN MACKAY[2]
[1]LIRMM, University of Montpellier, CNRS, 34095 Montpellier, France
[2]Crocus Technology, 38025 Grenoble, France

Corresponding author: Frederic Ouattara (frederic.ouattara@lirmm.fr)

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

ABSTRACT Noises exist in digital circuits can be leveraged as the source of entropy to design true random numbers generators (TRNGs), which is an important primitive component in cryptography and hardware-based security applications. In this paper, we present practical experiments and results of a TRNG implemented on magnetic random-access memory (MRAM) dies, fabricated by the thermally-assisted-switching MRAM (TAS-MRAM) technology. We, first, explain how one can find out a heating voltage value using that writing operations in the TAS-MRAM dies have a stochastic behavior. Then, we propose an improvement based on a feedback loop from being generated random bits. It helps to adjust the founded heating voltage value for writing operation with the aim of reaching the maximum entropy. Finally, we report the results of some post-processing methods, which are usually required in TRNGs to successfully pass the statistical test of NIST SP-800. The results show that one can generate random numbers with a high quality of randomness using the proposed TRNGs besides simple post-processing methods.

INDEX TERMS True random number generator, magnetic RAM, thermally-assisted-switching MRAM.

I. INTRODUCTION

Random numbers generators (RNGs) are a primitive component in cryptography, hardware-based security, statistical sampling, stochastic simulations such as Monte Carlo methods, etc. [1], [2]. RNGs are categorized into pseudo RNGs (PRNGs) and true RNGs (TRNGs). As the word pseudo in the name of PRNG implies, such generators do not literally output random numbers [3]. PRNGs include a deterministic algorithm and generate a sequence of numbers while applying a randomly chosen seed. One can certainly find out the output of a PRNG if its algorithm and using seed are revealed. Contrariwise, TRNGs generate truly random numbers. They take advantage of fluctuation of physical phenomena that usually appear as statistically random ''noise'' signals such as thermal noise, meta-stability, etc. [4]. The stochastic nature of such phenomenon makes them non-deterministic and unpredictable.

An important source of noise in integrated circuits (ICs) is the inaccuracy of their fabrication process, the so-called process variation [5]. This source can be leveraged to design TRNGs because it varies physical properties and, consequently, electrical/magnetic characteristics of a device in each of its fabricated instance. For instance, one important feature of a magnetic tunnel junction (MTJ) device in magnetic random-access-memory (MRAM) circuits is switching threshold voltage (Vth), which is the minimum voltage required to change the state of an MTJ [6]. Due to process variation, MTJ physical attributes (such as tunneling oxide thickness and cross-sectional area) and consequently the Vth in each MTJ of a fabricated MRAM is slightly different. This variability causes stochastic switching behavior in MTJs while applying a current equal to the theoretically calculated Vth.

As matter of fact, MRAMs will be dominant non-volatile memories in near future since MRAM prototypes have shown promising properties such as non-volatility, low fabrication cost, high speed, low power consumption, high reliability, etc. [7]. Therefore, researchers have studied different TRNGs designed and implemented using MRAM technologies [8]–[14]. However, most of these studies have been conducted on simulation environments. Despite the valuable knowledge

The associate editor coordinating the review of this manuscript and approving it for publication was Bora Onat.

obtained in these studies, the lack of practical experiments is very tangible.

In this work, we present the analysis and results of a TRNG implemented on some fabricated MRAM dies. The technology of the used dies is thermally-assisted-switching MRAM (TAS-MRAM). In our practical experiments, the stochastic switching behavior of the TAS-MRAM bits is concerned and analyzed while a voltage near to the Vth is used.

The rest of the paper is organized as follows: Section II presents basic background on TRNG and MRAM. Section III represents the materials and methods employed in this work. Section IV explains the experiments and exhibits obtained results. Finally, Section V draws conclusions.

II. BACKGROUND

TRNGs usually include three modules: (1) a traducer makes an electrical signal from a targeted physical fluctuation; (2) an amplifier increases the amplitude of the electrical signal to a measurable level; (3) an analog-to-digital converter (ADC). Each of these modules effects on three main features of a TRNG: throughput, quality of randomness, and ease of integration.

Several fluctuations in different physical parameters of integrated circuits (ICs) make various noise in the form of an electrical signal such as clock jitter, meta-stability, etc. Thus, there is no necessity to design and employ a special traducer in ICs [15].

Analog circuits suffer from various noises, some of which are completely random and appropriate for designing TRNGs. However, employing these circuits imposes to use an amplifier and ADC and, consequently, impedes easy integration [16]. On the contrary, one can eliminate the need for these two modules in digital circuits. For this purpose, those noises must be employed that can stochastically make values in state elements (i.e. flip-flops) of digital circuits. One popular type of digital circuits is MRAM, which these days their usage as the non-volatile memory of system on chips (or on boards) is increasing.

The main device of a memory bit in all MRAM technologies is a magnetic tunnel junction (MTJ). A simple schematic of an MTJ is shown in Fig. 1.b. It consists of two ferromagnetic layers separated by a thin insulating barrier. If this barrier is thin enough, electrons can tunnel from one layer into the other. The resistance of MTJs changes significantly when their ferromagnetic layers have a parallel (P) or anti-parallel (AP) magnetic orientation [17]. This phenomenon is called the Tunnel magnetoresistance (TMR) effect [18]. In other words, TMR causes MTJs to operate like a switch. In fact, if the two ferromagnetic layers of an MTJ have the parallel magnetic orientation the junction resistance is low; in the antiparallel configuration, it is high [19], shown in Fig. 1.a as Rp and Rap.

In each MTJ, one of the two ferromagnetic layers has a fixed magnetic orientation. This layer is usually called pinned layer (PL). Contrary, the other layer, the so-called free layer (FL) has an easy-changeable magnetic orientation.

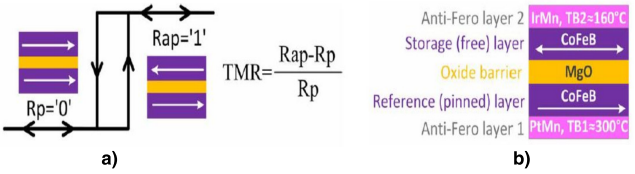

FIGURE 1. a) An MTJ in the parallel and antiparallel state, b) the general schematic of an MTJ device in the TAS-MRAM technology [19].

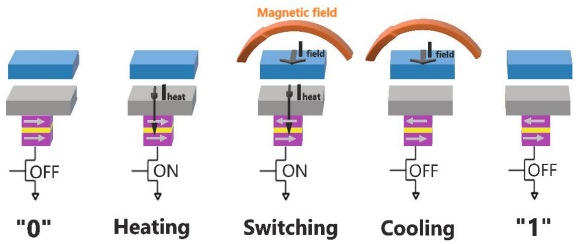

FIGURE 2. Steps of writing "1" in a TAS-MRAM bit holding "0" [20], 1) heating: applying a current (I_{heat}) through the MTJ, 2) switching: applying a current (I_{field}) in order to make a magnetic field while heating, and 3) cooling: stop I_{heat} and maintain I_{field}.

In each MRAM technology, a specific method is designed to change the magnetic orientation of FL. For example, in the spin transfer torque MRAM (STT-MRAM) technology a polarized current is used to change the magnetic orientation of FL [21].

In the TAS-MRAM technology, which is considered and focused in this work, the magnetic orientation of FL is changed by increasing the temperature through the MTJ while applying an external magnetic field. In this technology, one antiferromagnetic layer (AFML) with high blocking temperature (Tb) is adjoined to PL; Another AFML with low Tb is adjoined to FL. The magnetic orientation of FL and PL remains fixed and insensitive to external magnetic fields for temperatures below these blocking temperatures. Fig 1.b shows the schematic of an MTJ device in the TAS-MRAM technology. This MTJ has AFML1 and AFML2 with Tb1 = 300 °C and Tb2 = 160 °C corresponding to the PL and FL, respectively. In order to change the magnetic orientation of the FL in Fig. 1.b, AFML2 must heat up 160 °C. For this purpose, a voltage is applied to TAS-MRAM cells. This voltage is called ''heating voltage'' in literature.

The writing process in a TAS-MRAM cell is depicted in Figure 2. At first, the cell heats up. When it is enough warmed up, its FL becomes ready to store '0' or '1'. Then, a field line current is applied to the cell. The direction of this current determines the direction of the FL. Finally, a short time space is required to cool down the cell by stopping the heating while maintaining the field line current.

Due to process variation, the threshold of the amplitude and duration of the heating voltage is not identical for all the memory bits of a chip. In addition, due to the environmental variation and aging effects, this threshold is not always a fixed value even for a bit. Thus, one needs to use a value

for the heating voltage more than the threshold in order to reliably set/reset a TAS-MRAM cell. Employing a value near to the threshold may cause failures in the set/reset operations. If one can find a value that causes a failure probability of 50%, this value can be used to design a TRNG. However, broadly speaking, having exactly 50% is not practically feasible.

A problem exists in all TRNGs is their bias. A TRNG is called biased if the probability of one or some of its outputs is not equal to the probability of other outputs. In order to remove the bias of TRNGs, several post-processing procedures have been proposed. Two well-known procedures are *Von-Neumann* [22] and *Exclusive OR (XOR)* post-processing [23]. In addition, the authors in [8]-[11] proposed an approach that helps MRAM-based TRNGs generate numbers with less bias. In our experiments and analysis, we used these procedures and approach. In the following, they are briefly explained.

A. VON-NEUMANN PROCEDURE

It is a simple post-processing procedure and results in perfectly unbiased outputs [22]. It consecutively groups the bits of a binary stream in subsequences of non-overlapping pairs and generates outputs as follows:

- If a pair is 00 or 11, it is discarded.
- If a pair is 01 or 10, the output is the first bit of the pair.

Suppose the bits of a given stream have the bias ϵ; this means each bit of the stream has the probability of being '0', P (0), equal to "$0.5+\epsilon$"; and P (1) equal to "$0.5-\epsilon$". This stream as the input of the Von-Neumann procedure results the output 'y' with the probability of being '0' as following:

$$\begin{aligned} \mathrm{P}(\mathrm{y}=0) &= \frac{P(\text{“01”})}{P(\text{“01” } or \text{ “10”})} \\ &= \frac{(0.5-\varepsilon)(0.5+\varepsilon)}{(0.5-\varepsilon)(0.5+\varepsilon)+(0.5-\varepsilon)(0.5+\varepsilon)} = \frac{1}{2} \end{aligned}$$

This is the best result for the output probability. However, the stream output of the Von-Neumann procedure is shorter than its inputs. The length of the output is at most 25% of the length of the raw input stream.

B. XOR PROCEDURE

The probability bias decreases when an XOR operation is performed between two independent bits. Suppose two independent bits 'x_1' and 'x_2' have the probability bias 'ϵ_1' and 'ϵ_2', respectively. The XOR of 'x_1' and 'x_2', "$x_1 \otimes x_2$" has the probability of being '0':

$$\begin{aligned} &\mathrm{P}(\mathrm{x}_1 \otimes \mathrm{x}_2 = 0) \\ &= \mathrm{P}(\mathrm{x}_1 = \mathrm{x}_2 = 0) \text{ OR } \mathrm{P}(\mathrm{x}_1 = \mathrm{x}_2 = 1) \\ &= P\,(\mathrm{x}_1 = 0)\mathrm{P}(\mathrm{x}_2 = 0) + \mathrm{P}(\mathrm{x}_1 = 1)\mathrm{P}(\mathrm{x}_2 = 1) \\ &= (0.5+\epsilon_1)(0.5+\epsilon_2)+(0.5-\epsilon_1)(0.5-\epsilon_2) = 0.5+2\epsilon_1\epsilon_2 \end{aligned}$$

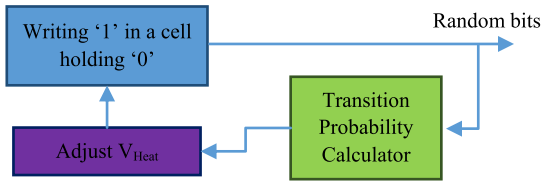

FIGURE 3. Architecture of RTOPT.

Since $\epsilon_1 < 0.5$ and $\epsilon_2 < 0.5$, so $2\epsilon_1\epsilon_2$ is less than ϵ_1 and ϵ_2. In a general case:

$$\mathrm{P}(\mathrm{x}_1 \otimes \mathrm{x}_2 \ldots \otimes \mathrm{xn}) = 0.5 + 2^{n-1} \prod_{i=1}^{n} \varepsilon_i$$

In this procedure, the output bit-stream rate is equal to $\frac{1}{n}$ of the input bit-stream.

C. REAL-TIME OUTPUT PROBABILITY TRACKING (RTOPT)

The authors in [11] proposed the RTOPT approach to generated numbers with less bias. As observed in Fig. 3, this method consists of a feedback from a bit memory cell, probability calculator, and decision unit. As mentioned, in order to design a TRNG based on an MRAM technology, one can try to set (or reset) an MTJ cell using a current or voltage that causes a failure probability of 50% for the set (or reset) operation. In the RTOPT method, the decision block adjusts the value of the current or voltage in the set (reset) operation such that the set (or reset) operations fail with a 50% chance. This method somehow compensates the low rate of the output of the Von-Neumann corrector and XOR post-processing.

III. MATERIALS AND METHODS

A. MATERIALS: TAPE-OUT TAS-MRAM

In our experiments, we employed TAS-MRAM dies designed and fabricated by CROCUS Technology. Each die includes 1K bits arranged in a 32 × 32 array such that each bit is individually addressed and accessed. One of the used die and its holding package is shown in Fig. 4. The architecture of the dies is shown in Fig. 5. IOF, IOM, and IOR are sense pads being used during the read operation. As seen in Fig. 5, IOF is on the top of the MTJ; IOM is connected right below the MTJ, and IOR is between a poly 500 Ω resistance and a select transistor. The total impedance of a cell holding '0' can be changed from Rmin to R_{max} using the write '1' operation (W_1). Likewise, the write '0' (W_0) operation changes the MTJ resistance from R_{max} to R_{min}. The both operations require three voltages: V_{Heat}, V_{Field1}, and V_{Field2}. The first one is needed to locally heat the selected MTJ, whereas the second and third ones allow changing the magnetic orientation of FL in the desired state after heating. In order to have a certain W_0, one needs to apply 2V, 3.3V, and 0V to V_{Heat}, V_{Field1}, and V_{Field2}, respectively. Likewise, the certain W_1 operation needs to apply 2V, 0V, and 3.3V 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

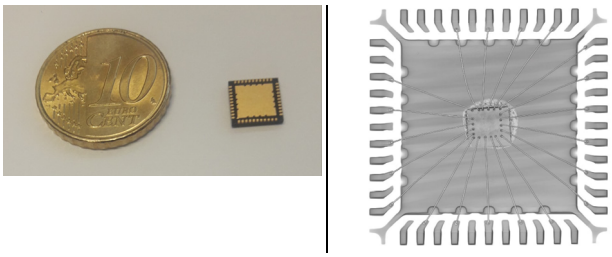

FIGURE 4. QFN44 package (Left) and microscopic picture of the TAS-MRAM die in QFN44 (right).

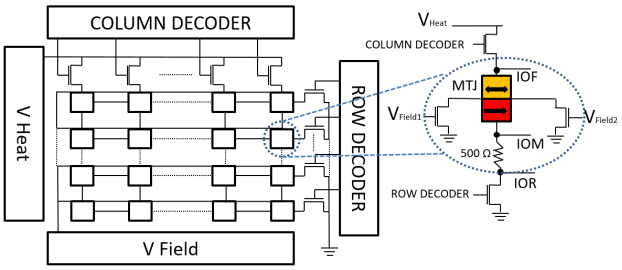

FIGURE 5. Architecture of the employed TAS-MRAM die.

done without any fail. We call these operations "*Certain Write 0*" (CW_0) and "*Certain Write 1*" (CW_1). The read operation need $V_{Field1} = 0V$, $V_{Field2} = 0V$, $V_{Heat} = 0.3V$, and $T_{Heat} = 30$ ns.

B. METHODS: VOLTAGE-CONTROLLED TRNG

In this work, we aimed to explore a Voltage-Controlled TRNG (VC-TRNG) implemented on the TAS-MRAM dies. VC-TRNGs leverage one or some noises on controlling signals designed to set/reset a memory cell. This type of TRNGs can be efficient if noises on controlling signals cause that write operations fail with a probability of 50%.

In the previous section, it was explained that the signals V_{Heat}, V_{Field1}, and V_{Field2} are employed in the TAS-MRAM dies for the W_0 and W_1 operations. In addition, the required properties of these to have the CW_0 and CW_1 operations were introduced. In order to design a VC-TRNG, we use CW_0 and the "*Uncertain Write 1*" (UW_1) in which a voltage in the range of [0V, 2V) is selected for applying to V_{Heat}. In this case, the probability that a cell have '1' after performing the sequence of CW_0-UW_1 depends on (1) the selected voltage and (2) the effects of the process variation on the cell. In order to have an efficient VC-TRNG, one must select a value from the mentioned range such that it results in a failure probability of 50%.

IV. EXPERIMENTS AND RESULTS

A. PRIMARY EXPERIMENT

In order to find out a voltage value by which 50% of the UW_1 operations fail, experiments begin from a test voltage equal to 1V. For this voltage, the sequence of CW_0-UW_1 was executed on an MTJ 10^3 times; and the switching probability, P (1), is calculated. Then, 0.01 V is added to the test voltage and again the 10^3 times the sequence of CW_0-UW_1 is executed. This procedure is continued until the test voltage reaches 2V. The results of this procedure applied to two MTJs of a die are presented in Fig. 6. As observed, the switching probability depends on the value of the heating voltage. It gradually increases for voltages between 1.5V and 1.7V. The difference between the curves in this figure is due to cell-to-cell process variations.

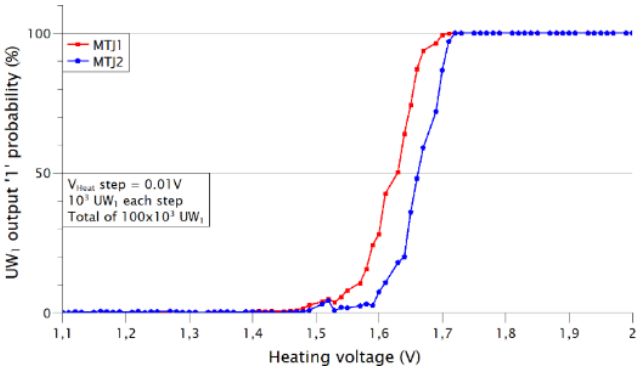

FIGURE 6. TAS MRAM cell switching probability as a function of heating voltage amplitude.

B. EXPLORING TRNG ON A SINGLE MTJ

The results shown in Fig. 6 inform us that a random bit (Rb) with a probability of 50% can be generated by adjusting V_{Heat}. In order to have an efficient TRNG, a switching activity of 50% however is necessary, it is not sufficient. High-quality Rbs require equiprobability of each switching event. In other words, the statistical distribution of the switching probability of Rbs should be the same as the binomial distribution. However, the switching probability fluctuates a lot around the nominal value of P = 50% due to environmental effects such as thermal and voltage fluctuations. Figure 7 shows the histogram of the equiprobability paucity of switching probability for two MTJs, MTJ1 (red) and MTJ2 (blue). For each histogram, 10^7 bits are generated. These bits are gathered in 10^3 groups including 10^4 bits. Each group makes a switching probability value. In the histograms, each point in the x-axis presents a switching probability; and the y-axis shows how many times a switching probability happens among the 10^3 groups. For MTJ1, the mean and the standard deviation are 54.22% and 8.66%; and for MTJ2, these values are 53% and 6.79% respectively. The same experiments on other cells in the dies results (almost) the same as MTJ1 and MTJ2.

C. USE OF POST-PROCESSING PROCEDURES TO ENHANCE OUTPUT PROBABILITY

As mentioned in Section II, the randomness quality of raw Rbs generated by TRNGs can be enhanced using post-processing procedures, like Von-Neumann and XOR ones.

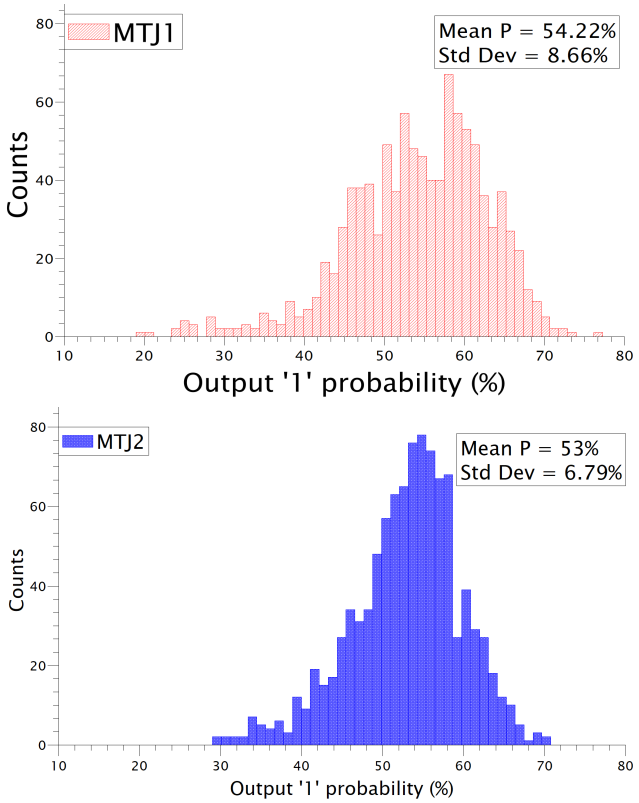

FIGURE 7. Histogram of Switching probability obtained from each 10^4 Rbs from a total of 10^7 Rbs generated by both MTJ 1 (red) and MTJ 2 (blue).

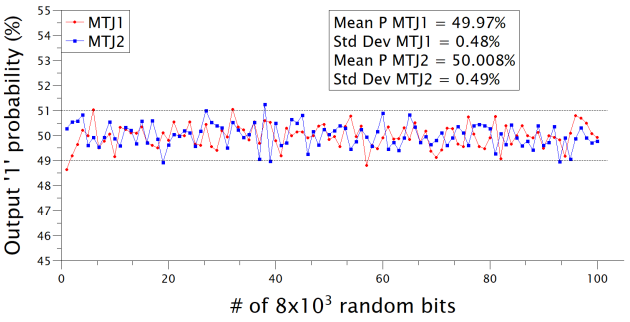

FIGURE 8. Switching probability obtained by performing Von Neumann on the raw Rbs.

Fig. 7 shows that the designed VC-TRNG needs such procedures to obtain high-quality Rbs.

By applying the Von-Neumann corrector to the raw Rbs generated by both MTJ1 and MTJ2, less than $9*10^5$ processed Rbs is obtained from a total of 10^7 raw Rbs generated by each MTJ. The processed Rbs are less than 9% of the initial raw Rbs. Fig. 8 shows the switching probability obtained for each $8*10^3$ Rbs from a total of $8*10^5$ raw Rbs for both MTJ1 (red) and MTJ2 (blue) after the Von-Neumann correction. The mean P value and standard deviations are 49.97% and 0.48% for MTJ1 and 50.008% and 0.49% for MTJ2. As observed, the bias is considerably reduced but the output rate is quite low.

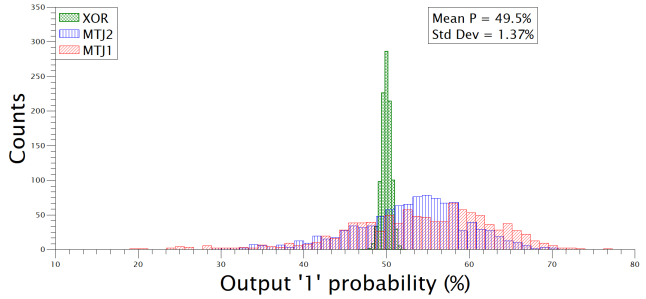

FIGURE 9. Histogram of Switching probability after an XOR post processing on two MTJs (MTJ1 and MTJ2).

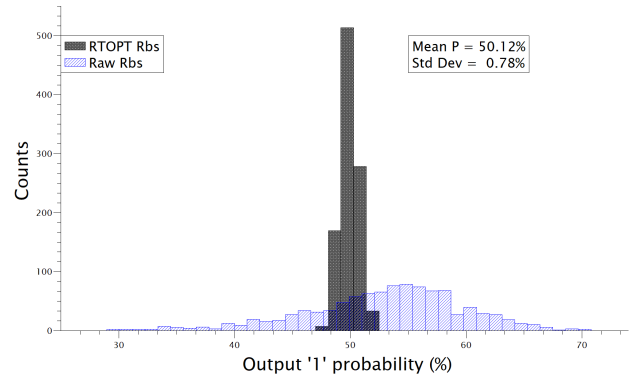

FIGURE 10. Histogram of Switching probability of Rbs generated through an RTOPT (dark) compare to raw Rbs (blue).

Performing one XOR post-processing on the raw Rbs generated by MTJ1 and MTJ2 results in the mean 49.5% and standard deviation of 1.37%. These results confirm a good enhancement provided by an XOR post-processing. The histogram of switching probability is depicted in Fig. 9.

D. USE OF RTOPT TO ENHANCE OUTPUT PROBABILITY

The histogram of switching probability obtained from every 10^4 Rbs from a total of 10^7 Rbs generated by the RTOPT method is shown in Fig. 10. This figure shows the improvement of the distribution. P (1) fluctuate around 47.45% and 52.47% with a mean value of 50.12% and a standard deviation of 0.78%. This compensation method has the advantage of being immune against thermal or voltage fluctuation while keeping the output bit-stream rate to 100% of initial bit-stream.

E. NIST TEST RESULTS

In order to qualify an RNG, the randomness of its generated Rbs is studied. This is done through statistical tests that compare the RNG outputs with those, theoretically, have a sequence of truly Rbs. For instance, the National Institute of Standard and Technology (NIST) has developed a suite of tools available online that can statistically test the randomness

TABLE 1. Result of NIST test on the generated raw Rbs and the outputs of the XOR^2, XOR^3, and Von Neumann.

Test name	Raw Rbs	XOR^2	XOR^3	Von Neumann
Frequency	Fail	Pass	Pass	Pass
Block frequency	Fail	Pass	Pass	Pass
Run	Fail	Pass	Pass	Pass
Longuest Run	Fail	Pass	Pass	Pass
Cumulative Sums	Fail	Fail	Pass	Pass
Binary Rank	Fail	Fail	Pass	Pass
FFT	Fail	Fail	Pass	Pass
Serial	Fail	Fail	Pass	Pass
Approximate Entropy	Fail	Fail	Pass	Pass
Non-Overlapping Template	Fail	Fail	Pass	Pass

TABLE 2. Results of NIST test on the Rbs generated by an RTOPT structure (in column 2), and the XOR^2 function of 4 RTOPT structures (in column 3).

Test name	RTOPT Rbs	XOR^2
Frequency	Pass	Pass
Block frequency	Fail	Pass
Run	Pass	Pass
Longuest Run	Fail	Pass
Cumulative Sums	Fail	Pass
Binary Rank	Fail	Pass
FFT	Fail	Pass
Serial	Fail	Pass
Approximate Entropy	Fail	Pass
Non-Overlapping Template	Fail	Pass

of any RNG [24]. For this purpose, we organize sequences of Rbs as follows:

1) 100 sequences of 10^5 bits generated by a single MTJ (raw Rbs)
2) 100 sequences of 8×10^3 bits obtained by performing the Von Neumann correction on raw Rbs
3) 100 sequences of 10^5 bits generated by RTOPT accompanying a single MTJ
4) 100 sequences of 10^5 bits obtained by XORing 8 MTJs (XOR^3 on Raw Rbs)
5) 100 sequences of 10^5 bits obtained by XORing 4 MTJs in 4 RTOPT architectures (XOR^2 on RTOPT Rbs).

Results are reported in Table 1 and 2. All the 10 applicable tests failed for the initial raw Rbs. However, four of them passed for the Rbs generated after XOR^2. When applying Von Neumann correction or the XOR^3 post-processing procedure, all the tests passed. As a result, one needs to use such post-processing procedures to have a high-quality TRNG based on VC-TAS-MRAM.

RTOPT results better, as seen in Table 2. Two out of 10 tests can be passed no need any post-processing; and in order to pass all the test, one only needs to perform XOR^2.

F. THROUGHPUT

As mentioned in Section II, one important feature for TRNGs is throughput. The throughput of the studied TRNG in this work is determined by the minimum required time to consecutively perform the CW_0, UW_1, and Read operations. Thus, according to the datasheet of the used TAS-MRAM technology, the throughput is calculated to 11 Mb/s. This throughput can be tripled if one uses three TAS-MRAM cells, and make a pipeline for the CW_0, UW_1, and Read operations.

In order to have a fair comparison between the throughput of the TAS-MRAM-based TRNG proposed in this work and that of STT-MRAM-based TRNGs, we chose the works [10] and [12]. In these two works, the CW_0, UW_1, and Read operations were performed on fabricated STT-MRAM dies. Based on the required time for these operations in the STT-MRAM technology, the throughput of the TRNGs in [10] and [12] is about 66 Mb/s.

It is noteworthy to mention that in the STT-MRAM technology, the maximum working frequency is higher than that of TAS-MRAM; nonetheless, the throughput of TRNGs based on these two technologies are in the same decade range. In addition, the TAS-MRAM technology has its own benefits, like the capability of designing Magnetic Logic Unit [25].

V. CONCLUSION

In this work, practical experiments on real dies were performed to analyze the efficiency of a TRNG designed in the TAS-MRAM technology. The stochastic switching behavior in MTJ cells as a source of randomness was the subject of the study. The results showed that the randomness quality of generated raw Rbs is not sufficient to pass standard tests, like NIST. The XOR post-processing or Von Neumann correction enhances the randomness quality which allows passing the NIST test suite. In addition, an adaptive method including feedbacks from being generated Rbs was studied in this work. This method resulted in better than the simple TRNG, and it needed less post-processing procedures. The main conclusion is that one can easily have TRNGs in a circuit if it includes memory elements based TAS-MRAM technology.

VI. ACKNOWLEDGMENT

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

REFERENCES

[1] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC," *IEEE Trans. Comput.*, vol. 52, no. 4, pp. 403–409, Apr. 2003.

[2] R. F. W. Coates, G. J. Janacek, and K. V. Lever, "Monte carlo simulation and random number generation," *IEEE J. Sel. Areas Commun.*, vol. 6, no. 1, pp. 58–66, Jan. 1988.

[3] A. O. Prokofiev, A. V. Chirkin, and V. A. Bukharov, "Methodology for quality evaluation of PRNG, by investigating distribution in a multidimensional space," in *Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus)*, Moscow, Russia, Jan./Feb. 2018, pp. 355–357.

[4] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw, and D. Sylvester, "16.3 a 23mb/s 23pj/b fully synthesized true-random-number generator in 28 nm and 65 nm CMOS," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, vol. 57, Feb. 2014, pp. 280–281.

[5] J. Lorenz *et al.*, "Simultaneous simulation of systematic and stochastic process variations," in *Proc. Int. Conf. Simul. Semicond. Processes Devices (SISPAD)*, Yokohama, Japan, 2014, pp. 289–292.

[6] 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 J. Emerg. Sel. Topics Circuits Syst.*, vol. 6, no. 2, pp. 120–133, Jun. 2016.

[7] T. Kishi *et al.*, "Lower-current and fast switching of a perpendicular TMR for high speed and high density spin-transfer-torque MRAM," in *IEDM Tech. Dig.*, San Francisco, CA, USA, Dec. 2008, pp. 1–4.

[8] A. Fukushima *et al.*, "Spin dice: A scalable truly random number generator based on spintronics," *Appl. Phys. Express*, vol. 7, no. 8, 2014, Art. no. 083001.

[9] Y. Wang, H. Cai, L. A. B. Naviner, J.-O. Klein, J. Yang, and W. Zhao, "A novel circuit design of true random number generator using magnetic tunnel junction," in *Proc. IEEE/ACM Int. Symp. Nanosc. Archit. (NANOARCH)*, Jul. 2016, pp. 123–128.

[10] S. Oosawa, T. Konishi, N. Onizawa, and T. Hanyu, "Design of an STT-MTJ based true random number generator using digitally controlled probability-locked loop," in *Proc. IEEE 13th Int. New Circuits Syst. Conf. (NEWCAS)*, Jun. 2015, pp. 1–4.

[11] W. H. Choi *et al.*, "A magnetic tunnel junction based true random number generator with conditional perturb and real-time output probability tracking," *IEDM Tech. Dig.*, Dec. 2014, pp. 12.5.1–12.5.4.

[12] K. Yang *et al.*, "A 28NM integrated true random number generator harvesting entropy from MRAM," in *Proc. IEEE Symp. VLSI Circuits*, Honolulu, HI, USA, Jun. 2018, pp. 171–172.

[13] Y. Kim, X. Fong, and K. Roy, "Spin-orbit-torque-based spin-dice: A true random-number generator," *IEEE Magn. Lett.*, vol. 6, pp. 1–4, 2015, Art no. 3001004. doi: 10.1109/LMAG.2015.2496548.

[14] E. I. Vatajelu and G. Di Natale, "High-entropy STT-MTJ-based TRNG," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 2, pp. 491–495, Feb. 2019.

[15] M. Ben-Romdhane, T. Graba, J.-L. Danger, and Y. Mathieu, "Design methodology of an ASIC TRNG based on an open-loop delay chain," in *Proc. IEEE 11th Int. New Circuits Syst. Conf. (NEWCAS)*, Paris, France, Jun. 2013, pp. 1–4.

[16] H. Saleem, S. Afzal, and N. Ahmed, "Robust entropy harvester for analogue noise sources in TRNG," in *Proc. 15th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Islamabad, Pakistan, Jan. 2018, pp. 405–414.

[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 Trans. Magn.*, vol. 53, no. 11, Nov. 2017, Art. no. 1400504.

[18] S. Bea, N. Matsushita, S. Zurn, L. Sheppard, E. J. Torok, and J. H. Judy, "Effects of initial layer surface roughness on GMR performance of Si/Cu/NiFe/Cu/Co/Cu/NiFe dual spin-valves for MRAM," *IEEE Trans. Magn.*, vol. 36, no. 5, pp. 2850–2852, Sep. 2000.

[19] 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 Trans. Magn.*, vol. 51, no. 2, Feb. 2015, Art. no. 340011.

[20] S. Senni, L. Torres, G. Sassatelli, A. Bukto, and B. Mussard, "Power efficient thermally assisted switching magnetic memory based memory systems," in *Proc. 9th Int. Symp. Reconfigurable Commun.-Centric Syst.-Chip (ReCoSoC)*, Montpellier, France, 2014, pp. 1–6.

[21] A. V. Khvalkovskiy *et al.*, "Basic principles of STT-MRAM cell operation in memory arrays," *J. Phys. D, Appl. Phys.*, vol. 46, no. 7, 2013, Art. no. 074001.

[22] J. V. Neumann, "Various techniques used in connection with random digits," in *Monte Carlo Method* (National Bureau of Standards Applied Mathematics Series), vol. 12, A. S. Householder, G. E. Forsythe, H. H. Germond, Eds., 1951.

[23] R. Davies. (Feb. 2002). *XOR and Hardware Random Number Generator*. [Online]. Available: http://www.robertnz.net

[24] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST publication, Gaithersburg, MD, USA, Tech. Rep. 800-22rev1a, Apr. 2010.

[25] J. Clément, B. Mussard, D. Naccache, and L. Torres, "Implementation of AES using NVM memories based on comparison function," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Jul. 2015, pp. 356–361.

FREDERIC OUATTARA received the engineering 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, joint the research laboratory between Montpellier University and CNRS (French National Center for Scientific Research). His research interest includes HW security primitives.

ARASH NEJAT received the M.Sc. degree in computer engineering from the Amirkabir University of Technology, Iran, in 2012, and the Ph.D. degree in nanoelectronic and nanotechnology from Université Grenoble Alpes (UGA), France, in 2019. He is currently a Postdoctoral Researcher with CNRS (French National Center for Scientific Research), LIRMM, the joint research laboratory between Montpellier University and CNRS. His research interests include ASIC/FPGA design, MRAM technologies, hardware security, and test and testability.

LIONEL TORRES received the master's and Ph.D. degrees 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 interest includes 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.

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 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.