Thermally Assisted Switching (TAS) MRAM based TRNG

Frédéric Martial Ouattara, Lionel Torres, Ken Mackay

Thermally Assisted Switching (TAS) MRAM based TRNG

Frederic Ouattara[1], Lionel Torres[1], Ken Mackay [2]
[1]LIRMM - CNRS University of Montpellier, 161 Rue Ada Montpellier 34090, France
[2]Crocus Technology Grenoble, 4 place Robert Schuman, 38025 Grenoble Cedex, France
name[1]@lirmm.fr

Abstract

An important building block for many cryptographic systems is a random number generator (RNG). However, RNGs are categorized into two distinct groups: pseudo random number generators (PRNGs) and truly random generators (TRNGs). This work experimentally demonstrates a TRNG based on Thermally Assisted Switching Magnetic Random Access Memory (TAS-MRAM). The heating voltage when writing TAS-MRAM is used to provide the stochastic switching behavior as a source of randomness. XOR post processing are used to performed a good random numbers which passed the statistical test of NIST SP-800 with the appropriate pass rate.

1. Introduction

Random numbers (RNs) are always needed in a wide variety of applications ranging from cryptography and hardware based security to statistical sampling and advanced simulation techniques. According to the manner of generating RNs, random numbers generators (RNGs) are classified in two distinct category : pseudo RNGs (PRNGs) and true RNGs (TRNGs). PRNGs are implemented in software and use deterministic algorithms to generate a sequence of RNs; whereas TRNGs are implemented in hardware and exploit physical elements such as thermal noise, metastability, or oscillator jitter which are non deterministics and unpredictable. However, existing CMOS based TRNGs are often complicated to design and have scalability issues. With the rapid development of non-volatile devices, many novel TRNG designs have been proposed by using memristor [4], phase-change memory (PCM) [3] and magnetic tunnel junction (MTJ) [1],[2]. The stochastic behavior of MTJ have been considered as a promising physical noise source for TRNGs [1],[2]. Compared with the conventional CMOS based TRNGs, the MTJs based TRNGs designs effectively can achieve simplified structure, more compact area, higher speed and better energy-efficiency. This paper presents our experimental study on generating RNs based on Thermally Assisted Switching Magnetic Random Access Memory (TAS-MRAM).

2. Memory architecture and experiemental setup

MRAM cell is based on the magnetic tunnel junction (MTJ) which is composed of two ferromagnetic layers, a reference layer (with a fixed magnetization) and a storage layer (with a freely imposable magnetization) separated by a thin insulator (tunnel barrier). The Tunnel Magnetoresistance (TMR) effect causes the resistance of the MTJ to depend on the relative orientation of the two magnetic layers: the antiparallel state have a resistance larger than the parallel state. It enables the magnetic state of the FL to be sensed thanks to a current flowing through the MTJ. Hence, stored information can be read. In order to switch the orientation of the FL, several methods have been proposed: Toggle, Spin Transfer Torque (STT) [1], Spin Orbit Torque (SOT) [2] and Thermally Assisted Switching (TAS). In TAS method the MTJ is slightly modified by adding two antiferromagnetic (AFM) layers with different (low and high) blocking temperatures. To switch (write) the MTJ, heating current is passed through the MTJ stack to heat the junction above the blocking temperature of the FL. Thus, the FL becomes unpinned and ready to store the non-volatile data determined by an applied external field.
The 1kbits MRAM memory device used in this work was designed by CROCUS Technology and it made of 32x32 array that can be individually addressed. The cell and the test array architecture are depicted in Fig. 1. IOT, IOM and IOR are sense pads used during read. In order to change the resistance value of a memory cell, two differents writing operations are available: Write '0' (W0) and Write '1' (W1). Both operations require two voltages: VHeat is required to locally heat the magnetic material, whereas VField allows changing the magnetic field polarization after heating.

2.1. Experimental study on the heating voltage

We made an exploration to evaluate the impact of heating voltage on writing probability, for that VField was fixed to the maximal value (3.3V) in both writing operations W0 and W1 while VHeat was fixed to 2V when W0 to avoid any writing fail, then keep sweeping from 1.1V

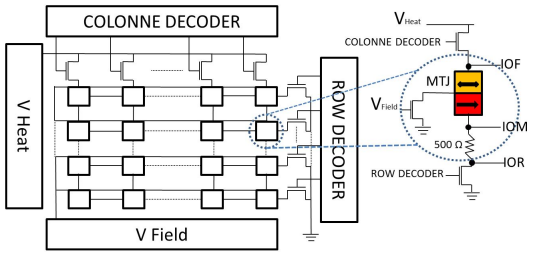

Figure 1. 1Kbits TAS-MRAM cells and its integration into the array tested in this work

to 2V when W1 with $\triangle Vheat = 0.01V$.
For each step of $\triangle Vheat$, 10^3 cycle of W0 and W1 were performed and the probability to have an effective switching when W1 is compute. As shown in Fig. 2 the writing probability gradually increases with increasing heating voltage from 1.5V to 1.7V for both MTJ1 (red) and MTJ2(blue). Thus for a given heating voltage, a writing probability can be associated. The drift of the curve according to the MTJ is due to the cell to cell process variation affecting the resistance values of each MTJ.

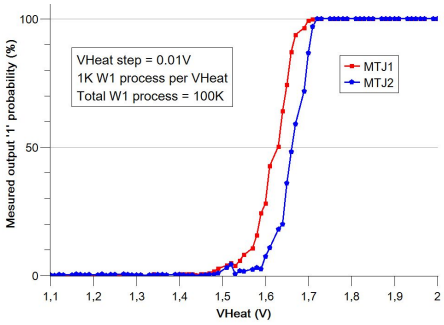

Figure 2. TAS MRAM cell switching probability as a function of heating voltage

2.2. Exploring TRNG on a single MTJ

Based on the results of our experimentation, it seem to be possible to make a TRNG based on Spin Dice [1] which consist to first write the MTJ in one of it state with both VHeat and VField values large enough to be sure to have 100% probability (RESET when W0) then try to write back the MTJ with VHeat and VField aurond 50% of switching (Random switching when W1). The entropy source in this case is the heating voltage when W1. To generate high-quality RNs, equiprobability of each switching event is indispensable. If the probability (P) is exactly equal to 50% for all switching events, the statistical distribution of P of the generated random bits should be the same as the binomial distribution. However, the switching probability fluctuates around the nominal value of P = 50% owing to environmental effects such as thermal and voltage fluctuations. This lack of equiprobability causes the deviation from the binomial distribution. Fig. 3 shows the histogram of the output 1 probability for two differents MTJs, MTJ1 (red) and MTJ2 (blue) obtained for each 10^3 random bits from a total of 10^7 bits and a Xor post processing between these two MTJs which enhance the RNs quality. The RNs generated after Xor post processing on at least 8 MTJs passed all NIST statistically tests [5].

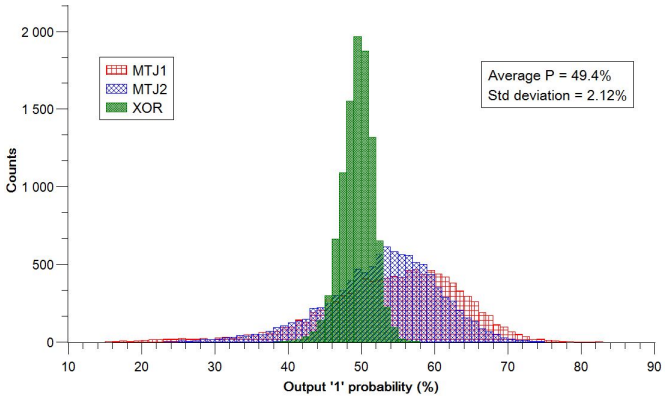

Figure 3. Histogram of output 1 probability after a XOR post processing on two MTJs (MTJ1 and MTJ2)

3. Conclusion

We have presented a simpler way to design TRNG based TAS MRAM by using the stochastic switching behavior provide by the heating voltage when writing the MTJ as a source of randomness. The Xor post processing enhance the quality of random numbers generated that permit to passed the NIST statiscally tests.

References

[1] A. Fukushima, T. Seki, K. Yakushiji, H. Kubota, H. Imamura, S. Yuasa, and K. Ando. Spin dice: A scalable truly random number generator based on spintronics. *Applied Physics Express*, 7(8):083001, 2014.

[2] Y. Kim, X. Fong, and K. Roy. Spin-orbit-torque-based spin-dice: A true random-number generator. *IEEE Magnetics Letters*, 6:1–4, 2015.

[3] E. Piccinini, R. Brunetti, and M. Rudan. Self-heating phase-change memory-array demonstrator for true random number generation. *IEEE Transactions on Electron Devices*, 64(5):2185–2192, May 2017.

[4] V. K. Rai, S. Tripathy, and J. Mathew. Memristor based random number generator: Architectures and evaluation. *Procedia Computer Science*, 125:576 – 583, 2018. The 6th International Conference on Smart Computing and Communications.

[5] A. Rukhin and all. A statistical test suite for random and prng for cryptographic applications. *special publication from NIST 800-22 rev 1a*, April 2010.