Magnetic Memory based secure devices

Frédéric Ouattara, Lionel Torres

Magnetic Memory based secure devices

Frederic Ouattara
LIRMM – UMR CNRS – University of Montpellier
Frederic.Ouattara@lirmm.fr

Lionel TORRES
LIRMM – UMR CNRS – University of Montpellier
Lionel.Torres@ lirmm.fr

Abstract

Magnetic memory (MRAM) never stops attracting both industry and academy for a wide range of applications. With its non-volatility, high density, ultra-low static power, radiation robustness, and easy integration with CMOS, MRAM is showing a good capability in secure applications. This paper aims at introducing the strong potential of using MRAM for secure devices.

1. Introduction

Beyond its storage feature, MRAM shows interesting potential for security applications. Several works [1][2][3] showed the possibility and the benefit using MRAM to implement some low cost secure blocs such as Physical Unclonable Functions (PUF) and True Random Number Generators (TRNG). PUF and TRNG are two very useful components in secure system design. PUFs can be used to extract chip-unique signatures and volatile secret keys, whereas TRNGs are used for generating random padding bits, initialization vectors and nonce in cryptographic protocols. This paper focuses on MRAM based TRNG devices.

2. MRAM based TRNG principle

On-chip True Random Number Generators (TRNGs) are part of cryptographic systems. They provide random keys, device identification and seeds for Pseudo Random Number Generators. These circuits are traditionally based on physical random variations like thermal noise or other quantum phenomena and are expected to generate random bits with very high entropy and zero correlation. Since the switching mechanism of the STT-MRAM is stochastic dependent and probabilistic, it is possible using MRAM to implement a real TRNG.
We remind that for MRAM a bit of information is stored as the resistance of a Magnetic Tunnel Junction (MTJ) which consists of two ferromagnetic layers separated by a thin insulating barrier (Figure 2). The parallel (antiparallel) state causes a low (high) resistance value and can be characterized as a logic zero (one). A read operation consists in measuring the resistance thanks to a sensing current flowing through the MTJ. For the write operation, a spin-polarized current flips the magnetization of the storage layer by direct transfer of the spin angular momentum from spin-polarized electrons. The direction of the current flow through the MTJ determines the final state of the bit cell.
What is important is that the STT switching is intrinsically stochastic (due to thermal fluctuation of magnetization). Figure 1 presents the switching probability depending of the current applied. As illustrated in Figure 2 extracted from [4], the basic idea is to use a MTJ for each 1-bit random number generator and apply a write current with 50% of success rate. We propose a new implementation of a fully CMOS/MRAM integrated TRNG.

3. MRAM based TRNG basic cells implementation

A basic circuit is designed to evaluate MRAM based TRNG. Cells design environment is composed of TowerJazz 0.18um CMOS process and SPINTEC 100nm STT-MTJ technology. As illustrated in Figure 3, the circuit is composed of a MRAM (MTJ) with a random writing part (an external control allow sweeping the writing current from 0 to Imax), a latch sense amplifier composed of two reversed inverters (inv1 and inv2) and a Reference cell with a resistance value between Rp and Rap (Rref = (Rp+Rap)/2).

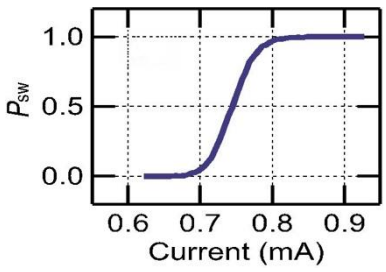

Figure 1: STT switching probability vs current

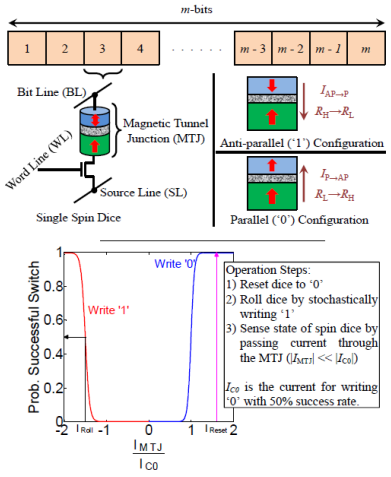

Figure 2: MRAM based TRNG principle [4]

The writing of the MTJ is done through the inverters inv3 and inv4 on both sides of the junction. The write current (Iw) is externally controlled and it is turn off when reading the resistance of the MTJ. Reading consist to enable the sense signal (SE high) which places the two reversed inverters (inv1 and inv2) in a metastable state and then, when disable the sense signal (SE low) the two reversed inverters take the closest stable state depending on the value of the resistances MTJ and REF. The functionality of the design is validated by transient simulation as illustrated in Figure 4. Signals (EN) and (DIN) control the writing current direction. Monte Carlo simulation and process corners simulations were performed to validate design stability. Then the layout of the design is done as illustrated in Figure 5.

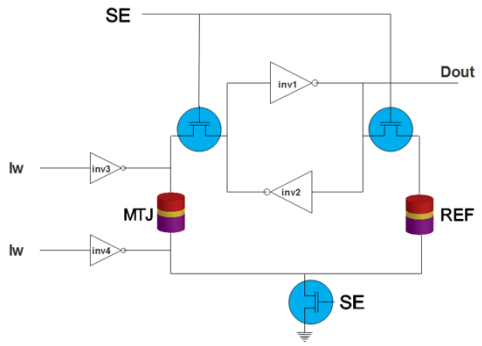

Figure 3: STT- MRAM based TRNG evaluation basic circuit

4. Conclusion

This work addressed a basic circuit design to evaluate TRNG based on MRAM. The circuit has been implemented with TowerJazz 0.18um CMOS process and SPINTEC 100nm STT-MRAM technology. As an extension of this work, we will add a control feedback scheme to this circuit to execute a real time output probability tracking inspired from [2].

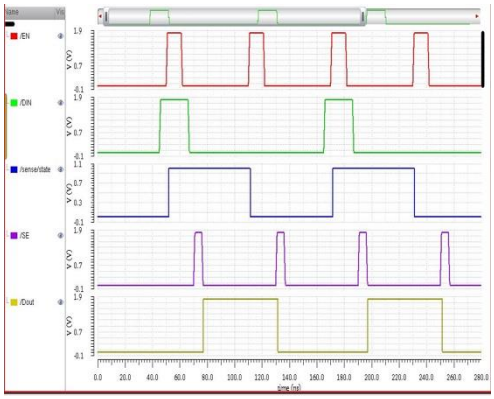

Figure 4 : Simulation validation

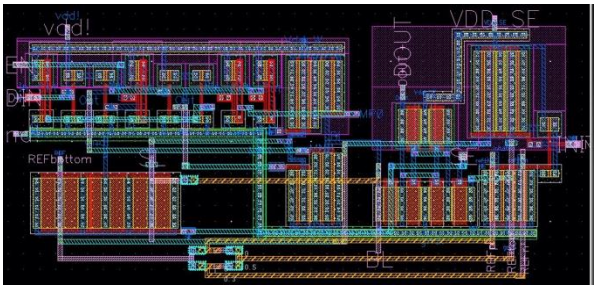

Figure 5: Circuit Layout

References

[1] Khaleghi, S., Vinella, P., Banerjee, S., & Rao, W. (2016, July). An STT-MRAM based strong PUF. *In Nanoscale Architectures (NANOARCH), 2016 IEEE/ACM International Symposium on (pp. 129-134). IEEE.*

[2] Wang, Y., Cai, H., Naviner, L. A., Klein, J. O., Yang, J., & Zhao, W. (2016, July). A novel circuit design of true random number generator using magnetic tunnel junction. *In Nanoscale Architectures (NANOARCH), 2016 IEEE/ACM International Symposium on (pp. 123-128). IEEE.*

[3] Oosawa, S., Konishi, T., Onizawa, N., & Hanyu, T. (2015, June). Design of an STT-MTJ based true random number generator using digitally controlled probability-locked loop. *In New Circuits and Systems Conference (NEWCAS), 2015 IEEE 13th International (pp. 1-4). IEEE.*

[4] Fong, X., Chen, M. C., & Roy, K. (2014, June). Generating true random numbers using on-chip complementary polarizer spin-transfer torque magnetic tunnel junctions. *In Device Research Conference (DRC), 2014 72nd Annual (pp. 103-104). IEEE.*

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