Magnetic Memory based True Random Number Generator

OUATTARA Frederic, TORRES Lionel

LIRMM – UMR CNRS – University of Montpellier (prenom.nom@lirmm.fr)

Abstract:

Magnetic memory (MRAM) is part of emerging memory which never stops attracting both industry and academy for a wide range of applications. Beyond its storage feature, MRAM shows interesting potential for security applications such as true random number generator (TRNG).

On-chip 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.

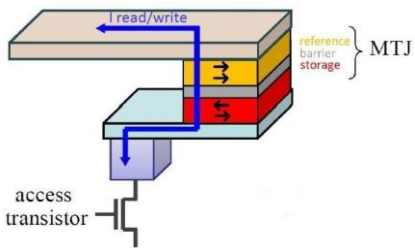

Figure 1

In 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 1). The parallel (antiparallel) state of these two ferromagnetic layers 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. This switching mechanism of STT MRAM is intrinsically stochastic (due to thermal fluctuation of magnetization). Figure 2 presents the switching probability depending of the current applied and the pulse duration.

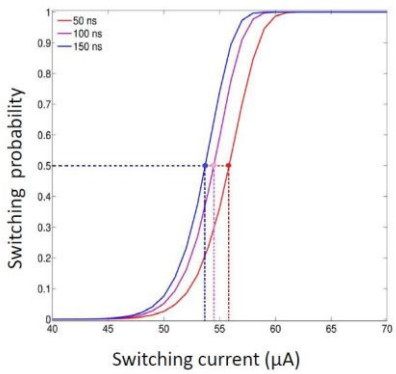

Figure 2

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 so the final state of the MRAM will be randomly one or zero.

We designed a basic circuit to evaluate the MRAM based TRNG.

Références :

[1] 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*

[2] 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.*

[3] 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.*