PHD POSITION

Date: 2019/11/21

Contacts: Florian PEBAY & Carlo CAGLI

forename.lastname@cea.fr

Object: PhD Position at CEA Grenoble (FR)

Keywords: silicon technologies, memories, security, random number generators

RTN entropy source extraction from RRAM for TRNG application

Objective

The objective of the thesis is to create a reliable entropy source for a True Random Noise Generator (TRNG) that will meet the IoT constraints, in terms of performance, robustness, cost and power consumption.

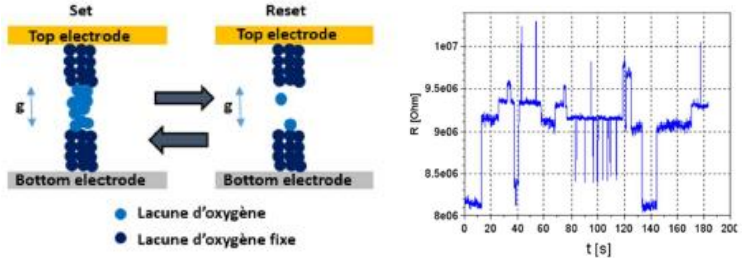
Detailed subject

As a consequence of the rapid development of the Internet of Things (IoT), where devices are massively interconnected, security breaches are discovered daily. The growing threat of physical attacks, on which connected objects are widely exposed, forces chipmakers to increase the security of their products. True Random Number Generators are the cornerstone of device security; they are required for running cryptographic algorithms and fully integrated into encryption engines [1]. The security level of the system directly depends on the randomness of the bits generated. Furthermore, IoT chips are facing harsh constraints in terms of price and power consumption. In order to be integrated into these chips, TRNG must offer an efficient tradeoff between cost and security. In this perspective, TRNGs based on already integrated components, such as memories, is a promising lead.

It is generally admitted [2] that TRNG are composed of three entities. First, the entropy source. It can be considered the core of the generator and it features a physical and random behavior. Then, the quantization stage, which permits to convert the analog signal (image of the physical random phenomenon) to a digital one. Finally, the post-processing part, which is responsible of enhancing randomness characteristics, allowing the output to be used for generating cryptographic keys, for example. In this Phd study we propose to focus on the entropy source that can be extracted from Resistive Random Access Memories (RRAM) cells.

RRAM is a class of solid state memory devices where the bit of information is stored as resistance level. This device can reversible switch between a high resistance level (HRS or RESET state), which code for “0” and a low resistance level (LRS or SET state) which codes for “1”. The typical RRAM cell is composed by a thin HfO_2 active layer sandwiched between an active (Ti) and an inert (TiN) electrodes. Ti absorbs oxygen ions from HfO_2, which generates oxygen vacancies (V_O) in the active layer. When a positive potential is applied on the Ti electrode, the V_Os are pushed towards the opposite electrode creating a percolative conduction filament (CF) which determines the LRS. Conversely, by applying a positive potential on the TiN electrode the CF is broken and a thin gap creates causing a resistance increase (HRS). While in LRS current conduction is mainly ohmic, HRS is characterized by Trap Assisted Tunneling (TAT): electrons “jump” from neighbor V_O to overcome the CF gap. In this regime, electrons can be temporary captured by positively charged traps (Vo or other point defects) in the proximity of the gap and interfere with the conduction via Coulomb interaction. When this

happens, a stochastic discrete current fluctuation, known as RTN, can clearly be measured across the device.



RTN has already been characterized in the prior art [3], [4], but only in the perspective of increasing the memory performance, i.e. reducing the noise source. We propose, based on existing research and on existing material, to characterize the RTN that can be extracted from RRAM cells to exploit it as an entropy source.
During the first half of the thesis, the work be organized as follows:

- First, the RTN signal will be characterized and linked to physical CFs' parameters, like length, diameter and gap size. Next, the RTN will be extracted from different HRS states and after multiple SET/RESET switches.
- Different programming and erasing conditions will be evaluated to improve RTN characteristics.
- In addition the statistical spread of RTN signal will be characterized in a whole 16Kbit RRAM array, to study the RTN spatial and temporal distribution over multiple bits. Eventually the temperature impact will be investigated and different strategies to compensate temperature drifts will be proposed.

During the second half of the thesis, the PhD candidate will propose a full architecture to manufacture an entropy source demonstrator. The latter will be then qualified with standard metrics for randomness and by using the NIS tests for entropy and TRNG. The entropy source will be designed to avoid the post processing part in order to reduce cost and power consumption. The design will eventually be integrated in a test run, depending on its maturity and on tape-out dates.

References

[1] B. Barak, R. Shaltiel, et E. Tromer, « True Random Number Generators Secure in a Changing Environment », in *Cryptographic Hardware and Embedded Systems - CHES 2003*, 2003, p. 166-180.

[2] P. Haddad, Y. Teglia, F. Bernard, et V. Fischer, « On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models », in *2014 Design, Automation Test in Europe Conference Exhibition (DATE)*, 2014, p. 1-6.

[3] C. Nguyen, « Caractérisation électrique et modélisation de la dynamique de commutation résistive dans des mémoires OxRAM à base de HfO2 », thesis, Grenoble Alpes, 2018.

[4] L. Pirro *et al.*, « RTN and LFN Noise Performance in Advanced FDSOI Technology », in *2018 48th European Solid-State Device Research Conference (ESSDERC)*, 2018, p. 254-257.