PHD POSITION

In-Memory Random Number Generator

Summary

Today, our digital world is massively connected through the Internet of Things, moreover remote and physical access to servers, computers, and electronic devices is mostly possible for all, at any moment. As a consequence, cybersecurity is present in many domains to reduce the risk and impact of potential attacks. In order to secure information, cryptography is massively used, and require cryptographic keys. To prevent an attacker to guess the keys (even partially) and access to sensitive information, key generation process require to be truly random. Therefore, Random Number Generators (RNG) can be considered as the cornerstone of information security. Full or partial failure in the random generator can jeopardize an entire system by ripple effect [1]. The purpose of this thesis work is to propose a new RNG concept, based on emerging memory cells – such as OxRAM and PCM – in order to deeply integrate the RNG into the electronic device. Such approach will enhance RNG performances in terms of throughput and robustness, and will also reduce costs in terms of power consumption, chip area, to be fully compatible to IoT devices constraints.

Educational preparation required

Master 2 Maths/Cryptography/IT/Statistics
Master 2 Semi-conductor physics/Microelectronics

Position details

Location: CEA Grenoble, System Department (LETI), LSCO and LDMC labs
The LSCO laboratory stands for Security of electronics Components, its mission is to provide security functions to electronic devices to prevent remote and physical attacks. Researches are involved at embedded software level, as well as digital design (FPGA, ASIC) and at micro-electronic level. In partnership with academic collaborators and industrial partners, researchers are working on innovative security functions and are also conducting attacks to test the robustness of their solutions.
The Memory and Computation Laboratory (LDMC) aims primarily at developing storage embedded devices. Its mission is the transfer towards the industry of new memory devices for both data storage and innovative memory-based computation circuits. The staff core skills rely on the manufacturing and on the device characterization.

Security clearance: security background check will be performed for each applicant.

PhD starting date: September 2022

PhD supervisors to contact for application

Florian PEBAY-PEYROULA
CEA DRT/DSYS/SSSEC/LSOSP
florian.pebay@cea.fr

Carlo CAGLI
CEA DRT/DCOS/S3C/LDMC
carlo.cagli@cea.fr

Director of research

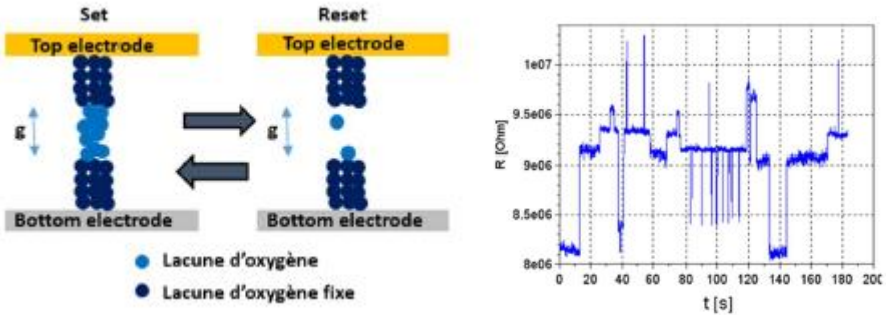
Giorgio DI NATALE (TIMA Laboratory), giorgio.di-natale@univ-grenoble-alpes.fr

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 (TRNG) 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 comes the entropy source. It can be considered the core of the generator and it features a physical and random behavior. Then, the quantization stage, that permits to convert the analog signal (image of the physical random phenomenon) to a digital signal. 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 thesis we propose to focus on the entropy source that can be extracted from Resistive Random Access Memories (RRAM) cells.

There are many types of resistive memories but all of them rely on the same principle: the memory information bit is coded as the resistance device level.
The OxRAM (short for Oxide RAM) 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 low resistive state (LRS). Conversely, by applying a positive potential on the TiN electrode the CF is broken and a thin gap causes the resistance to 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 V_Os or other point defects near 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 in the perspective of increasing the memory performance, thus 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.
Phase Change Memory (or PCM for short) is another example of resistive memory. This device takes advantage of the two possible meta-stable states, namely crystalline and amorphous, of an alloy of Germanium, Antimony and Tellurium (known as GST). A proper electrical pulse makes possible to switch between the two states reversibly. As these two states have different resistivity, the storage of a memory bit becomes possible. RTN is also observed in Phase Change devices and originates from similar mechanisms as seen for OxRAM.

During the PhD work the candidate will have the opportunity to work on both PCM and OxRAM devices as random seed generator.
During the first half of the thesis, the work be organized as follows:

- First, the RTN signal will be characterized and linked to programming parameters. Next, the RTN will be extracted from different resistive states and after multiple SET/RESET switches. Entropy will be qualified with standardized statistic analyzing tools.
- 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.

Then, during the second half of the thesis, the PhD candidate will propose a full architecture to manufacture an entropy source demonstrator. The work will focus on the reliability and stability of the random generation which will lead to a reduction of the post-processing cost and power consumption. The design will be then qualified with standard metrics for randomness and by using the NIST and BSI tests for entropy. The design will eventually be integrated in a test run, depending on its maturity and on tape-out dates. During this phase the candidate will also study the physics behind the random generation mechanisms in order to include it in the parametric entropy model.

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.