Method and device for a Physical Unclonable Function based on RTN

Method and device for generate a Physical Unclonable Function (PUF) whose source of entropy comes from a phenomenon known as Random Telegraph Noise (RTN). This phenomenon offers a critical advantage that few other entropy sources do: immunity to the degradation of the PUF performance that comes from circuit aging. To do so, the present invention uses a clever solution, in the form of a special metric, to capture, in a comprehensive manner, the amount of RTN present in a transistor. This new metric allows extracting entropy from just a couple of CMOS transistors, thus contributing to a considerable reduction of the required silicon area.

Industrial partners are sought to collaborate through a patent license agreement

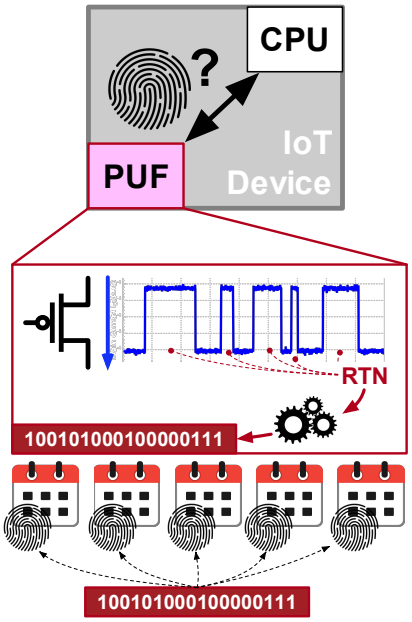
An offer for Patent Licensing

New device to increase the security of lightweight devices

The adoption of IoT-related technologies increases the challenge of data security and protection since data are no longer centralized but spread. An IoT device is secure if its authenticity, integrity, and confidentiality are all ensured. However, many IoT devices (such as wearables) cannot afford conventional cryptographic solutions, based on sophisticated software algorithms, which make use of power-hungry and expensive hardware. To give identity to the device and in this way ensure its authenticity, silicon Physical Unclonable Functions (PUF) have emerged as an ultra-low-power and low-cost solution.

In addition, and in the face of like the societal movement toward e-waste reduction, there is mounting pressure to extend the lifetime of IoT devices. However, of the myriad silicon PUF alternatives, very few are truly immune to electronic aging or, if they are, they come at a considerable cost in silicon area.

It is in this context where RTN-based solutions play a significant role, as this phenomenon, if tackled properly, materializes even at the lowest biasing conditions, thus preventing long-term degradation. Nevertheless, the biggest challenge is how to harness the power of RTN to be used as an entropy source for PUFs.



An aging-resilient identity can be obtained from the RTN present in the current of just a single transistor.

Main innovations and advantages

- A new method to harness RTN as an entropy source through the Maximum Parameter Fluctuation metric;
- A drastic reduction of the impact of aging-induced degradation since lower-than-the-nominal voltages can be used;
- For the same reason, a reduction of the power consumption is achieved, since transistors can operate even in the sub-threshold or linear regimes;
- Two architectural implementations are available: non-differential (with one single transistor to generate a bit response) or differential (with a pair of transistors to generate a bit response); the differential solution provides also immunity to common-mode disturbances like process or temperature variations;
- A reduction of silicon area when compared to other PUF solutions since only one or two transistors are required.

Patent Status

Spanish patent application field

For more information, please contact:

Víctor García Flores

Projects and Transfer Unit of the Instituto de Microelectrónica de Sevilla (IMSE-CNM)

Tel.: +34 954466666

Correo-e: victor@imse-cnm.csic.es
comercializacion@csic.es