Method and device for generating true random numbers

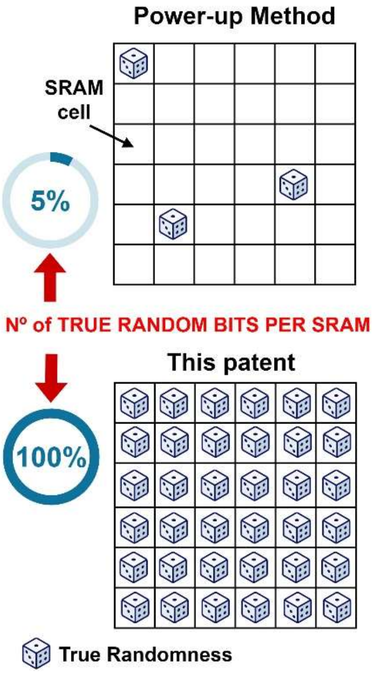
Method and device for generating true random numbers from Static Random Access Memory (SRAM) cells of any power-up bias, i.e., regardless of whether the cell has a greater or lesser tendency towards one of the logical power-up values. In contrast to the conventional power-up method, which is only able to generate True Random Numbers from a very limited portion of the total number of cells in an SRAM, this new method is based on the Data Retention Voltage metric, which provides the ability to extract randomness from any SRAM cell.

Industrial partners are sought to collaborate through a patent license agreement.

An offer for Patent Licensing

Maximizing the number of cells that can generate random numbers in SRAMs

The generation of random numbers by means of the method of the invention can be applicable in multiple fields. But the field where high-quality random numbers are requited is cryptography, with tasks like key generation, generation of "nonces", and generation of attack countermeasures. Ultra-low-power, low-cost lightweight cryptographic solutions use silicon Physical Unclonable Functions (PUF) to provide identity to devices and, in this way, ensure its authenticity. The power-up state of SRAM cells circuits is one of the most popular PUFs. Based on an initial selection process where the repeatability of the power-up value of each cell is evaluated, SRAM cells are classified to provide either identity or random numbers. However, due to the large variability in the fabrication process of nano-CMOS technologies, very few cells in an SRAM array can actually be used for random number generation using power-up methods. The developed method allows to extract randomness from any cell, independently of the technology of fabrication, improving dramatically the capabilities of these circuits for cryptographic applications.



Randomness can be extracted from any cell of the SRAM array.

Main innovations and advantages

- A prior cell selection is not required. Instead, any cell, independently of each power up bias, can be used as a random number generator, thus taking advantage of all available cells.
- A larger increase in minimum entropy is achieved when compared to other existing techniques, thus alleviating the need for intense post-processing.
- The reading process can be performed at the nominal supply voltage, unlike other techniques, thus eliminating the technical difficulties of reading at a very low voltage.

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

UNIVERSIDAD DE SEVILLA

MINISTERIO
DE CIENCIA
E INNOVACIÓN

CSIC
CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS