Chaotic MEMS-based TRNG

Martial Defoort*[1]

[1]TIMA, CNRS, Grenoble, France – Centre National de la Recherche Scientifique - CNRS – France

Résumé

Micro electromechanical systems (MEMS) are hardware tools present in most modern technologies, in the form of accelerometers, microphones, gyroscopes or even clocks (1). These types of devices present two especially relevant source of stochasticity, Brownian and 1/f noises, which are traditionally difficult to exploit as they are quite low compare to the signal of interest. However, by putting vibrating MEMS in a chaotic regime, the dynamics of these mechanical structures becomes exponentially sensitive to fluctuations, enabling to amplify their source of entropy and to use them as TRNGs. (2). In this presentation, I will first introduce the concept of chaotic MEMS, and then discuss their figures of merit in the context of TRNGs.

(1) J. Zhu *et al.*, " Development Trends and Perspectives of Future Sensors and MEMS/NEMS ", *Micromachines*, vol. 11, no 1, Art. no 1, janv. 2020.

(2) M. Defoort, L. Rufer, L. Fesquet, et S. Basrour, " A dynamical approach to generate chaos in a micromechanical resonator ", *Microsystems & Nanoengineering*, vol. 7, no 1, Art. no 1, févr. 2021.

*Intervenant