Chaotic micromechanical systems for asymmetric cryptography

Context:

Secured communications mostly rely on secret keys that enable to encrypt and decrypt messages. To share these keys between the emitter and the receiver in a secured way, another protocol is traditionally used: asymmetric cryptography. However, due to the recent advances in quantum computing, today's most used asymmetric protocols could soon become obsolete, calling for new secured communication techniques, such as chaos-based cryptography.

Chaos describes a complex dynamics that can be found in various fields such as economics, meteorology, turbulent phenomena or even in human brain activity. In the mechanical domain, Micro-ElectroMechanical Systems (MEMS) inherently present strong nonlinearities which can be used to obtain chaotic micromechanical systems [1]. On the one hand, thanks to the simple physical equations describing their dynamics, a comprehensive picture of their chaotic behaviors can be obtained, exploiting both analytical results and numerical simulations. On the other hand, MEMS are versatile and adjustable, providing an experimental platform to test various configurations as model systems.

This internship will contribute to the study of MEMS-based chaotic cryptography, on the path to offer an alternative technique for secured communications while enriching the knowledge on chaos.

Internship:

The main objective of this internship will be to study experimentally, numerically and theoretically the coupling between two chaotic micromechanical systems to obtain secured communication, using available piezoelectric MEMS designed by the laboratory TIMA. After a comprehensive characterization of the systems, the student will explore how their different parameters affect the quality of the security (Fig. 1). This study will be performed using state-of-the-art equipment, looking in particular at the mixing properties of the chaotic signal, their sensitivity to initial conditions, and the influence of the data rate on the quality of the secured transmission. The student will develop her/his own procedures for such characterizations and will perform involved signal post-processing to extract the relevant information from the noisy-like structure of the chaotic signals.

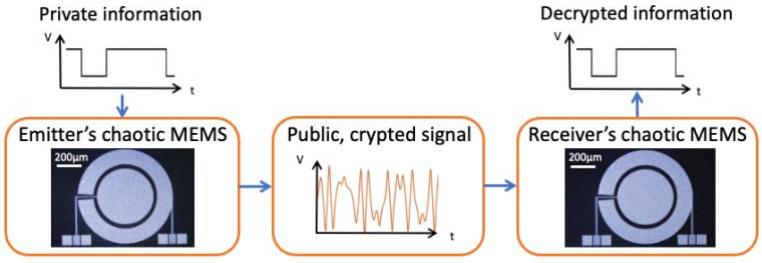

Figure 1: Schematic for chaotic MEMS-based cryptography, using micromechanical membranes. Data are encrypted within the chaotic dynamics of a first MEMS. This noisy-like structure is then transferred to a second MEMS, which decrypts the signal to retrieve the original information.

Student:

In last year of engineering school or Master 2, the candidate should have solid knowledge in physics and signal processing. The internship will last 5 months at TIMA laboratory, and is meant to be followed by a thesis.

Contact:

Martial DEFOORT
martial.defoort@univ-grenoble-alpes.fr

Bibliography :

[1] M. Defoort *et al*, A dynamical approach to generate chaos in a micromechanical resonator, *Microsyst. Nanoeng.* (2021)