Random numbers for Security Applications in Industrial Context

Ugo Mureddu*[1] and Patrick Haddad*[2]

[1]ST Microelectronics, Rousset, France – ST Microelectronics, Rousset, France – France
[2]ST Microelectronics, Rousset, France – ST Microelectronics, Rousset, France – France

Résumé

In cryptographic embedded systems, security is based on quality and unpredictability of confidential keys and on random numbers used in countermeasures against physical attacks. These critical values are generated in random number generators exploiting noisy physical phenomena appearing inside the system on chip. The most frequent source of randomness in integrated circuits is the jitter generated inside the device by clock signals such as ring oscillators, self-timed rings, RC oscillators, phase-locked loops (PLLs), etc. The quality and unpredictability of generated numbers is strongly linked to the amount of jitter and its nature. While academic effort focus on best-in-class performances purely true random number generator principles, cryptographic embedded systems manufacturers such as STMicroelectronics require robust random number generator implementations with stable performances over Process, Voltage and Temperature variations in addition with an efficient detection of any randomness failure. Such requirements are achievable thanks to a high confidence stochastic model-based entropy estimation and a precise jitter measurement. Indeed, a stochastic model is a mathematical formalization of the noisy clock signals and the process transforming them into random numbers. Consequently, when inputted with realistic jitter parameters, a stochastic model allows one to strongly understand the influence of each design and environmental variables on the random numbers' unpredictability. This is one of the main motivations for precisely characterizing the nature and the amount of jitter. In addition, continuously monitoring the amount of jitter while the random number generator is operating in the field is a relevant feature. Indeed, it allows to quickly detect quality reductions of the random numbers and avoid the security level degradation undetectable at system level.

In this talk, the industrial constraints of mass market random number generators design are presented. The speakers will also present the recent research activities overcoming those constraints.

*Intervenant