PhD Proposal

Title: Built-in Asynchronous Detection for Hardware Cryptography (BAD4HaCr)

PhD Advisors:
Laurent Fesquet, Giorgio Di Natale
laurent.fesquet@univ-grenoble-alpes.fr,
giorgio.di-natale@univ-grenoble-alpes.fr

Motivations
Securing data transactions and communications is today one of the major challenges we face in the Internet and Communication Technologies (ICT). This is done at both the software and hardware levels. In order to provide trusted systems, the root of the security is implemented in hardware with several primitives such as True Random Number Generator (TRNG), Physically Unclonable Function (PUF) or Crypto-processors. To tackle the attacks and threats on trusted systems, it is becoming essential to monitor the crypto-primitive behavior in order to detect possible breaches. Such a strategy could benefit from asynchronous circuits, which embed data signaling. This offers a unique opportunity for monitoring the sensitive security primitives.

Proposed Work
The PhD candidate will be in charge of developing a built-in monitoring strategy on several asynchronous security primitives. In order to develop a viable method, the approach will be first evaluated on a TRNG or a PUF, which are small security primitives. Indeed, the design of asynchronous TRNGs and PUFs have a small footprint, a low latency and a high throughput. The TRNGs and PUFs exploit asynchronous structures, which are particularly interesting for monitoring their activity thanks to their intrinsic asynchronous logic properties. Thus, the properties of randomness, uniqueness, stability and non "manipulability" can be monitored (completely or partially) in a relatively efficient way. For example, it is possible to correlate the entropy of noise sources to the operation of asynchronous oscillators (Self-Timed Rings) but also to observe the effect of an attack on the operation of the logic itself. Thus, in addition to the traditional measures against side-channel attacks and the difficulty to synchronize on an asynchronous circuit, the operation of this logic allows to go further in the observability and the monitoring of TRNG or PUF primitives. These methods and techniques will be developed in the framework of the project ARSENE.

The objectives of the PhD is to develop an original monitoring strategy applicable to asynchronous security primitives and potentially to extend it to any asynchronous circuit.

Agenda
1st year
- Bibliography
- Study of security primitives (TRNG, PUF, crypto-processors)
- Study of asynchronous circuit design
- First design of an asynchronous circuit

2nd year
- Implementation of a monitor on a TRNG (or a PUF)
- Optimization of the method and formalization
- Modelling of the TRNG and PUF entropy and its links with the monitor
- Design of security primitives on an FPGA or ASIC

- Writing of journal and conference articles

3rd year

- Analysis and characterization of the implemented security primitives
- Writing of journal and conference articles
- Writing of the manuscript