# Locking phenomenon on ring oscillators used in True Random Number Generators

Eloïse DELOLME[1], Florent BERNARD[1], Viktor FISCHER[1],
David LUBICZ[2], Maxime PELCAT[3]

[1]Université Jean Monnet, CNRS, Institut d Optique Graduate School, Laboratoire Hubert Curien
UMR 5516, F-42023, SAINT-ETIENNE, France
[2]DGA-MI, Bruz, France
[3]IETR UMR CNRS 6164 , INSA Rennes , 35700 Rennes, France

**Abstract**

To ensure the security of electronic devices, true random numbers are required by cryptographic systems. Several True Random Number Generators (TNRG) designs have been proposed, each with different characteritics and implementation properties. Multi Ring Oscillators (MURO) are used to counterbalance the low throughput of Elementary ring Oscillators (ERO). If the independance of RO is still maintained, the same modelling can be applied. However, the more ring oscillators, the greater the risk of influences between rings. This can go from mutual low influence of ROs to the worst case: full dependance between them. We talk about locking when rings are fully dependant.
In this presentation, we highlight the locking phenomenon and its danger for randomness generation. After a presentation of conditions where locking is more probable to appear and the ones limitating the phenomenon, embedded detection methods principle is explain. Finally, methods efficiency is compared. Then, they are implemented and used under several environmental conditions.

***Keywords***— TNRG, RO, locking