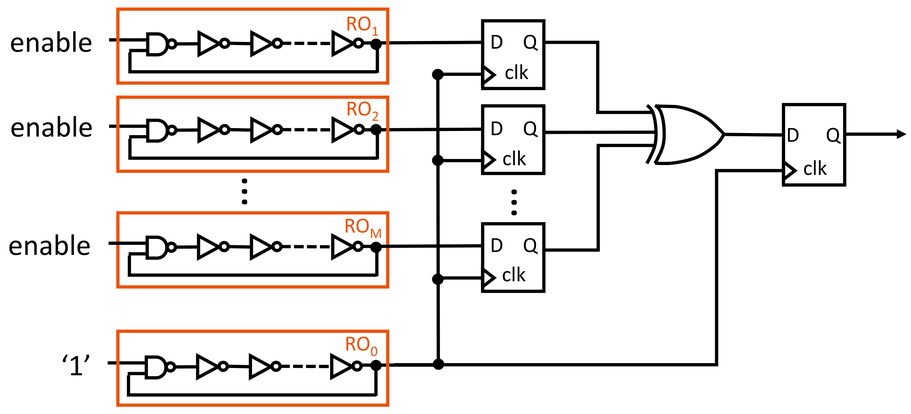
Beyond Total Locking: Demonstrating and Measuring Mutual Influence on a RO-Based True Random Number Generator on an FPGA

Eloïse DELOLME[1], Viktor FISCHER[1], Florent BERNARD[1], Nathalie BOCHARD[1], Maxime PELCAT[2]

[1] Université Jean Monnet Saint-Etienne, CNRS, Institut d Optique Graduate School, Laboratoire Hubert Curien UMR 5516, F-42023, SAINT-ETIENNE, France

[2] Univ Rennes, INSA Rennes, CNRS, IETR – UMR 6164, F-35000 Rennes, France

Context



Multiple Ring Oscillator based TRNG (MURO-TRNG)

☺ TRNG output bitrate better than elementary RO based TRNG.

☹ Stochastic model relies on the assumption that **RO_i are independent** but RO_i must have the **same topology and be placed close to one another** to reduce the impact of manipulable global noise sources.

Mutual Influence

Spontaneous: between ROs or with the surrounding logic

Active: EM attacks, supply voltage, temperature…

➥ Impact on the **operating frequencies** of ROs

Total locking

- Stable generator output value
- Easy to detect

Definition

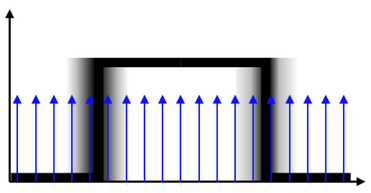
Mutual influence between two ROs appears when there are two small integers p, q such that

$$pf_0 \approx qf_1$$

Detection

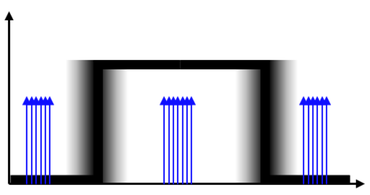
➥ **Sampling of signal:**

Ideal case:



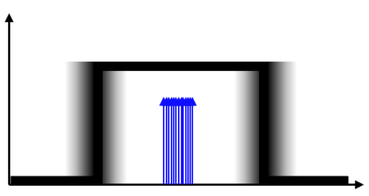
Phase differences are uniformly distributed

Influenced case:



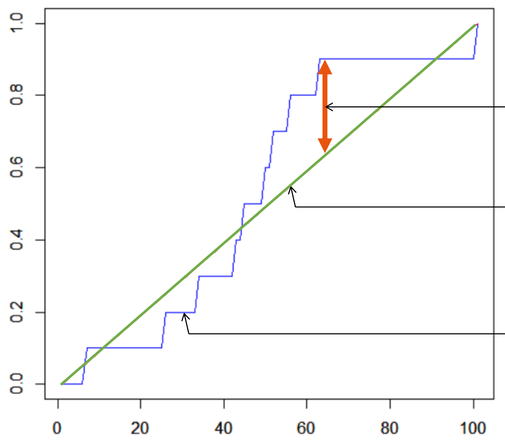
Loss of uniformity on phase differences distribution

Locked case:



➥ **How to detect this loss of uniformity?**

Kolmogorov-Smirnov test



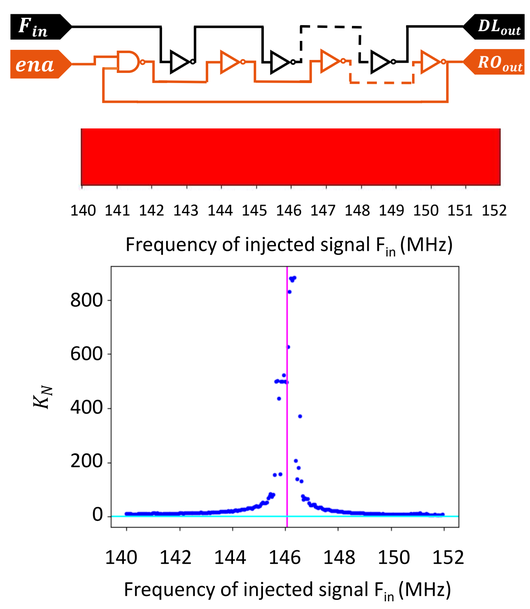
K_N : maximum distance

$F(x)$: uniform distribution function

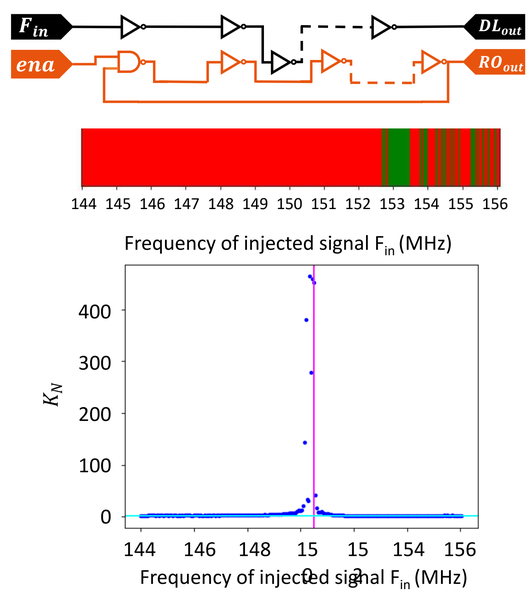
$F_N(x)$: phase differences distribution function

Results

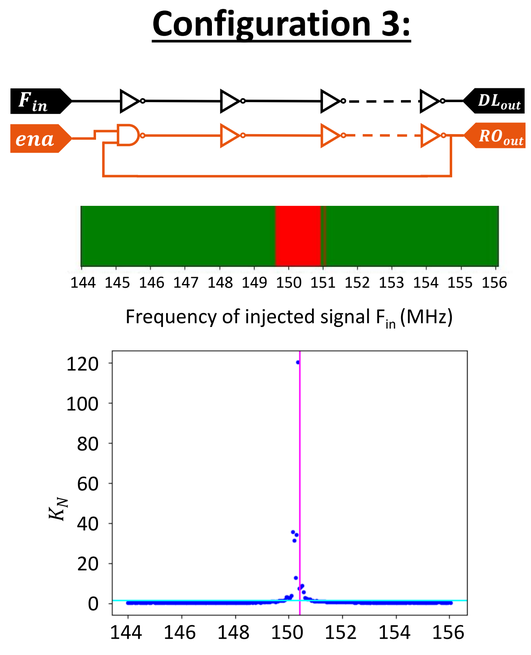
Configuration 1:



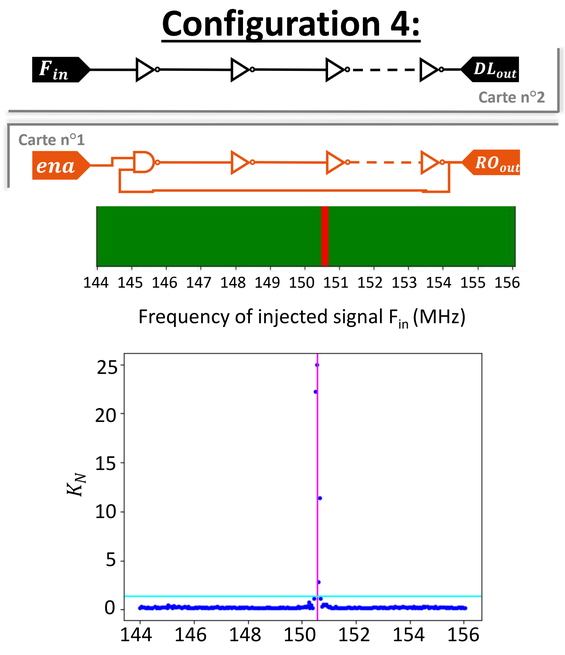
Configuration 2:



Configuration 3:



Configuration 4:



Conclusion

- Physical interactions can disturb ROs operating frequencies.
- Kolmogorov-Smirnov test quantifies the mutual influence by checking phase difference distribution.
- More precise information can be found in [1].

[1] Eloïse Delolme, Viktor Fischer, Florent Bernard, Nathalie Bochard, Maxime Pelcat. Beyond Total Locking : Demonstrating and Measuring Mutual Influence on a RO-Based True Random Number Generator on an FPGA. *37th IEEE International System-on-Chip Conference*, Sep 2024, Dresden, Germany. ⟨ujm-04649086⟩

Université Jean Monnet Saint-Étienne
Laboratoire Hubert Curien UMR ▪ CNRS ▪ 5516 ▪ Saint-Étienne
cnrs
DGA DIRECTION GÉNÉRALE DE L'ARMEMENT
INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES
ÉCOLE DOCTORALE 488
SIS SCIENCES INGÉNIERIE SANTÉ UNIVERSITÉ DE LYON