Study, characterization, and detection of locking in oscillating rings used in random number generators.

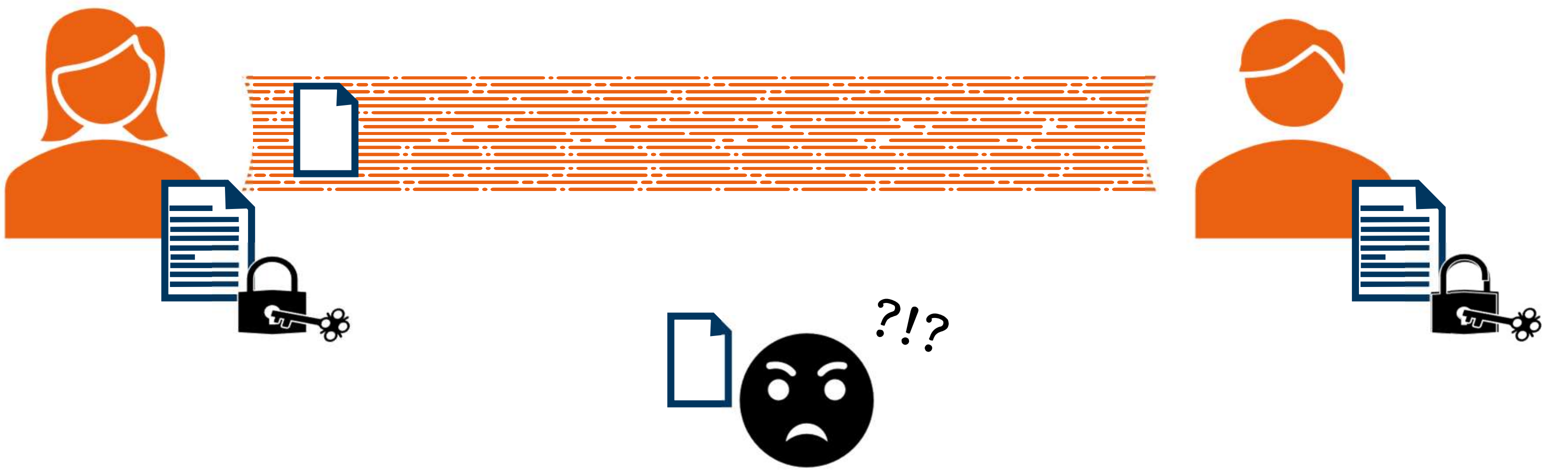
SemSecuElec seminar

29^{th} May 2026

Eloïse DELOLME

Laboratoire Hubert Curien
UMR • CNRS • 5516 • Saint-Étienne

CONTEXT



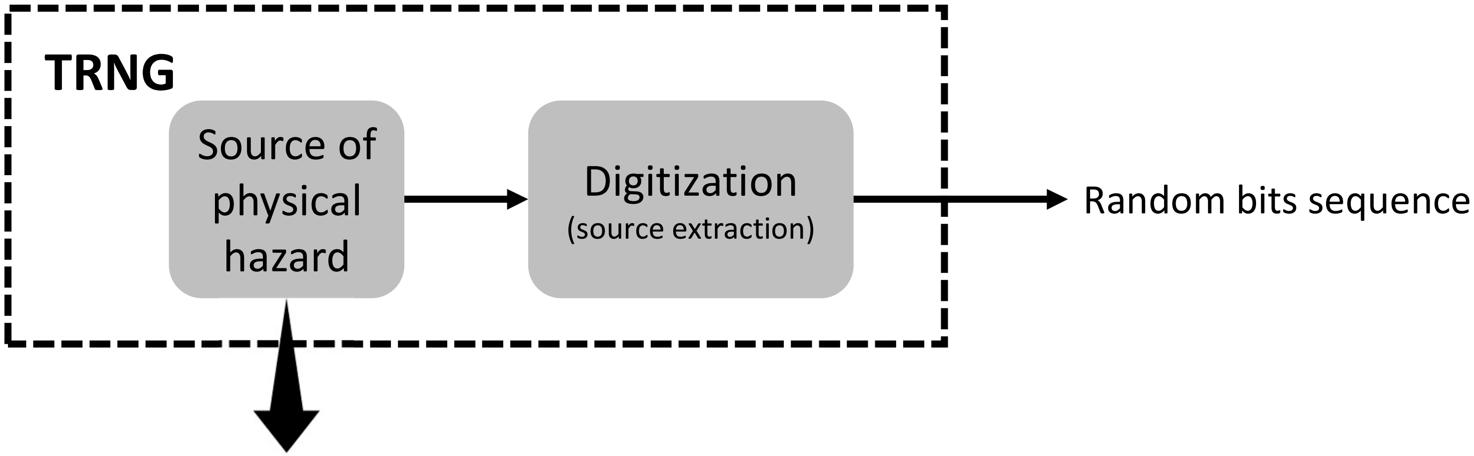
Cryptographic key:

- Unpredictable
- Non-reproducible

»» Random Number Generator (RNG)

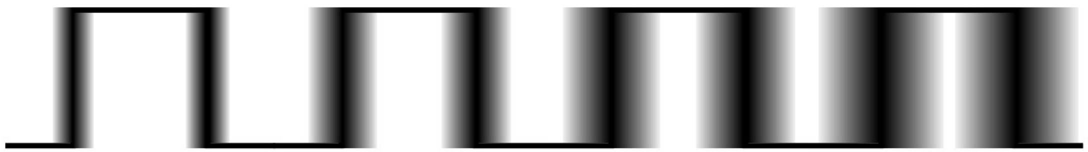
CONTEXT

TRNG (True Random Number Generator) :
Implemented in digital circuits based on a physical phenomenon.



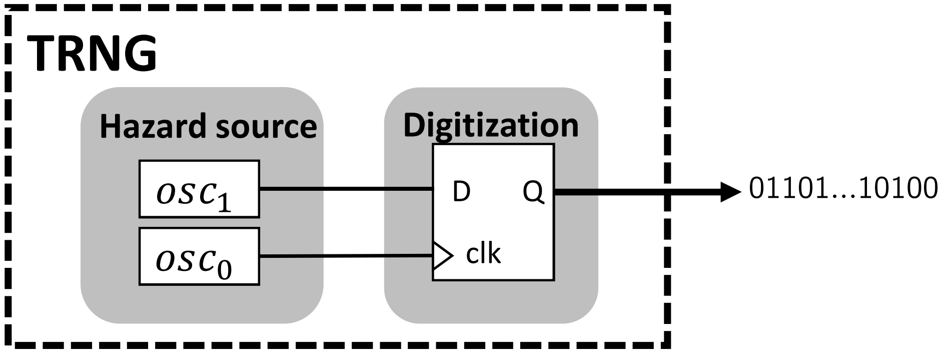
European standard: AIS 20/31 [1]
American standard: NIST 800-90B [2]

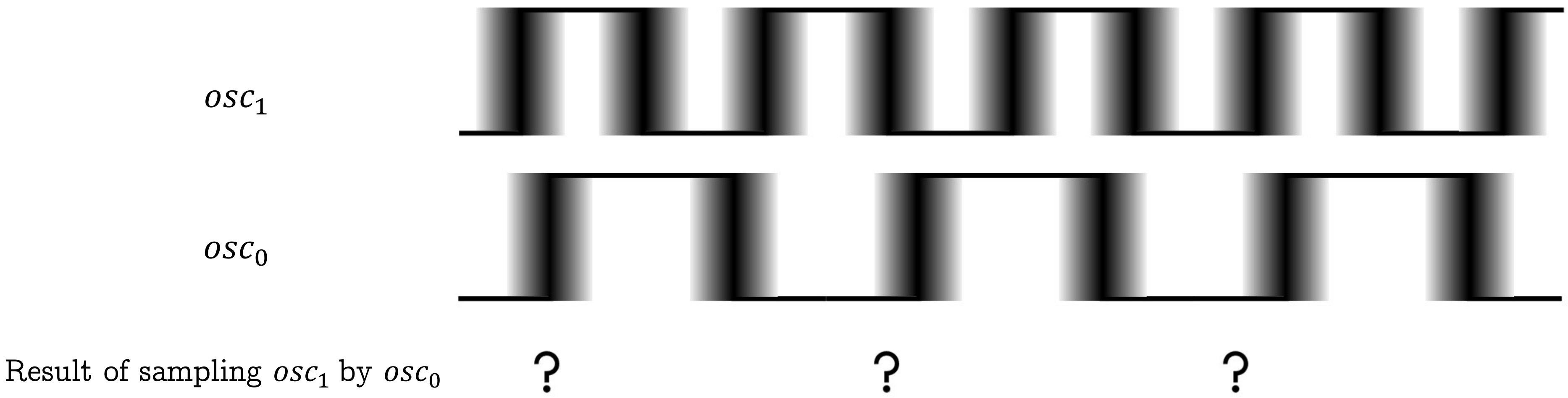
Clock jitter : temporal instability affecting the signal period.



[1] W. Schindler and M. Peter. A proposal for functionality classes for random generators, Sept. 2024.
[2] National Institute of Standards and Technology. (2015–2025). *NIST Special Publication 800-90 Series: Random Bit Generation Recommendations*. Gaithersburg, MD: U.S. Department of Commerce.

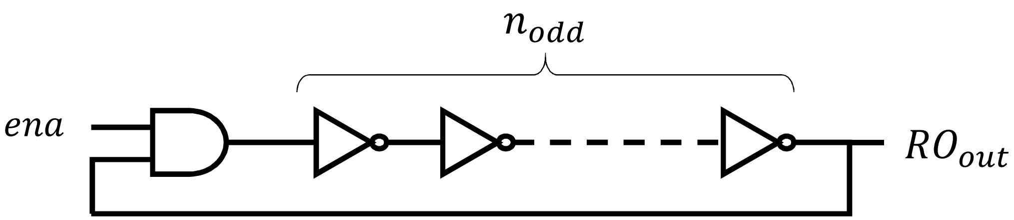
CONTEXT

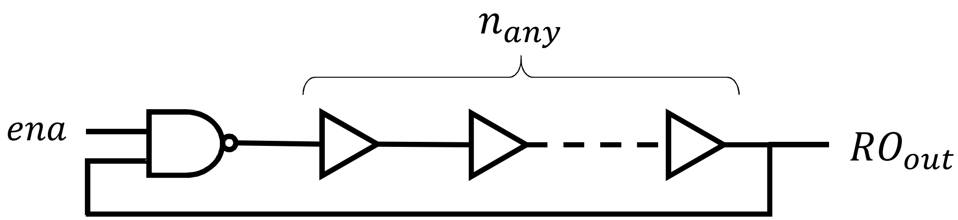

TRNG
Hazard source
Digitization
osc_1
osc_0
D
Q
clk
01101...10100


osc_1
osc_0
Result of sampling osc_1 by osc_0
?
?
?

CONTEXT

STRUCTURE OF A RING OSCILLATOR (RO)



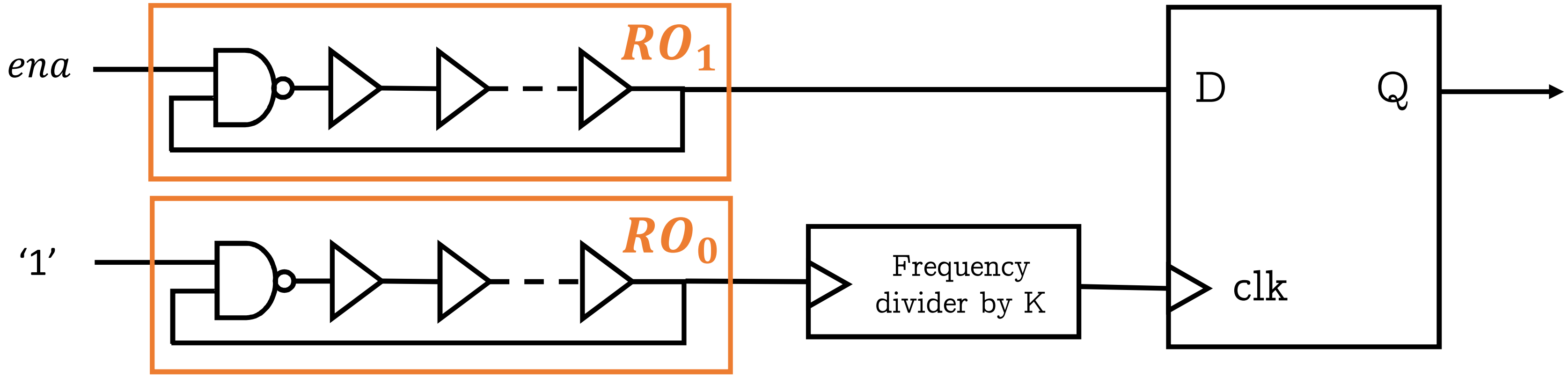


FREE RUNNING FREQUENCY

$$f_{RO} = \frac{1}{2 \times (d_{AND} + n_{odd} \times d_{INV})}$$

d_{AND} : average propagation delay of an AND gate
d_{INV} : average propagation delay of an inverter gate

CONTEXT

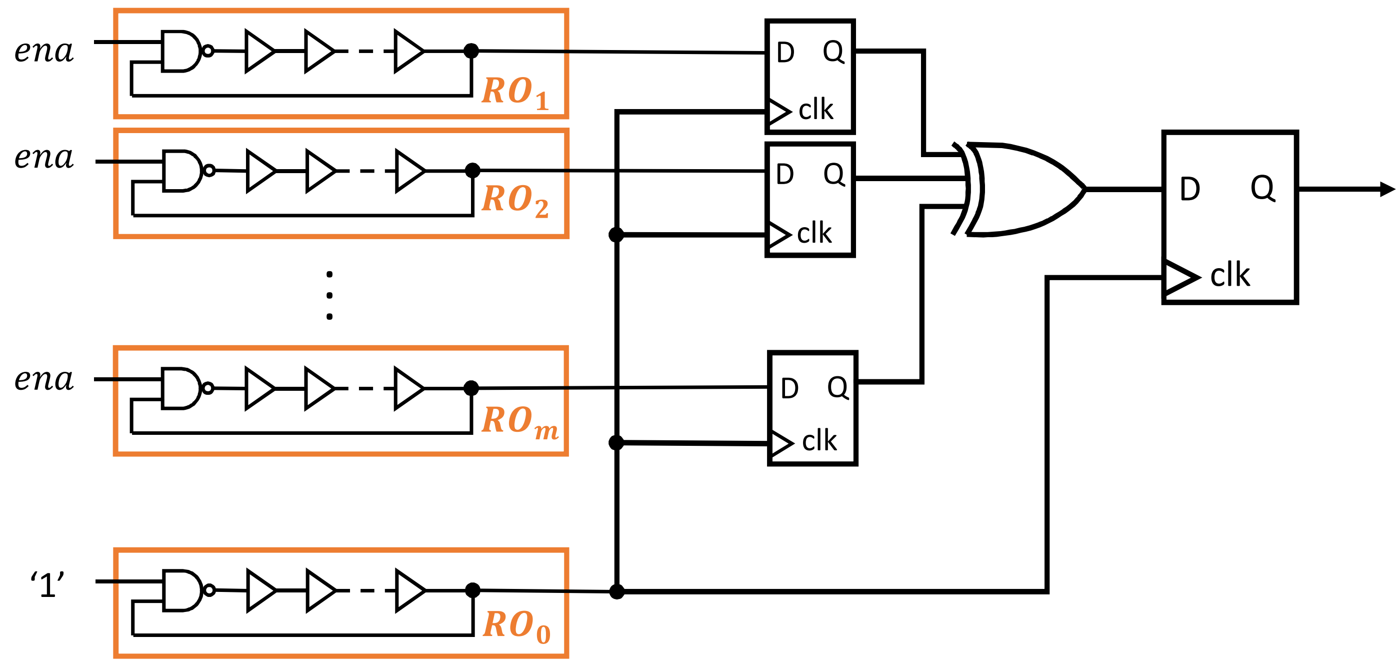


ERO-TRNG

- Easy to implement in logic circuits
- Resource-efficient

- High accumulation time: large K ($\approx 300\,000$)
- Low output bitrate

CONTEXT



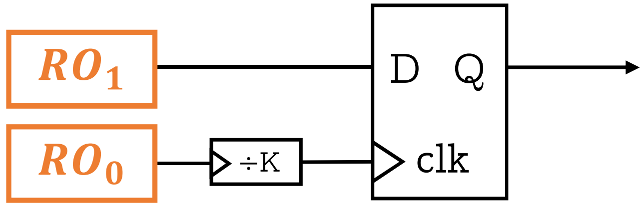
MURO-TRNG

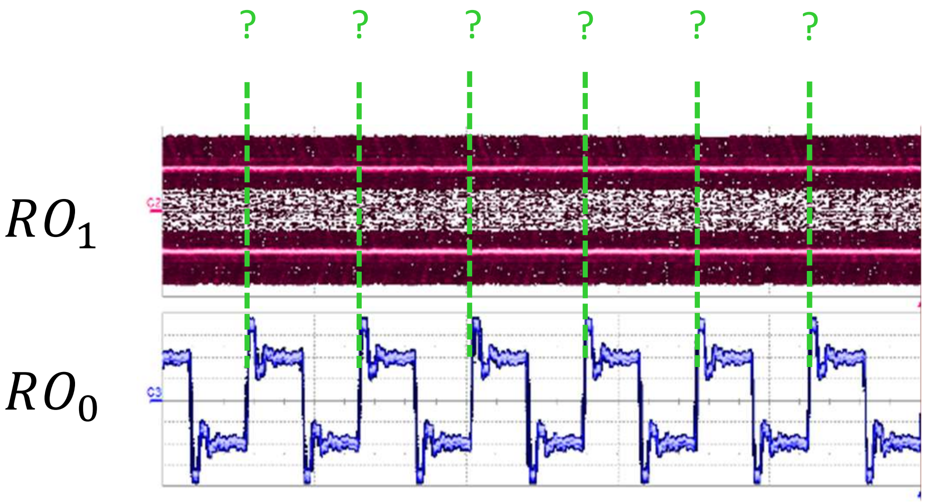
- Low accumulation time
- Better output bitrate

Stochastic model based on the independence of the ROs

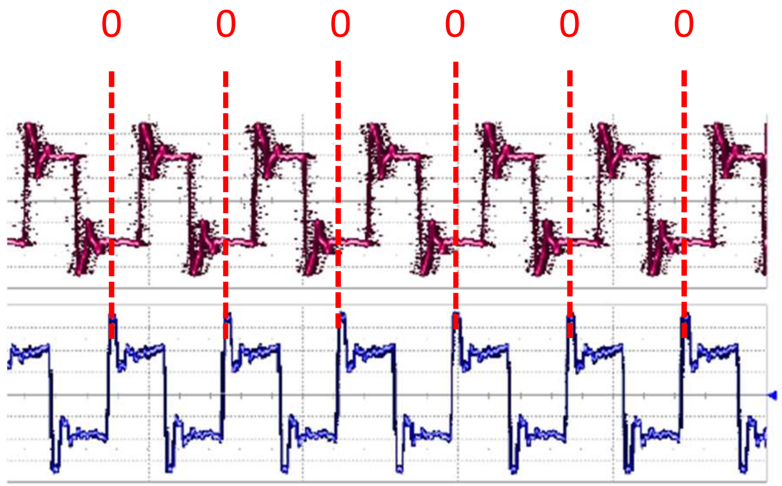
PROBLEM

Locking phenomenon



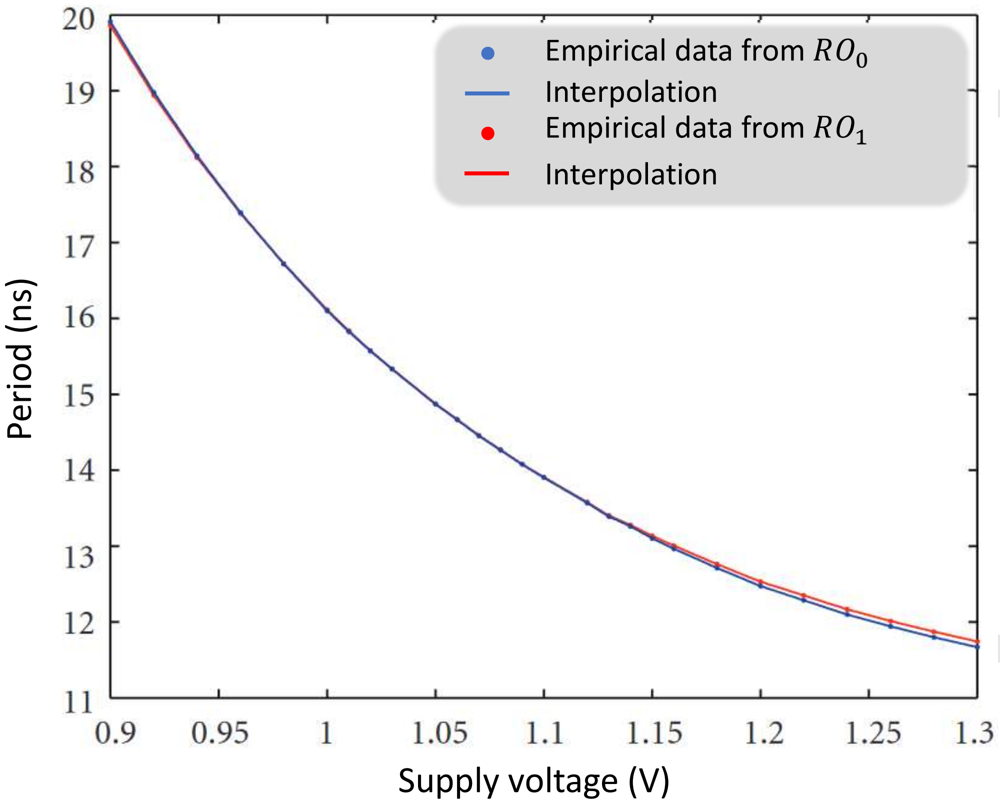


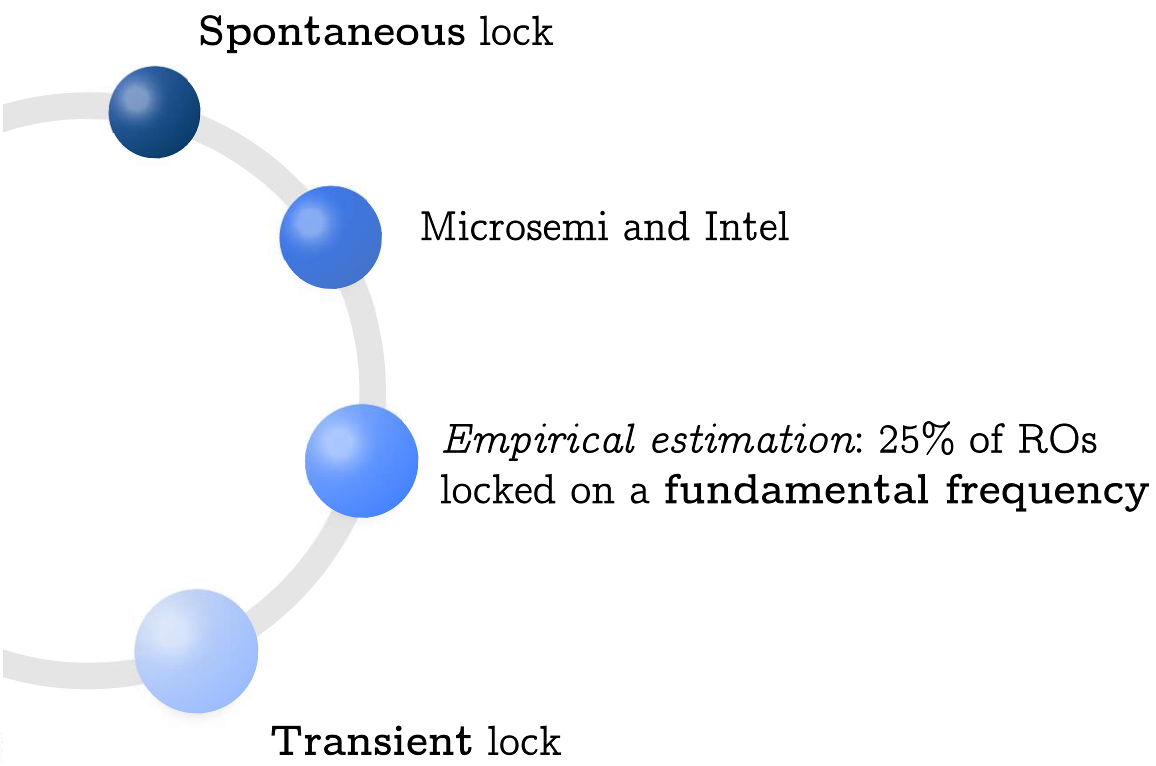
UNLOCKED



LOCKED

STATE OF THE ART [3]





[3] Nathalie Bochard, Florent Bernard, Viktor Fischer, and Boyan Valtchanov. *True-randomness and pseudo-randomness in ring oscillator-based true random number generators*. International Journal of Reconfigurable Computing, Janv 2010.

STATE OF THE ART

EXPLOITATION OF THE PHENOMENON

Markettos & Moore [4]

- Successful attack on a payment card.
- Reduction of key space : $2^{64} \rightarrow 3300$.

Frequency injection attack

Bayon *et al.* [5]

- Control of the bias at the output of a MURO-TRNG.
- Highlights the vulnerabilities of this type of TRNG.

EM injection attack

PHENOMENON STUDY

Murreddu [6]

- Supply voltage modification.
- Modification of the number of delay element in RO.
- Place and route.

Empirical study of the phenomenon

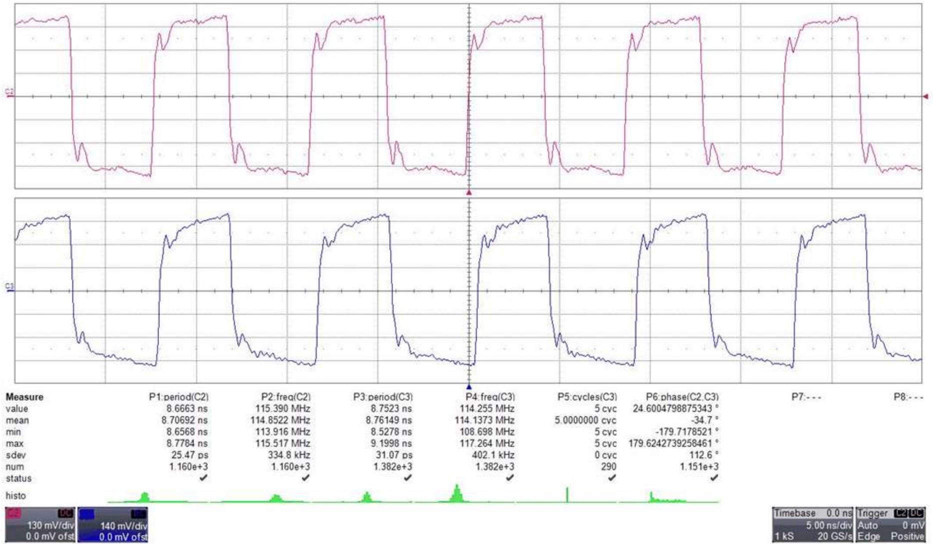
[4] : A. Markettos and S. Moore. The frequency injection attack on ring oscillator-based true random number generators. 2009.
[5] : P. Bayon, F. Pourcheret, L. Bossuet, B. Robisson, A. Aubert, P. Maurine, and V. Fischer. Contactless electromagnetic active attack on ring oscillator based true random number generator. 2012.
[6] : Ugo Murredu. Génération d'aléa dans les circuits électroniques numériques exploitant des cellules oscillantes. PhD thesis, Université Jean Monnet de Saint-Etienne, 2019

STATE OF THE ART

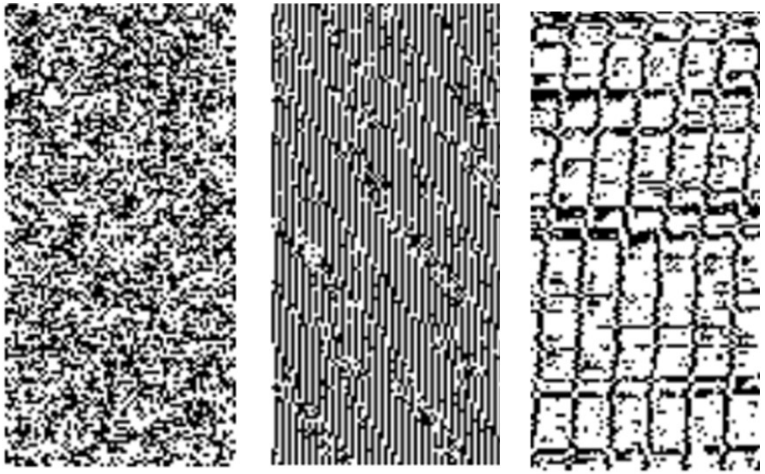
OBSERVING SIGNALS ON AN OSCILLOSCOPE

RO_0

RO_1



Injection of a signal with a frequency of 1.82 MHz



No injection

Injection of a signal with a frequency of 1.93 MHz

VISUAL REPRESENTATION OF THE BIT SEQUENCE [4,5]

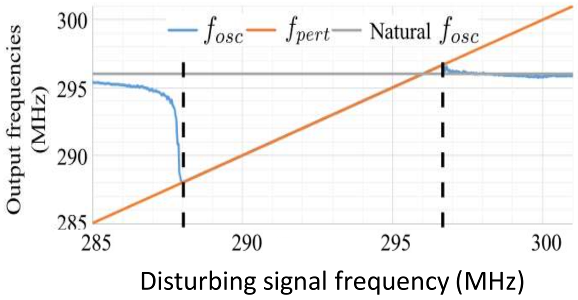
Effective for detecting total lock.

- Does not detect transient disturbances or partial locking.
- Detection methods that lack precision.

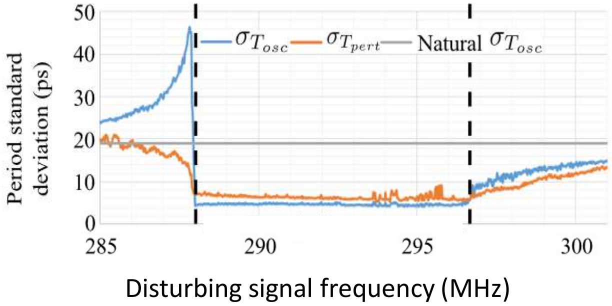
[4] : A. Markettos and S. Moore. The frequency injection attack on ring oscillator-based true random number generators, 2009.
[5] : P. Bayon, F. Pourcheret, L. Bossuet, B. Robisson, A. Aubert, P. Maurine, and V. Fischer. Contactless electromagnetic active attack on ring oscillator based true random number generator. 2012.

STATE OF THE ART

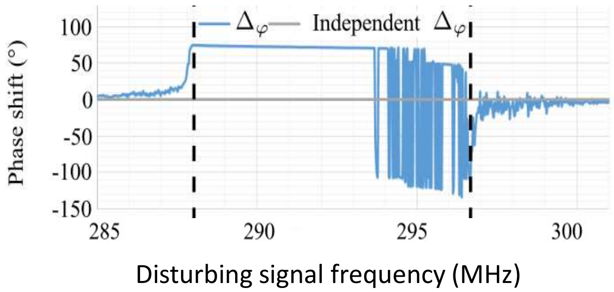
METRICS MEASURING THE PHENOMENON: [7]



OUTPUT FREQUENCIES



PERIOD STANDARD DEVIATION σ_T



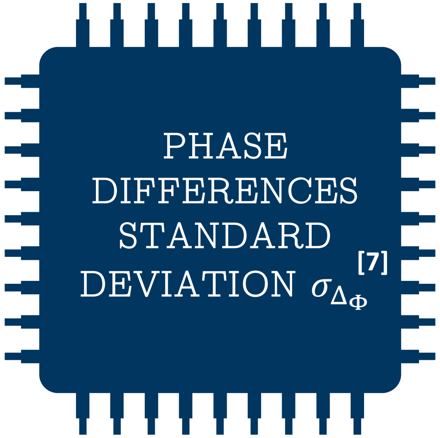
PHASE SHIFT $\Delta\Phi$

Effective for detecting total lock.

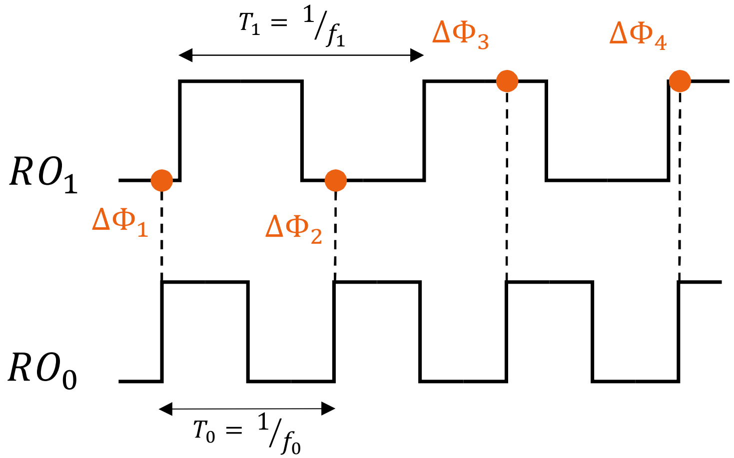
- Depends on the order of magnitude.
- Absence of an ideal value indicates a non-locking condition.

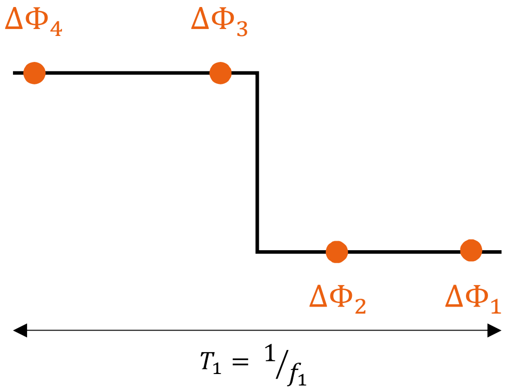
[7] : Ugo Mureddu, Nathalie Bochard, Lilian Bossuet, and Viktor Fischer. *Experimental study of locking phenomena on oscillating rings implemented in logic devices*. IEEE Trans. Circuits Syst. I Regul. 2019.

STATE OF THE ART

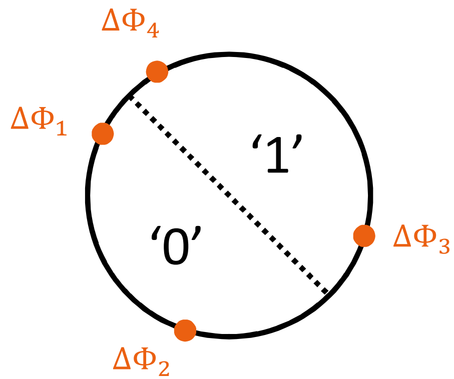


PHASE DIFFERENCES:





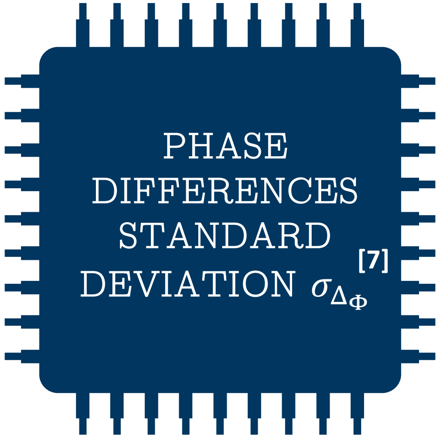
NOMINAL PERIOD of RO_1



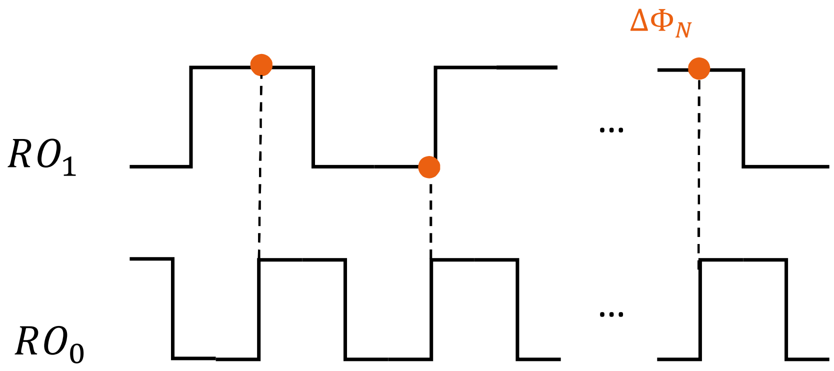
PHASES SPACE

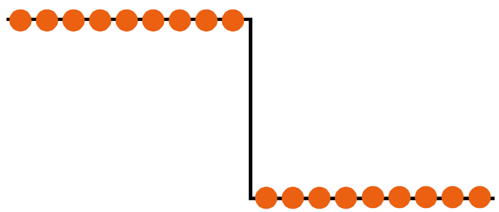
[7] : Ugo Mureddu, Nathalie Bochard, Lilian Bossuet, and Viktor Fischer. *Experimental study of locking phenomena on oscillating rings implemented in logic devices*. IEEE Trans. Circuits Syst. I Regul. 2019.

STATE OF THE ART

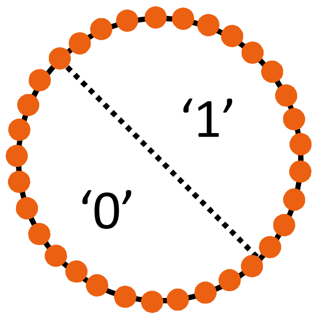


PHASE DIFFERENCES:





NOMINAL PERIOD of RO_1



PHASES SPACE

➜ Uniform distribution of phase differences over N periods of the sample signal

[7] : Ugo Mureddu, Nathalie Bochard, Lilian Bossuet, and Viktor Fischer. *Experimental study of locking phenomena on oscillating rings implemented in logic devices*. IEEE Trans. Circuits Syst. I Regul. 2019.

STATE OF THE ART

PHASE DIFFERENCES STANDARD DEVIATION σ_{Δ_Φ} [7]

Standard deviation of an uniform distribution on an interval $[a,b]$: $\sigma_{\mathcal{U}[a,b]} = \frac{b-a}{\sqrt{12}}$

Phases space: $[0°\,,360°]$

$$\sigma_{\mathcal{U}[0°,360°]} = \frac{360}{\sqrt{12}} \approx 103,9°$$

Locking phenomenon: characterized by a **deviation** from the ideal value of 103.9° of the standard deviation of the phase differences between two ROs.

Detection of a total lock but also partial or transient
$\rightarrow \sigma_{\Delta_\Phi} \notin [103,9° - \delta\,; 103,9° + \delta]$

[7] : Ugo Mureddu, Nathalie Bochard, Lilian Bossuet, and Viktor Fischer. *Experimental study of locking phenomena on oscillating rings implemented in logic devices*. IEEE Trans. Circuits Syst. I Regul. 2019.

OBJECTIVES

TO UNDERSTAND

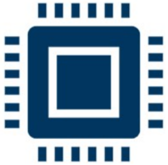
- Identification of the factors contributing to the occurrence of the locking phenomenon.

→ Recommendations for ROs implementation.

TO DETECT

- Detection of a loss of uniformity in phase difference samples.

→ Precise method.



TO EMBED

- Implementation of an embedded detection method.

→ On-line test.

OBJECTIVES

TO UNDERSTAND

- Identification of the factors contributing to the occurrence of the locking phenomenon.

→ Recommendations for ROs implementation.

TO DETECT

- Detection of a loss of uniformity in phase difference samples.

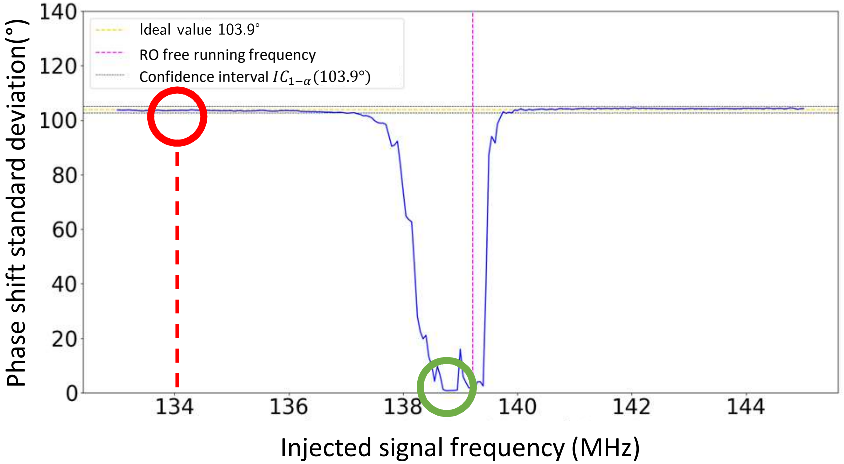
→ Precise method.

TO EMBED

- Implementation of an embedded detection method.

→ On-line test.

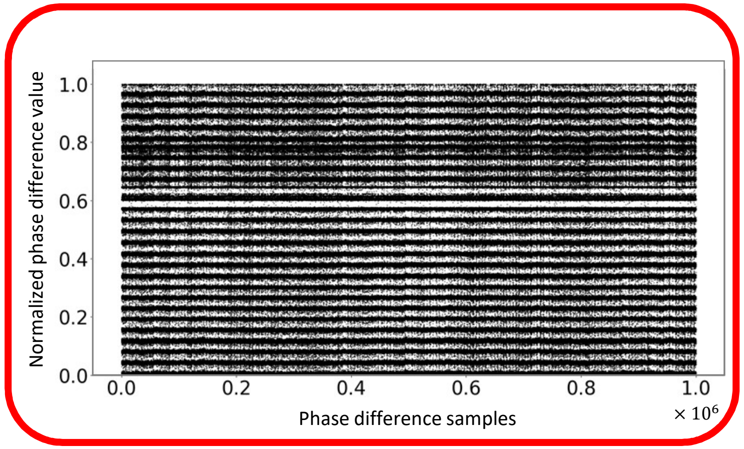
LIMITS OF METRICS OF THE STATE OF THE ART

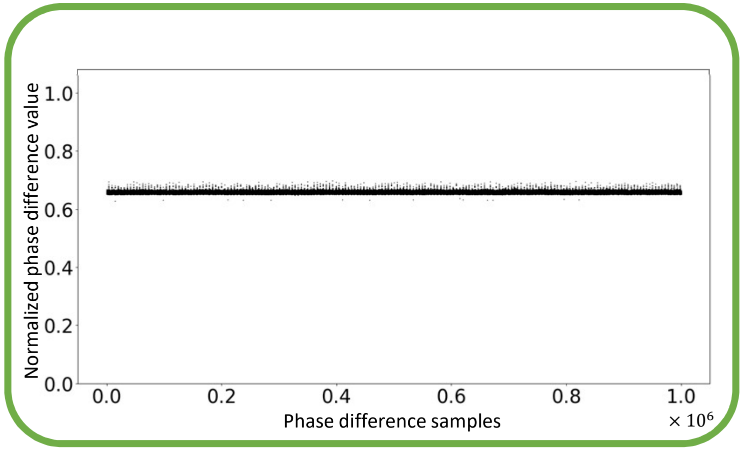


Standard deviation of an uniform distribution on an interval $[a, b]$:

$$\sigma_{\mathcal{U}[a,b]} = \frac{b-a}{\sqrt{12}}$$

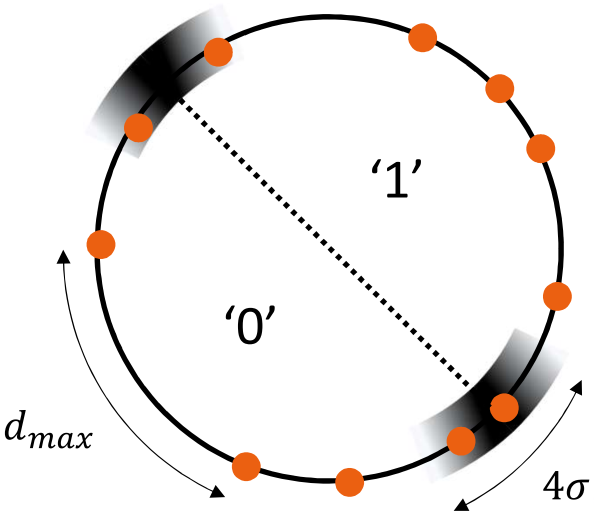
$\hookrightarrow$ Ideal value on $[0°, 360°] = 103{,}9°$

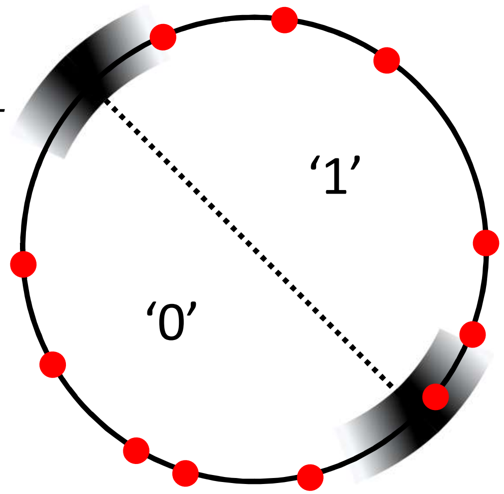




Total lock : $\sigma_{\Delta\phi} \approx 0°$

UNIFORMITY OF PHASES SHIFT DISTRIBUTION





$\sigma \in \left[\frac{0,5}{1000}, \frac{1}{1000}\right]$

At least two contributors per jittered zones:[8]

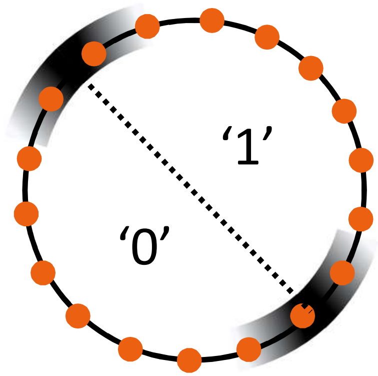
→ phases shift samples **cover** all **phases space.**
→ distance between two phase differences must be inferior to a threshold.

$$2d_{max} < 4\sigma$$
$$\Rightarrow \boldsymbol{d_{max} < 0,001}$$

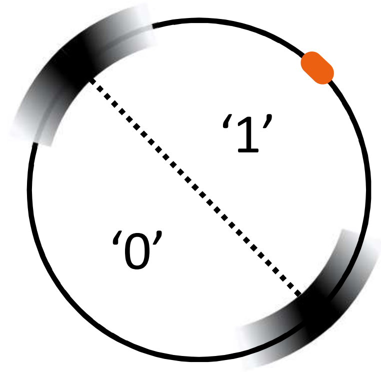
[8] Viktor Fischer, Florent Bernard, Quentin Dallison, and Maciej Skorski. Enhancing quality and security of the pll-trng. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023

LOSS OF UNIFORMITY

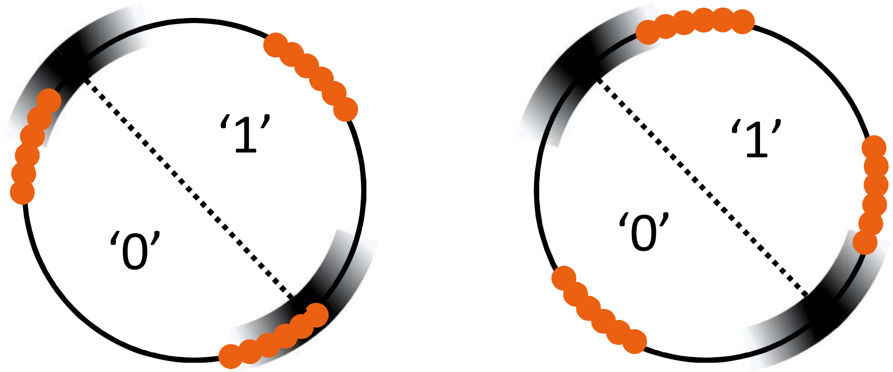
Uniform distribution on phases space



Total lock



Incorrect frequency ratio



Sampling when $2f_0 \approx 3f_1$ for different initial phase shift

DEFINITION OF MUTUAL INFLUENCE

> Let RO_0 with frequency f_0 and RO_1 with frequency f_1.
> The **mutual influence** between **two ring oscillators** RO_0 and RO_1 arises when the initial frequency ratio is degraded, i.e. when there exist small p and q such that
>
> $$q f_0 \approx p f_1$$

Total lock is a special case of mutual influence, which occurs when $q f_0 = p f_1$, for sufficiently **small** p and q.

DETECTION METRIC

Detect an incorrect frequency ratio for a given pair of ROs that exist from the implementation itself.

Detect an attack that degrades a good initial frequency ratio during operation.

Non-uniform distibution of phase differences

$\rightarrow$ Statistical test for compliance with a uniform distribution

GOODNESS-OF-FIT TESTS

1 χ^2 test

- Very difficult to set parameters.
- Suitable for discrete data where categorization into different classes is natural.
- Inconclusive empirical results.

2 Kolmogorov-Smirnov test

- Single parameter: the number of samples.
- Suitable for continuous data.
- Very good empirical results.

3 Cramér-von Mises test

- Similar to the Kolmogorov-Smirnov test.
- Less sensitive to outliers.

GOODNESS-OF-FIT TESTS

1

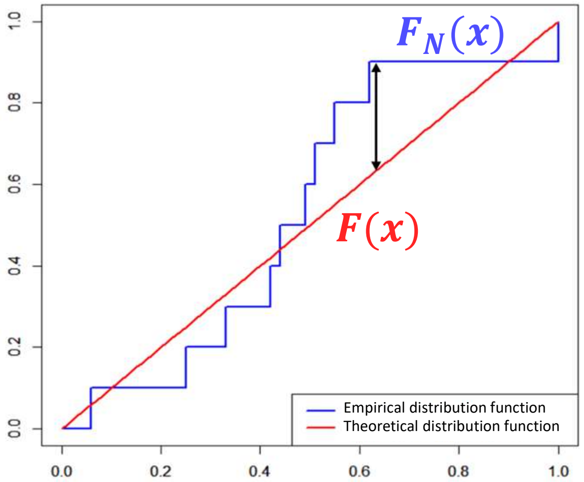
2

3

H_0 : « The phase difference samples are uniformly distributed. »

$$F_N(x) = \frac{\#\, samples < x}{N} \qquad F(x) = \begin{cases} 0 & when\ x < 0 \\ x & when\ 0 < x < 1 \\ 1 & when\ x > 1 \end{cases}$$

Kolmogorov-Smirnov test



- Calculation of the test statistic:

$$K_N = \max(K_N^-, K_N^+)$$

$$\hookrightarrow \quad K_N^- = \sqrt{N} \max_{-\infty < x < +\infty} (F(x) - F_N(x))$$

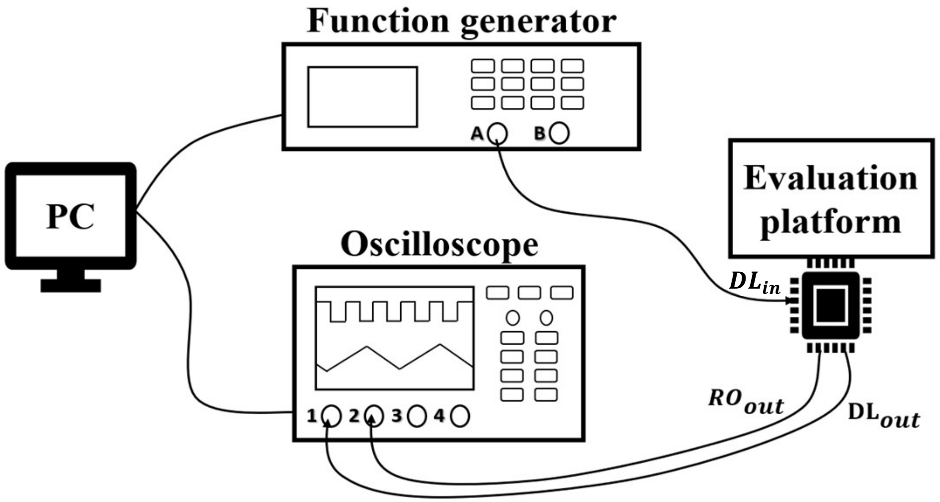
$$\hookrightarrow \quad K_N^+ = \sqrt{N} \max_{-\infty < x < +\infty} (F_N(x) - F(x))$$

- Binary result:

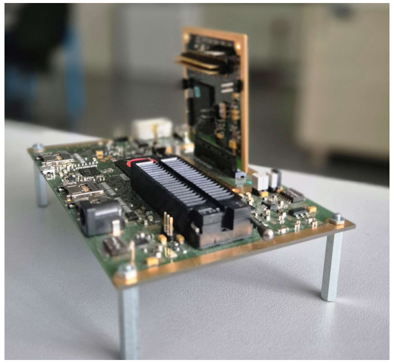
$K_N \geq s_{N,1-\alpha}$: H_0 rejected at the chosen level of significance $1 - \alpha$.

$K_N < s_{N,1-\alpha}$: not enough evidence to reject H_0

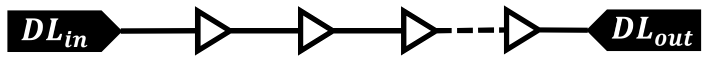
EXPERIMENTAL SETUP



- Intel Cyclone V
- Xilinx Spartan 6



Delay Line (DL):



Experiment procedure:

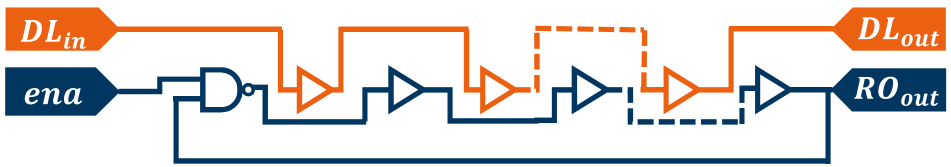
1. Configuration of the FPGA
2. Stabilization of the RO free running frequency
3. Frequency scan: ± 6 MHz by step of 0,05 MHz
    a. At each frequency, one million phase difference samples are captured by the oscilloscope.
    b. Writing data to a results file.
4. Asynchronous analysis of phase shifts.

KS test paramters:

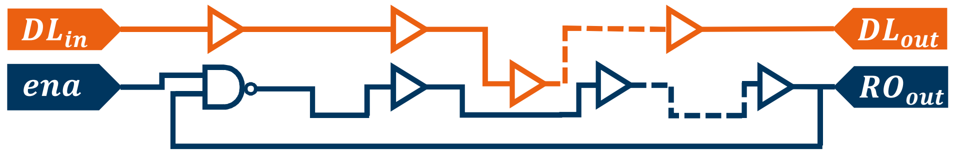
$N = 1\ 000\ 000$ $\alpha = 5\%$ $s_{N,1-\alpha} = 1{,}3581$

CONFIGURATIONS

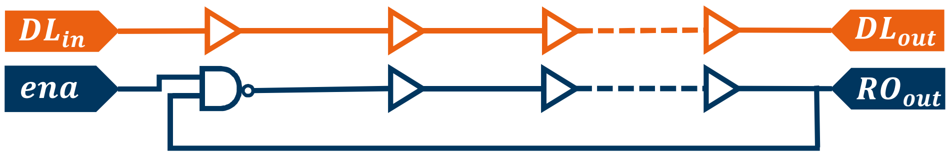
1. High interlacing (reference configuration)



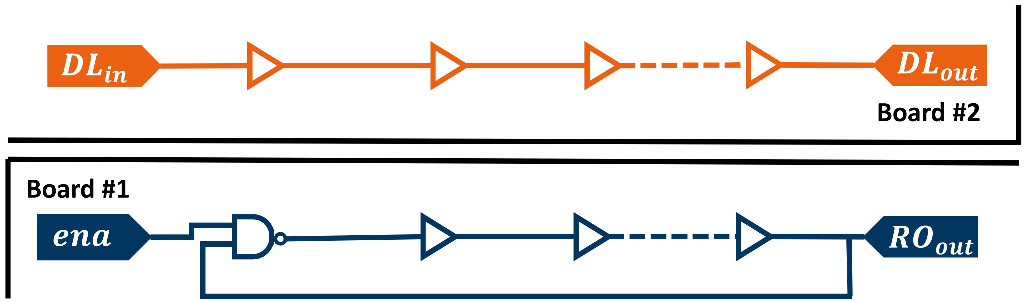
2. Low interlacing



3. Side-by-side

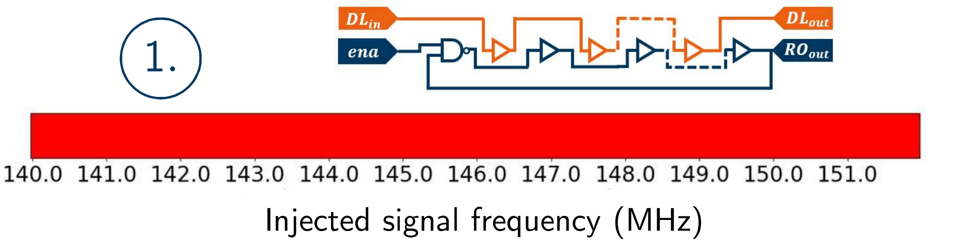


4. Two boards (reference configuration)

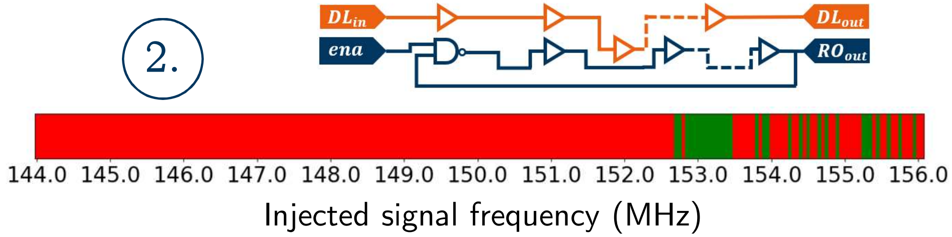


EXPERIMENTAL RESULTS

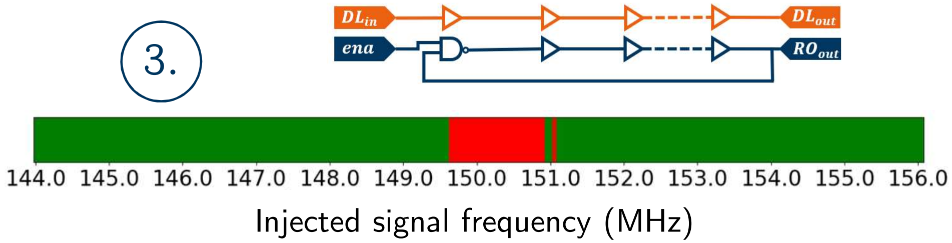
1.



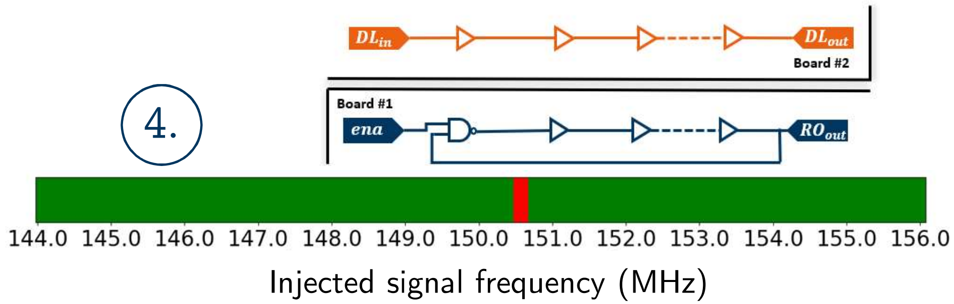
2.



3.



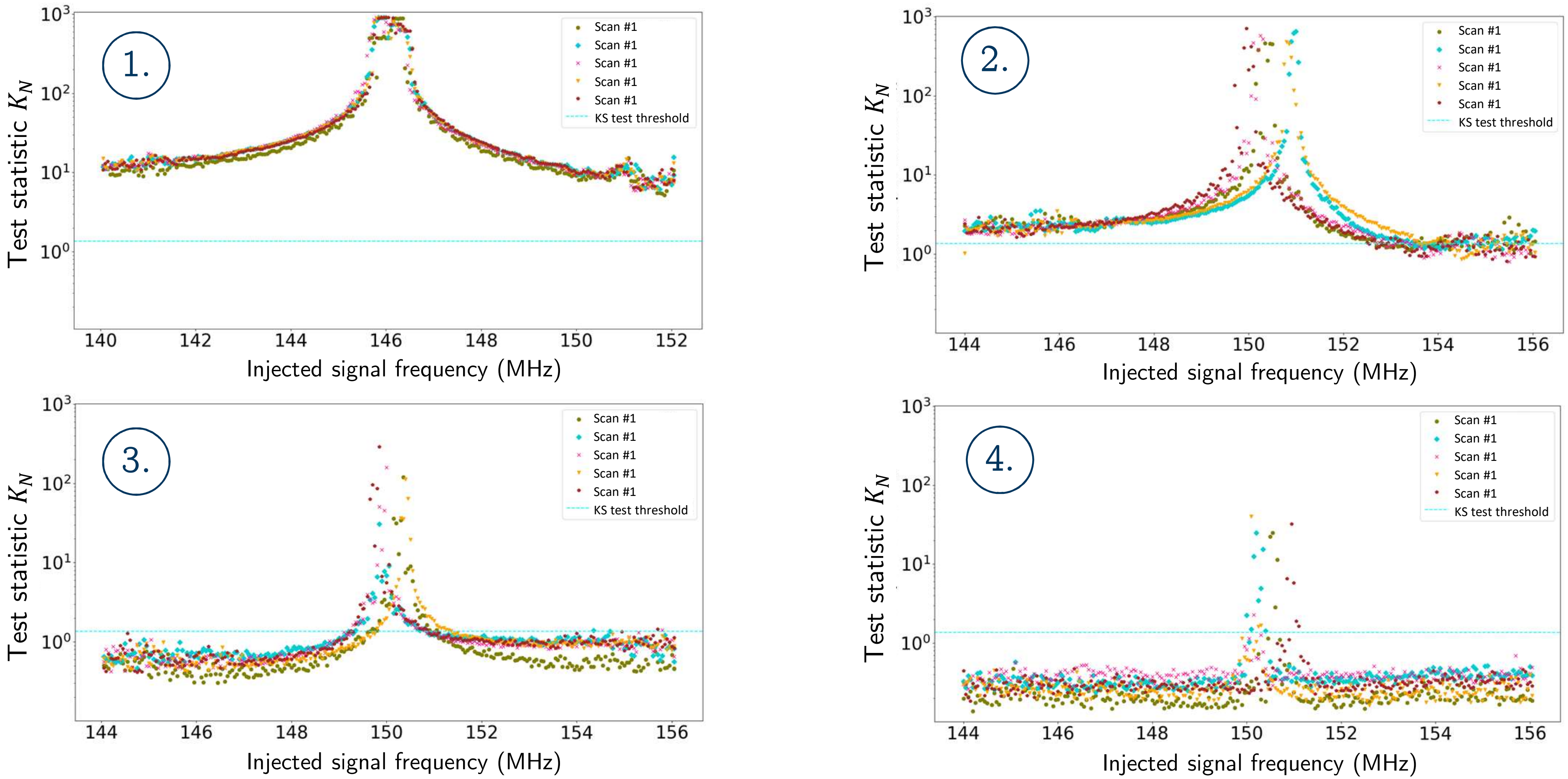
4.



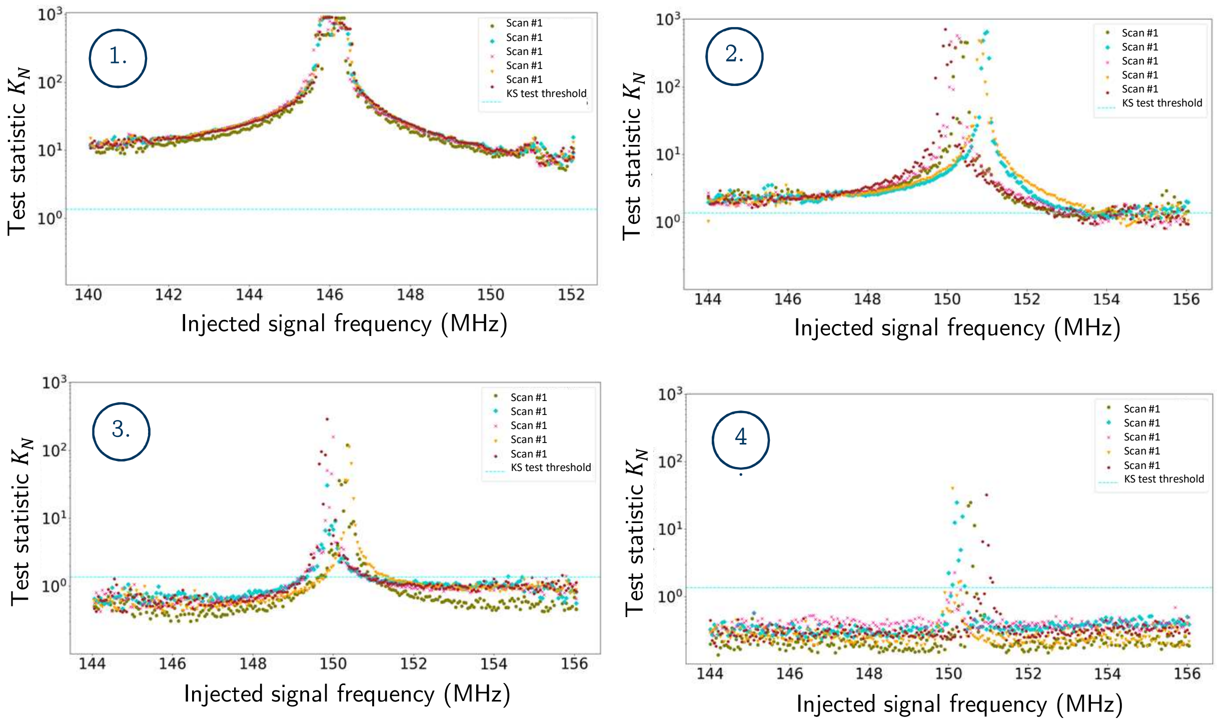
- When KS test fail, there are clusters in the phase differences distribution.
- The greater the risk of interference, the higher the number of KS tests that fail during the scan.

Detection of a mutual influence

EXPERIMENTAL RESULTS

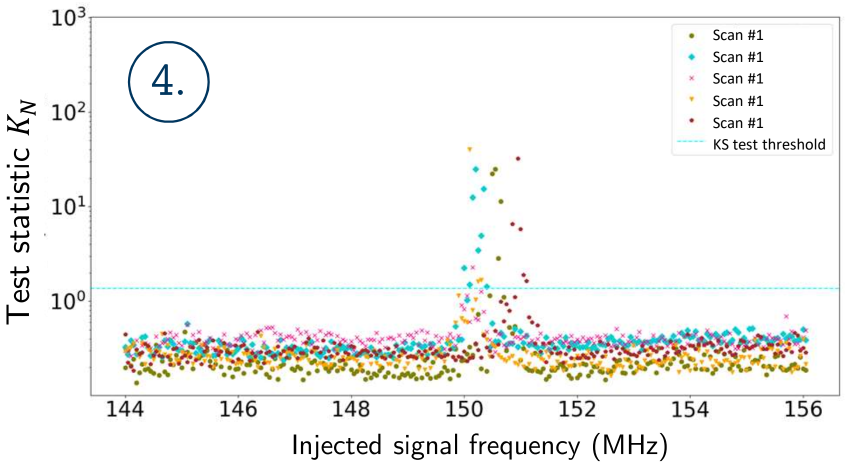


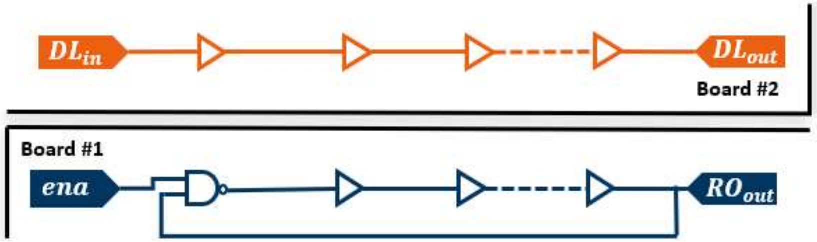
EXPERIMENTAL RESULTS



- Equivalent values of K_N regardless of the scan: **reproductibility.**
- The strength of influence varies depending on the risk of influence.
- Distinction between an area of strong influence and an area of weak influence.
- More relevant than the standard deviation of phase differences.

EXPERIMENTAL RESULTS





No physical cause, but the KS test fails

↪ Approximation of $\frac{f_{RO}}{f_{DL}}$ using the theory of continued fractions

- $f_{DL} = 150{,}50$ MHz ; $f_{RO} \approx 150{,}49$ MHz

$$\left.\begin{aligned} &\rightarrow \quad \frac{h_1}{k_1} = \frac{1}{1} \\ &\rightarrow \quad \frac{h_2}{k_2} = \frac{19360}{19361} \end{aligned}\right\} \quad f_{DL} \approx f_{RO}$$

The KS test can **detect**:

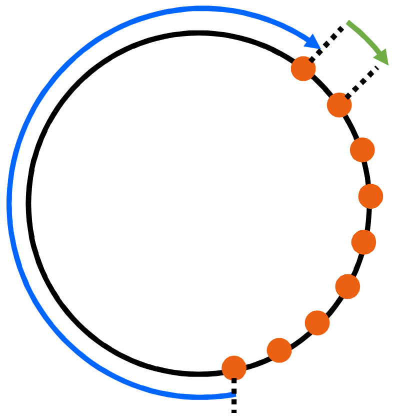
- an incorrect frequency ratio resulting from the implementation itself
- a mutual influence due to passive or active phenomenon

TEST REACTIVITY

$\hookrightarrow$ Set up a minimum sample size N to which the KS test is applied.

Distance between two consecutive phase differences
$\rightarrow$ **related to the error** in the frequency ratio approximation

Maximum distance
d_{max}



$$\boldsymbol{d_{max} < 0,001}$$

- Ensure that there are at least two contributors per jittered zones
- Ensure that the phase space is fully covered

We can adjust the number of samples to which the KS test is applied:

- need to know the frequency ratio
- to be performed prior to the TRNG going live, during the verification of the correct frequency ratios of the RO pairs.

CONCLUSION

The standard deviation of the phase differences does not guarantee that their distribution is **uniform**.

The uniformity of the phase differences ensures that:
- there are at least two contributors per jittered zones
- the phase space is fully covered

A deterioration in the frequency ratio can lead to the formation of clusters during sampling
$\rightarrow$ introduction and définition of **mutual influence** between two ROs.

A new metric for detecting mutual influence based on a statistical test of conformity to a uniform distribution.

Kolmogorov-Smirnov test: suitable for phase difference samples, quantification of the influence, evaluation of distribution uniformity.
- detection of incorrect frequency ratios coming from the implementation itself
- detection of a deterioration in the frequency ratio caused by physical phenomena

Éloïse Delolme *et al.*« **Beyond Total Locking: Demonstrating and Measuring Mutual Influence on a RO-based True Random Number Generator on an FPGA** ». *2024 IEEE System-On-Chip Conference (SOCC 2024)*, Sept 2024

OBJECTIVES

TO UNDERSTAND

• Identification of the factors contributing to the occurrence of the locking phenomenon.

→ Recommendations for ROs implementation.

TO DETECT

• Detection of a loss of uniformity in phase difference samples.

→ Precise method.

TO EMBED

• Implementation of an embedded detection method.

→ On-line test.

PILLING-UP LEMMA

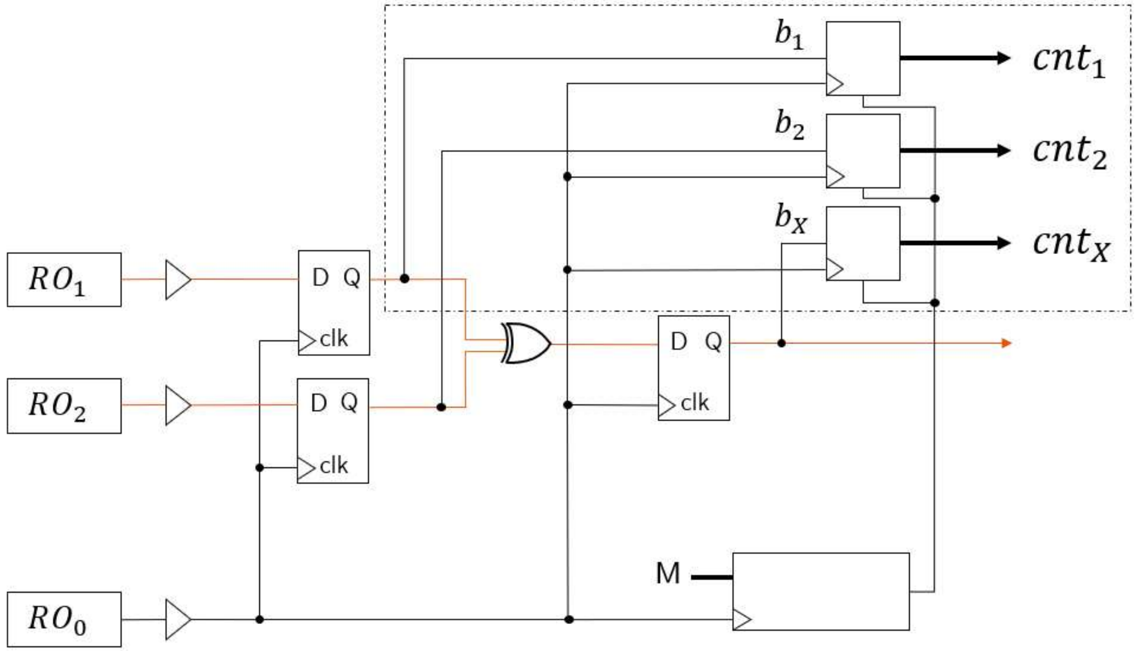
"The probability that the XOR operation between several random variables with values in {0,1}, when they are independent, equals 0 is given by:

$$\mathbb{P}(X_1 \oplus X_2 \oplus \cdots \oplus X_N = 0) = \frac{1}{2} + 2^{N-1} \prod_{i=1}^{N} \varepsilon_i$$

with $\varepsilon_i = \mathbb{P}(X_i = 0) - \frac{1}{2}$ the bias of the random variable X_i"

When N = 2, with X_1 and X_2 are independent : $\mathbb{P}(X_1 \oplus X_2 = 0) = \frac{1}{2} + 2\varepsilon_1\varepsilon_2$

INTERNAL BIAS RECOVERY



- X_1 : the binary random variable with values in $\{0,1\}$ representing the value sampled by a rising edge of RO_0 on RO_1.

- X_2 : the binary random variable with values in $\{0,1\}$ representing the value sampled by a rising edge of RO_0 on RO_2.

- $\widetilde{\varepsilon_i}$ where $i \in \{1,2\}$: an estimation of the quantity ε_i : $\widetilde{\varepsilon_i} = \left|\frac{1}{2} - \frac{cnt_i}{M}\right|$

- $\widetilde{\varepsilon_X}$: an estimation of the quantity ε_X : $\widetilde{\varepsilon_X} = \left|\frac{1}{2} - \frac{cnt_X}{M}\right|$

- $\widetilde{p_X}$: an estimation of the quantity $\mathbb{P}(X_1 \oplus X_2 = 0)$: $\widetilde{p_X} = 1 - \frac{cnt_X}{M}$

OBJECTIVES

Detect, during operation, mutual influence or an incorrect frequency ratio between different pairs of ROs:

- the sampling RO and a sampled RO
- two sampled ROs

Use the contrapositive of the pilling-up lemma :

→ if $\widetilde{p_X} \neq \frac{1}{2} + 2\widetilde{\varepsilon_1}\widetilde{\varepsilon_2}$ then the random variables X_1 and X_2 are not independent.

DIFFERENT CASES OF SIMULATION

The simulation is used to create incorrect frequency ratios for random generation.

D

$f_0 = f_2$
Creation of an incorrect frequency ratio between the sampling RO and a sampled RO → simulation of total lock.

C

$f_1 = f_2$
Simulation of a case of total lock between two sampled ROs.

B

$f_1 \approx f_2$
Creation of an incorrect frequency ratio between 2 sampled ROs: RO_1 and RO_2.

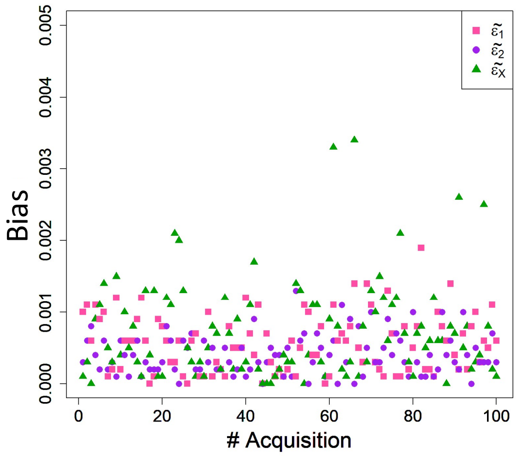
A

Reference configuration
No problematic frequency ratios.

SIMULATION RESULTS

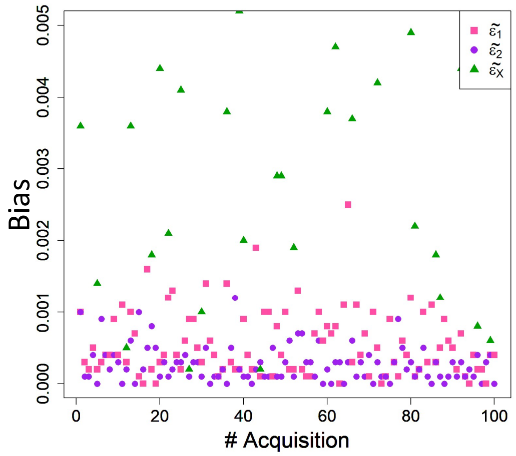
Reference configuration

A



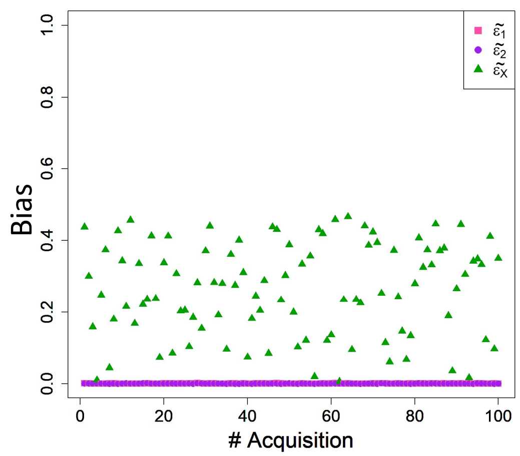
$f_1 \approx f_2$

B



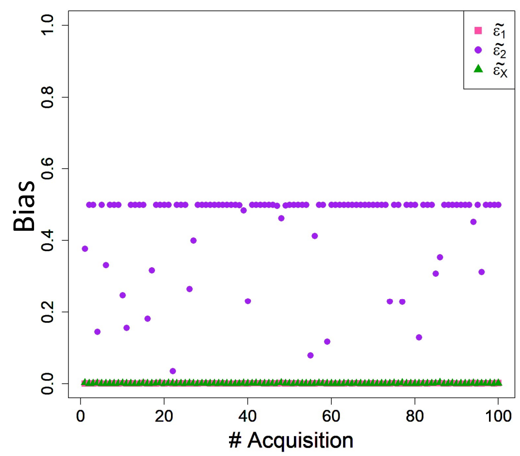
$f_1 = f_2$

C



$f_0 = f_2$

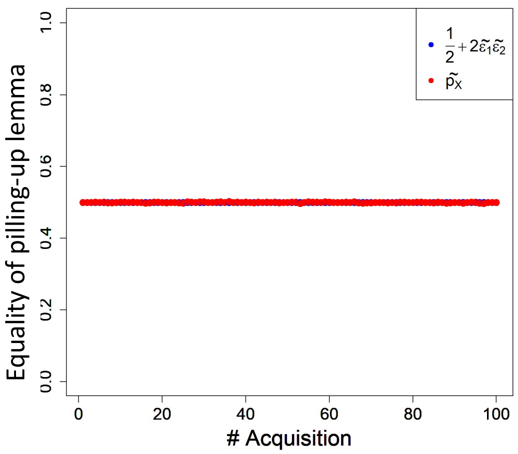
D

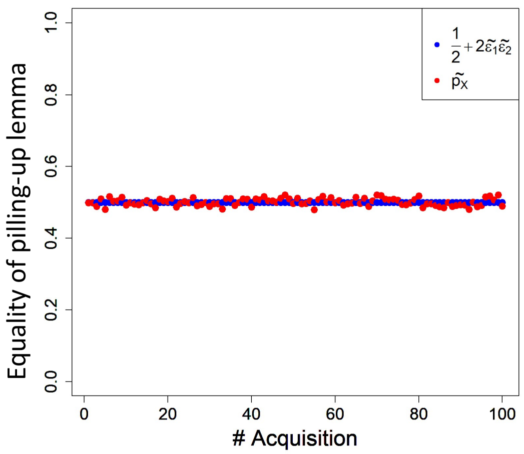


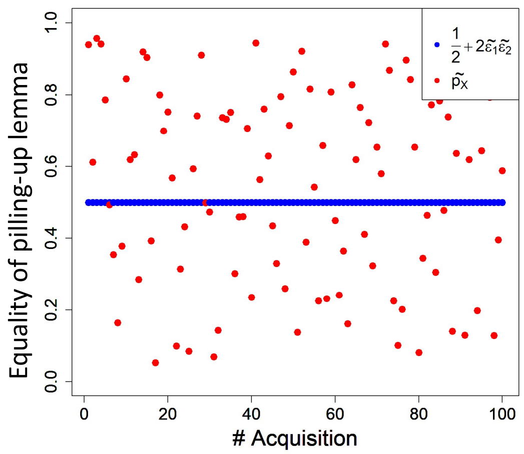
- Empirical bias at the output of the XOR operation $\widetilde{\varepsilon_X}$: strong and scattered when $f_{RO_1} = f_{RO_2}$
- Empirical bias at the output of the sampling of RO_2 by RO_0 $\widetilde{\varepsilon_2}$: strong

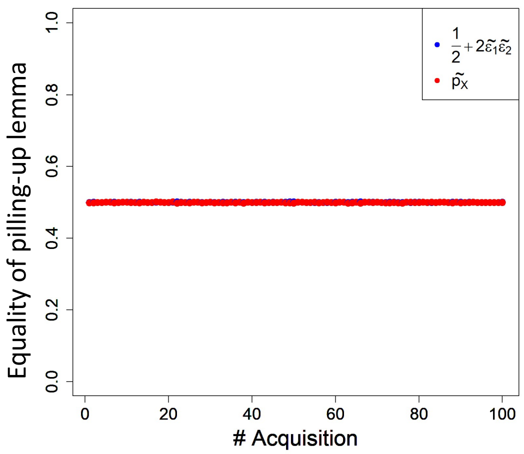
SIMULATION RESULTS

Reference configuration	$f_1 \approx f_2$	$f_1 = f_2$	$f_0 = f_2$
A	B	C	D









- A high dispersion of $\widetilde{p_X}$ allows us to detect an incorrect frequency ratio between two sampled ROs.
- An increase in the empiricial bias at the end of the sampling process $\widetilde{\varepsilon_2}$ allows us to detect an incorrect frequency ratio between a sampled RO and the sampling RO.

DIFFERENT CASES OF IMPLEMENTATION

The implementation is used to cause a mutual influence between different ROs (using results from the empirical study).

PR1

Minimization of mutual influence and unproblematic frequency ratios

PR2

Minimization of mutual influence for different frequency ratios

PR3

Maximization of mutual influence for different frequency ratios

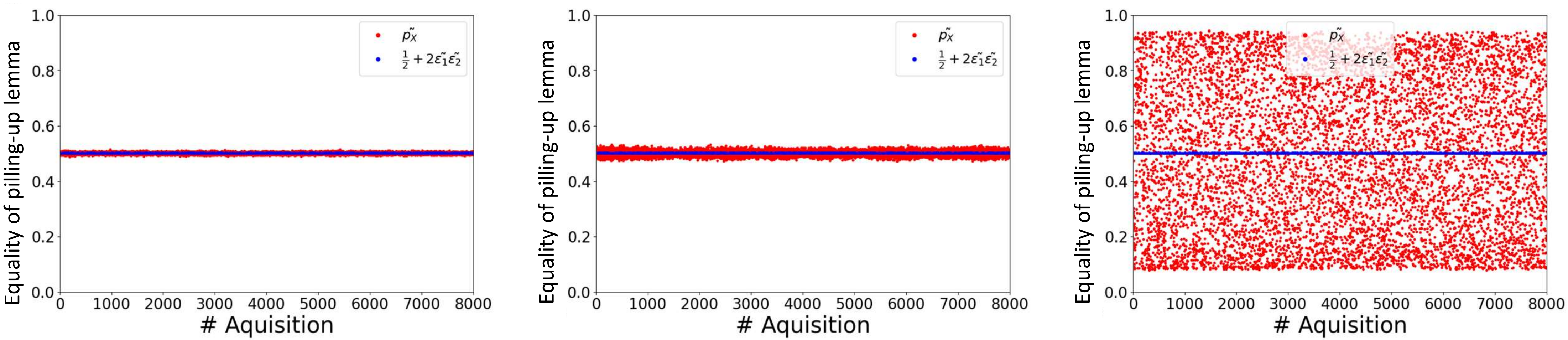
IMPLEMENTATION RESULTS

- Detection of an incorrect frequency ratio between two sampled ROs with a high dispersion of $\widetilde{p_X}$

Good frequency ratios betwwen f_{RO_2} and f_{RO_1}

f_{RO_2} near f_{RO_1}

f_{RO_2} equal to f_{RO_1}



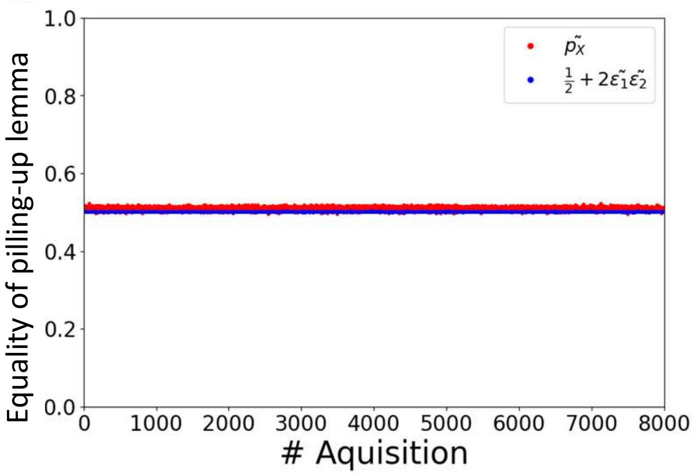
Minimization of mutual influence for different frequency ratios

PR2

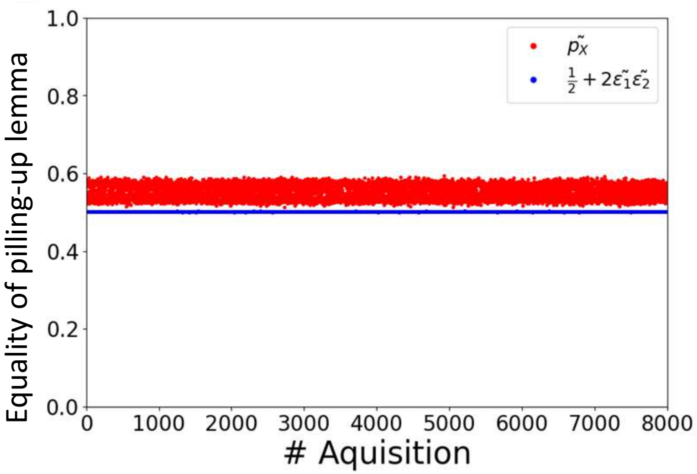
IMPLEMENTATION RESULTS

- Detection of a mutual influence between two sampled ROs with a shift in the mean value of $\widetilde{p_X}$

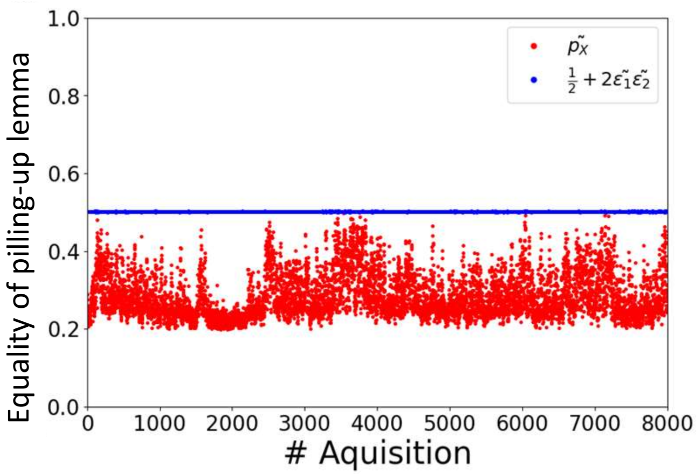
Good frequency ratio between f_{RO_2} and f_{RO_1}



f_{RO_2} near f_{RO_1}



f_{RO_2} equal to f_{RO_1}



Maximization of mutual influence for different frequency ratios

PR3

RÉSULTATS DE L'IMPLANTATION RÉELLE

- Detection of a mutual influence between two sampled ROs with a shift in the mean value of $\widetilde{p_X}$

Davies formula:[9]

$$\mathbb{P}(X_1 \oplus X_2 = 1) = \frac{1}{2} - 2\left(\frac{1}{2} - p_1\right)\left(\frac{1}{2} - p_2\right) - \rho_{12}\sqrt{(1-p_1)p_1(1-p_2)p_2}$$

$p_1 = \mathbb{P}(X_1 = 0) = \frac{1}{2} + \varepsilon_1$
$p_2 = \mathbb{P}(X_2 = 0) = \frac{1}{2} + \varepsilon_2$
ρ_{12} : correlation between X_1 and X_2

When ε_1 and ε_2 are small, we have:

$$\mathbb{P}(X_1 \oplus X_2 = 0) = \frac{1}{2} + 2\varepsilon_1\varepsilon_2 + \frac{\rho_{12}}{4}$$

The term $\frac{\rho_{12}}{4}$, which relates to the correlation between the random variables X_1 and X_2, accounts for the shift in the mean value, reflecting a mutual influence between RO_1 and RO_2.

[9] Robert B. Davies. *Exclusive or (xor) and hardware random number generators*. 2002.

CONCLUSION

Detection of an incorrect frequency ratio between the sampling RO and a sampled RO : increase in the empirical bias at the output of the sampling.

Detection of an incorrect frequency ratio between two sampled ROs:
$\rightarrow$ dispersion of the empirical probability $\widetilde{p_X}$ to obtain a '0' at the output of the XOR operation

Detection of an mutual influence between two sampled ROs:
$\rightarrow$ shift in the mean value of the empirical probability $\widetilde{p_X}$ to obtain a '0' at the output of the XOR operation

Article **currently being written**

OVERALL CONCLUSION

Mutual influence detection

- **Mutual influence** : a broader concept encompassing the locking phenomenon
- New metric: goodness-of-fit test → Kolmogorov-Smirnov test
- Detection of incorrect initial frequency ratios between the sampling RO and a sampled RO
- Detection of deteriorations caused by active or passive physical phenomena

Embedded detection method

- Using the contrapositive of the pilling-up lemma
- Detection of incorrect frequency ratios between different pairs of ROs on a MURO-TRNG with 2 sampled ROs
- Detection of a mutual influence between two sampled ROs on a MURO-TRNG with 2 sampled ROs

PERSPECTIVES

- Estimate the order of magnitude of the number of samples to which the Kolmogorov-Smirnov test should be applied, based on the frequency ratio under consideration, in order to achieve a good balance between responsiveness and accuracy.
- Development of a "turnkey" tool that incorporates the proposed methodology to simplify its use and encourage its adoption in practical and industrial settings.
- Improving the embedded detection method to make it efficient and cost-effective when deployed on MURO architectures with more than two sampled ROs.
- Estimate of the percentage of ROs that were influenced in adjusting the safety margins established by the designers.

Thank you for your attention !

Eloïse DELOLME

29^{th} May 2026

Study, characterization, and detection of locking in oscillating rings used in random number generators.

SemSecuElec seminar

29^{th} May 2026

Eloïse DELOLME

Laboratoire Hubert Curien
UMR • CNRS • 5516 • Saint-Étienne