Locking phenomenon on ring oscillators used in True Random Number Generators

Éloïse DELOLME

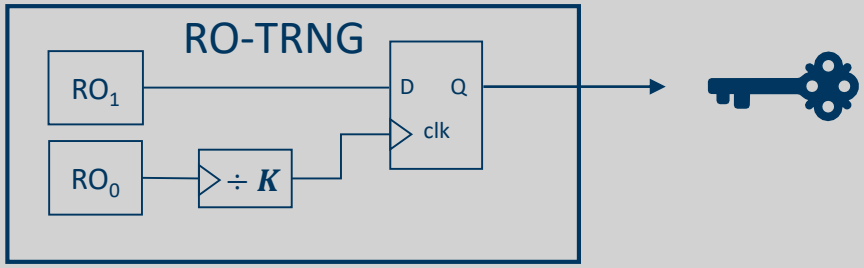
CryptArchi
June 12th 2023

Thesis supervisor :
- Viktor FISCHER[1]

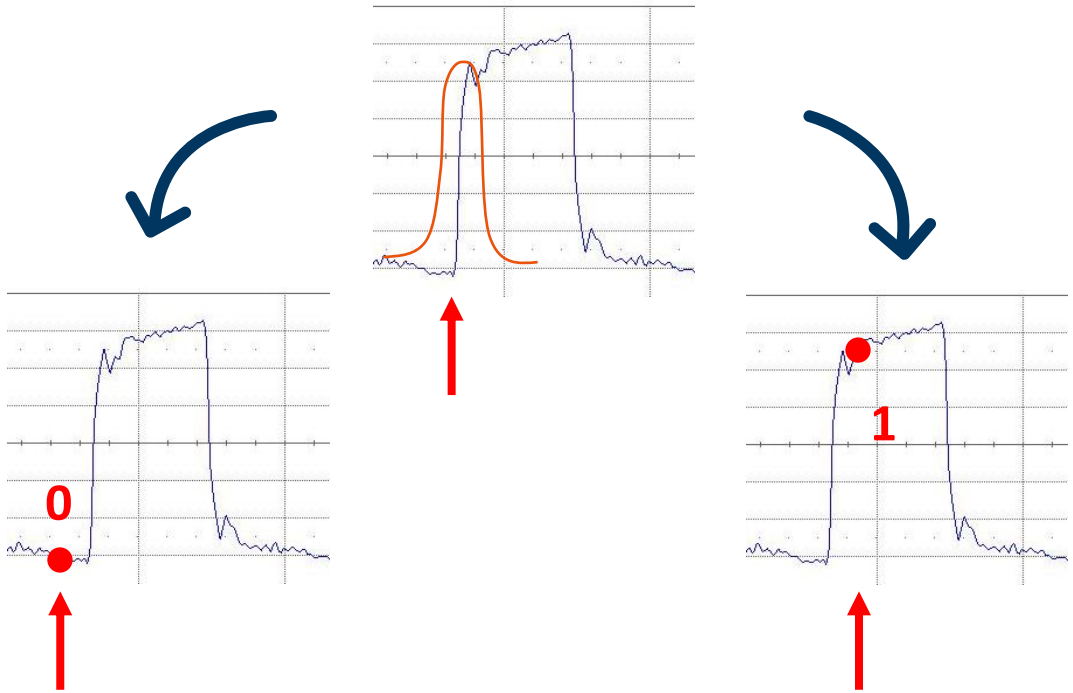
Co-advisors :
- Florent BERNARD[1]
- Nathalie BOCHARD[1]
- David LUBICZ[2]
- Maxime PELCAT[3]

1 LABORATOIRE HUBERT CURIEN UMR • CNRS • 5516 • SAINT-ETIENNE
UNIVERSITÉ DE LYON
UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE
cnrs
2 DGA DIRECTION GÉNÉRALE DE L'ARMEMENT
3 INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

INTRODUCTION



- Easy implementation on FPGA
- Model known and caracterized

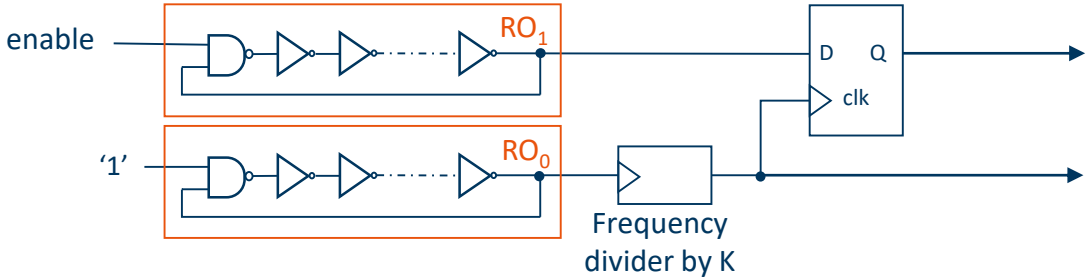


Randomness sources : noises

↪ all ROs are impacted by local and global noises

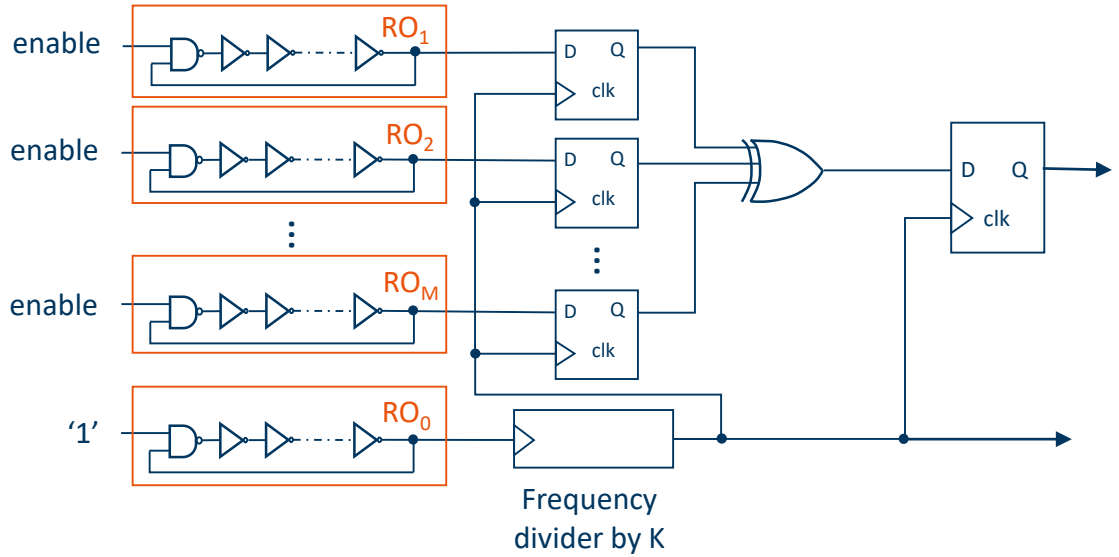
Jitter : rising edges are distributed around the nominal period according to a Gaussian curve

FROM TRNGs BASED ON ERO TO MURO



ERO-TRNG

- High accumulation time i.e large K
- Low throughput



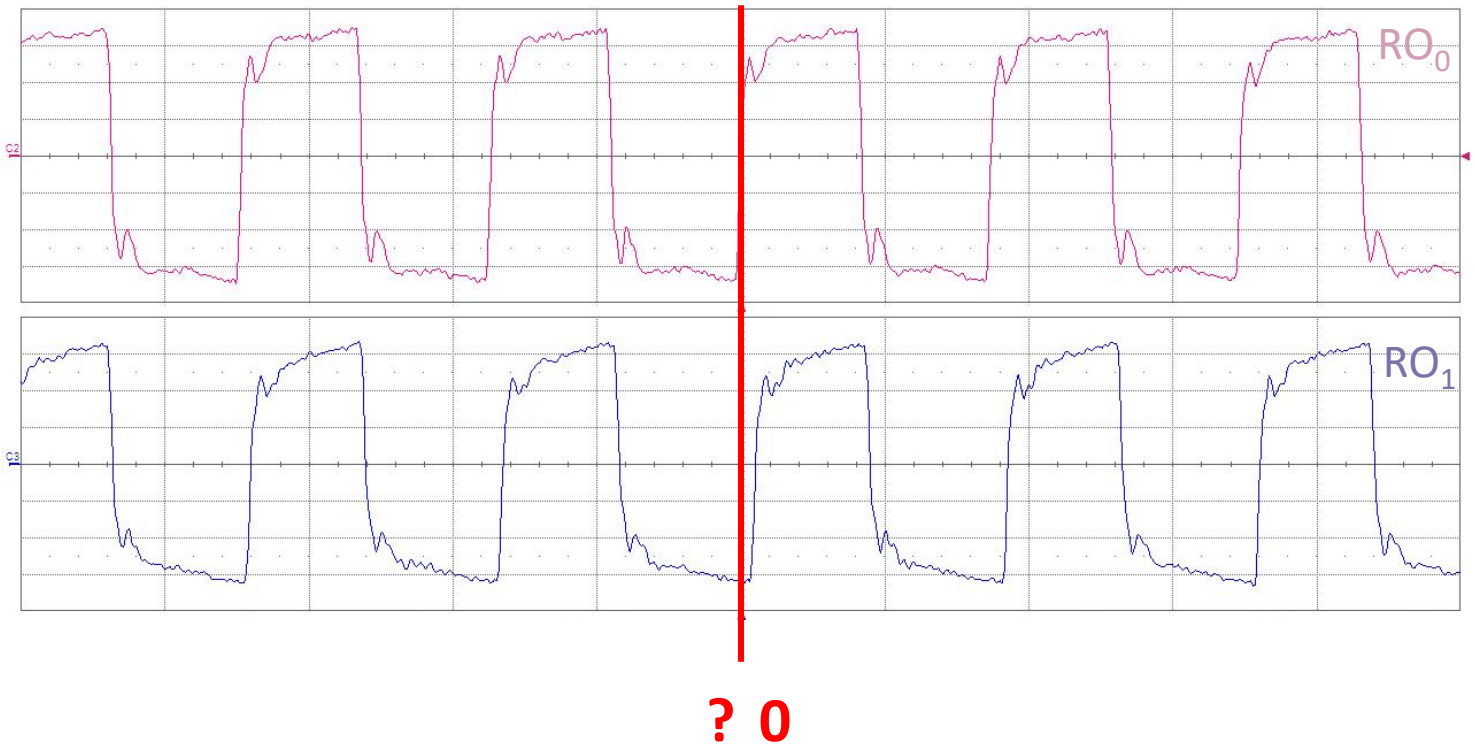
MURO-TRNG

- Lower accumulation time i.e. short K
- Better throughput
- Model relies on the assumption that **ROs are independent**

TABLE OF CONTENTS

- ❑ What is locking phenomenon?
- ❑ Experimental setup and design
- ❑ Metric used to characterize locking strength
- ❑ Causes of locking and experimental results
- ❑ Conclusion and future work

WHAT IS LOCKING PHENOMENON?



Trigger set on RO_0

3 steps :

1. Free oscillations of RO_0 and RO_1
2. RO_0 and RO_1 locked
3. Free oscillations of RO_0 and RO_1

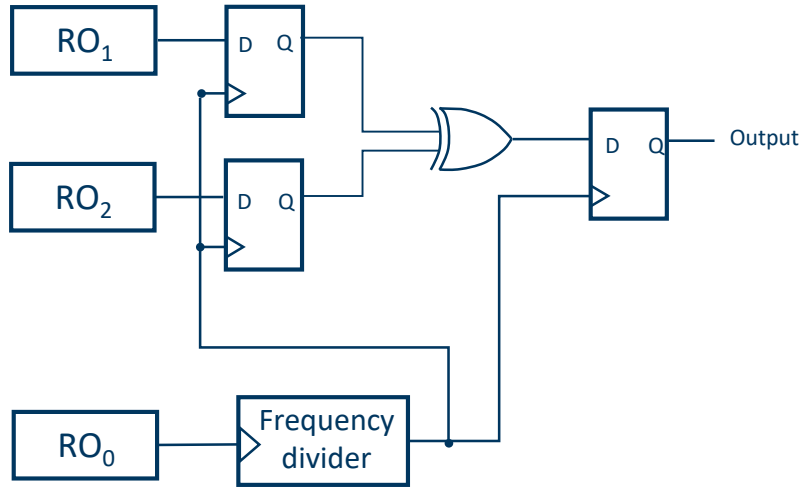
TABLE OF CONTENTS

EXPERIMENTAL SETUP

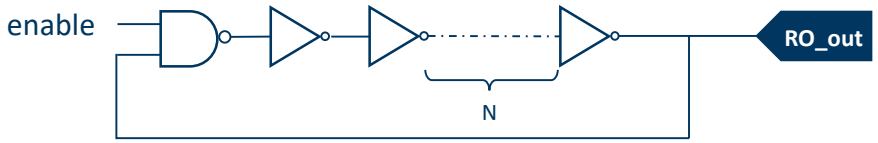
- Understand the locking phenomenon
- Characterize it
- Establish configurations and/or conditions maximising the locking

↪ Provide recommendations for the TRNG implementation

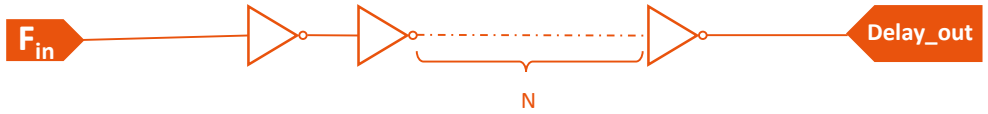
SPONTANEOUS LOCKING



EXPERIMENTAL DESIGN

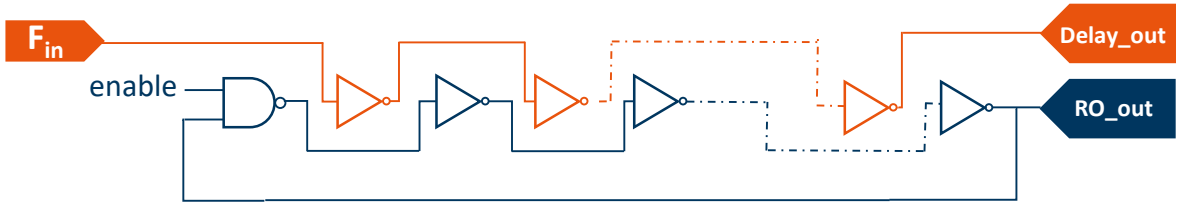


Ring Oscillator

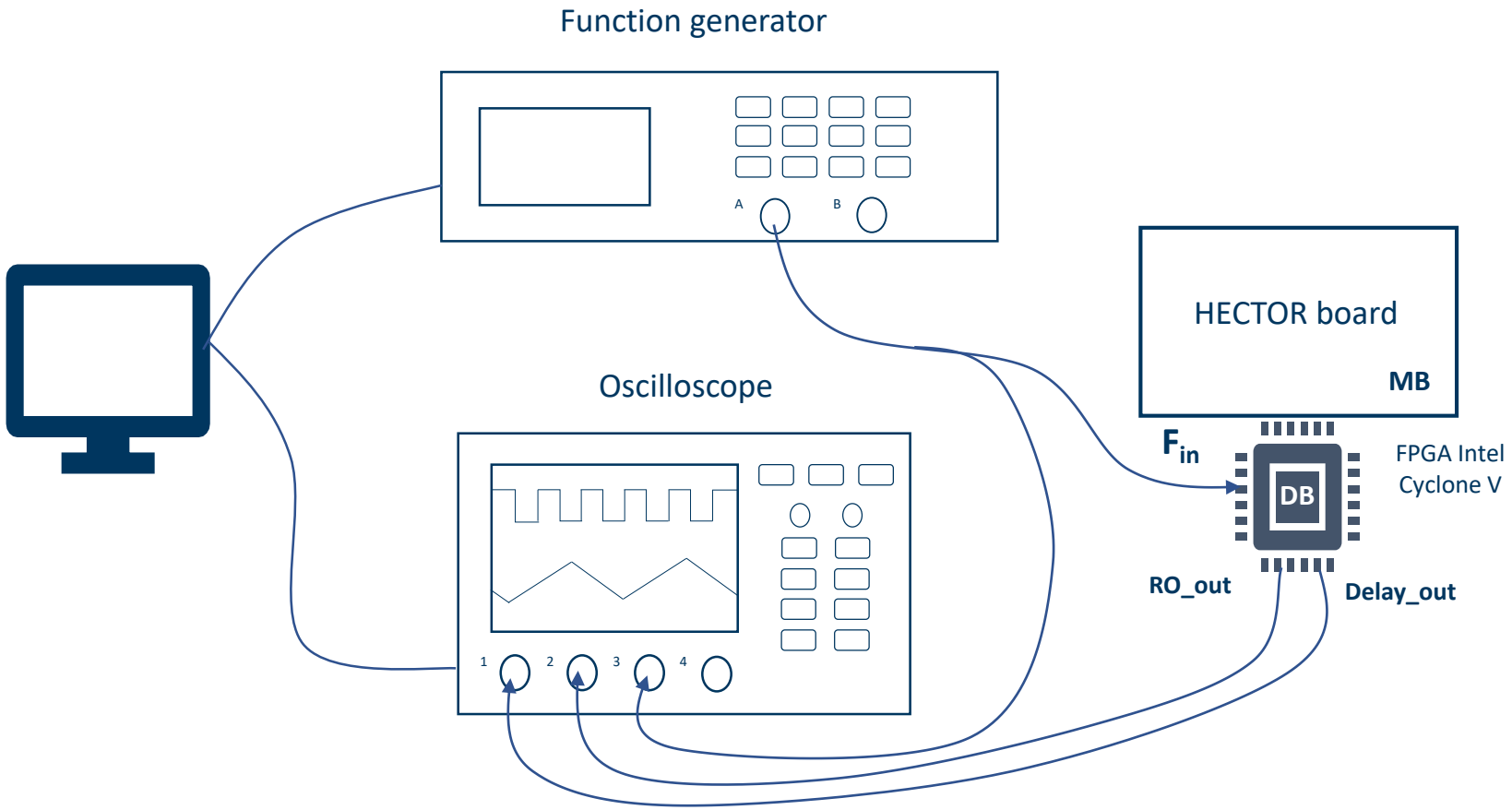


Delay Line

ENFORCED LOCKING



EXPERIMENTAL SETUP



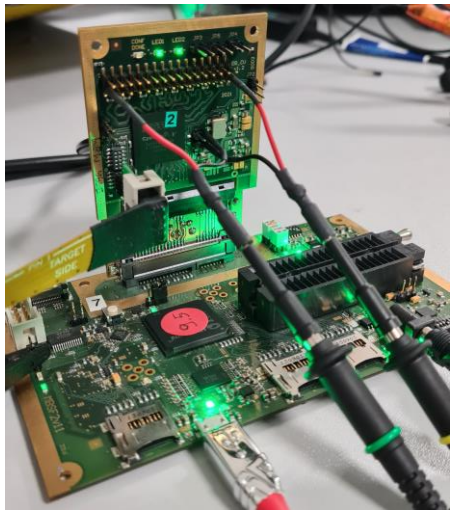
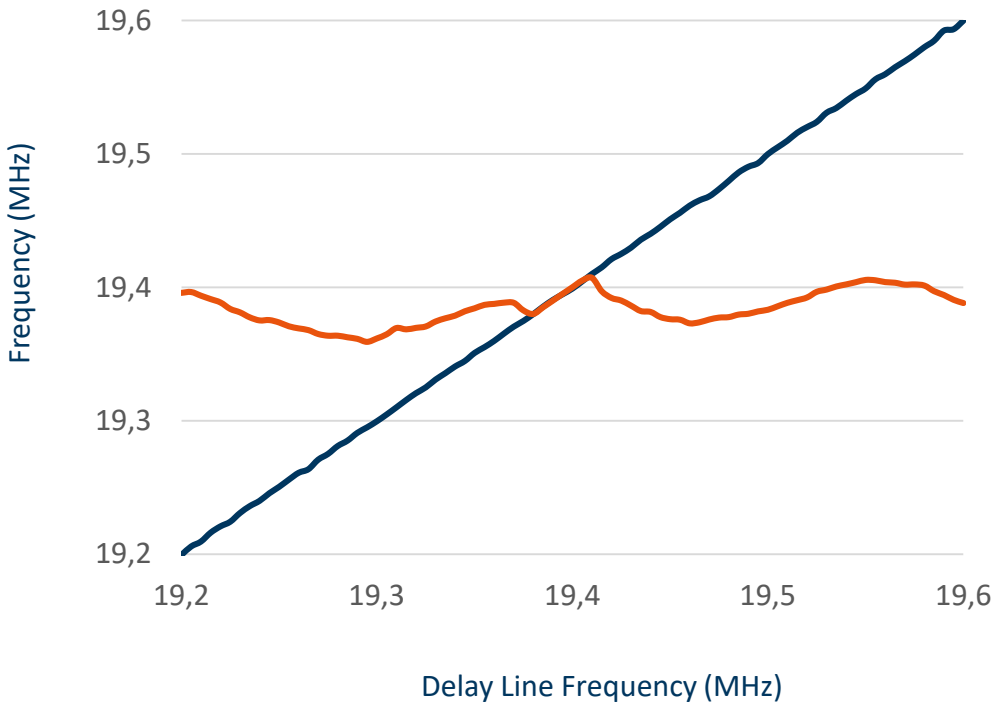
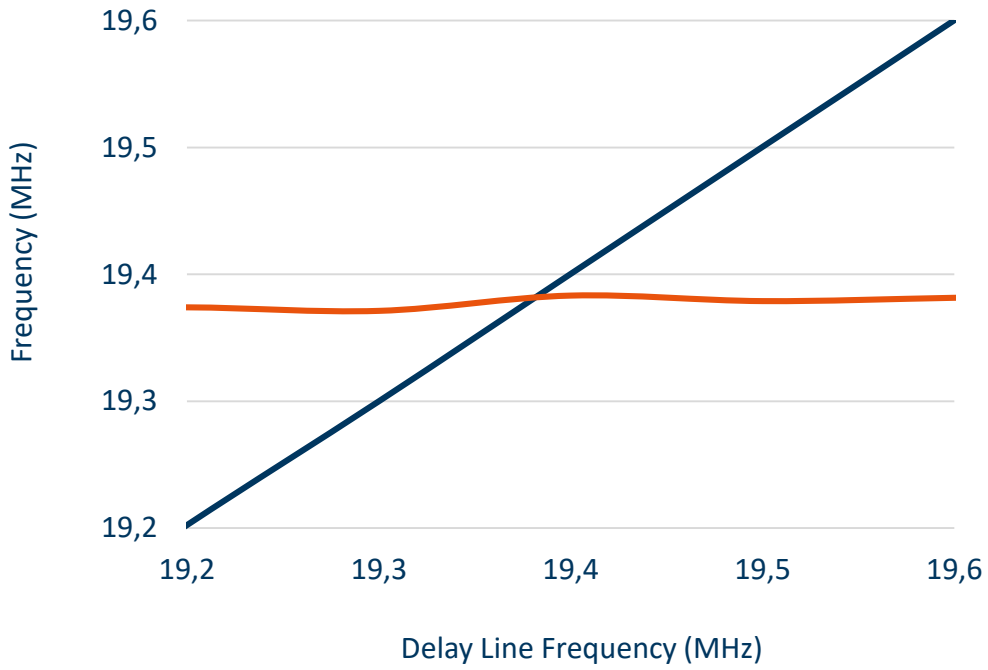


TABLE OF CONTENTS

METRIC USED TO CARACTERIZE LOCKING STRENGH





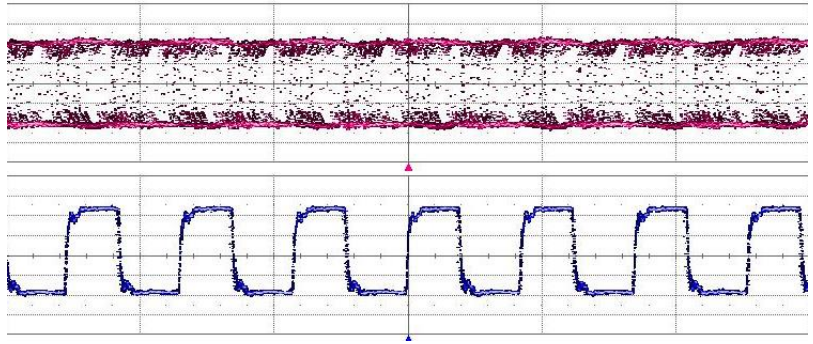
Delay Line
Ring Oscillator

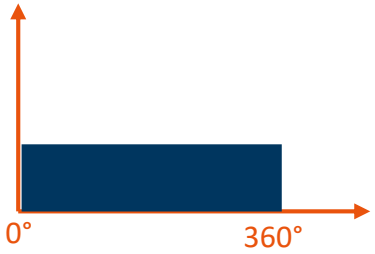
METRIC USED TO CARACTERIZE LOCKING STRENGH

Independent

RO

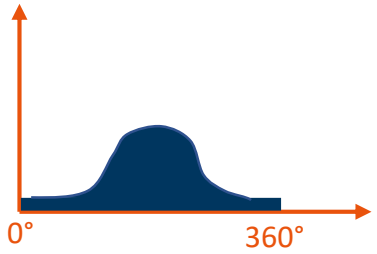
Delay Line

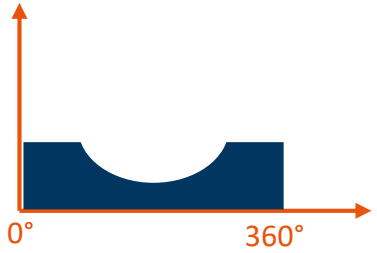




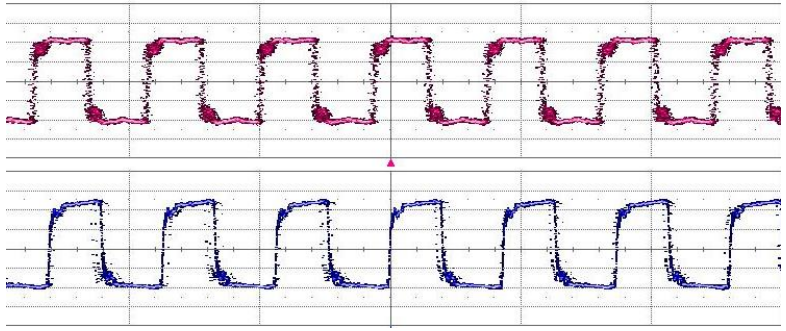
PERSISTENCY

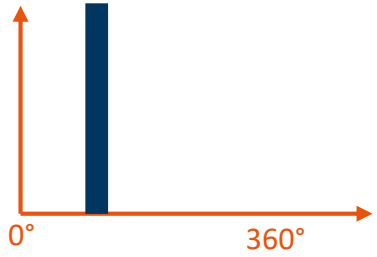
Trigger set on Delay Line





Locked





ROs are considered independent when their phase difference is uniformely distributed over the range 0-360°.

METRIC USED TO CARACTERIZE LOCKING STRENGH

Standard deviation of a uniform distribution over the range [a,b] :

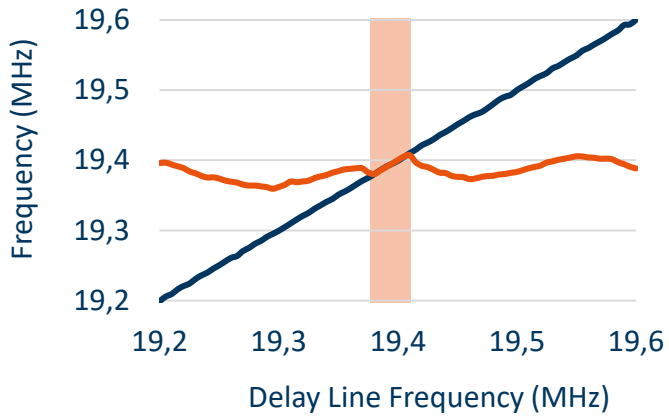
$$sdPhase = \frac{b - a}{\sqrt{12}} = \frac{360}{\sqrt{12}} = \mathbf{103,9°}$$

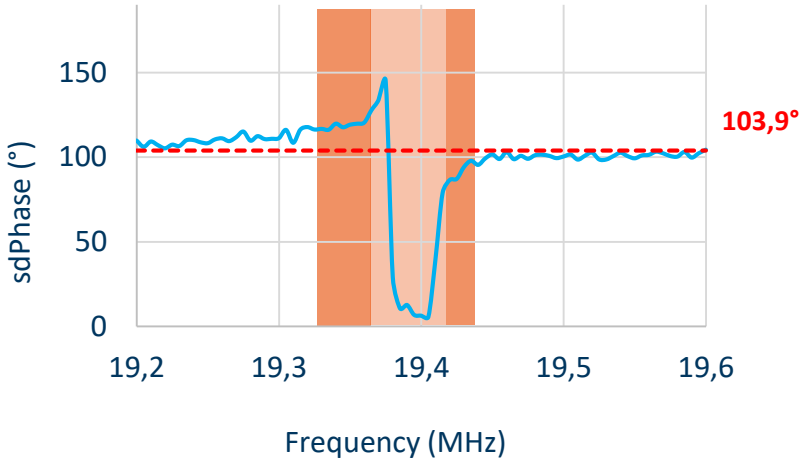
Locking : phenomenon caracterized by a **deviation from** the ideal value **103,9°** in the standard deviation of the phase difference between two ring oscillators.

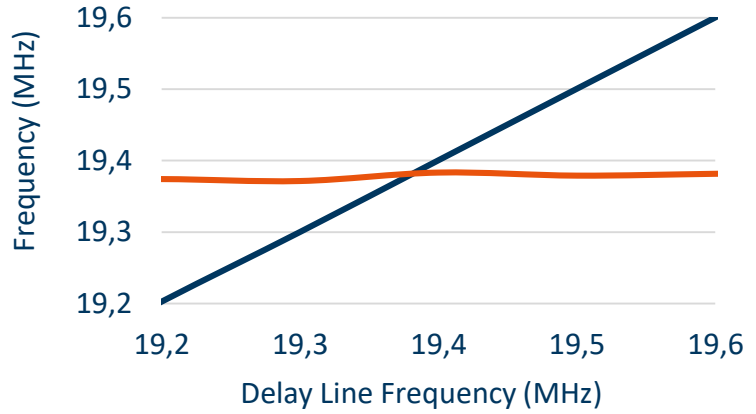
METRIC USED TO CARACTERIZE LOCKING STRENGH

Full Locking range

Partial Locking range







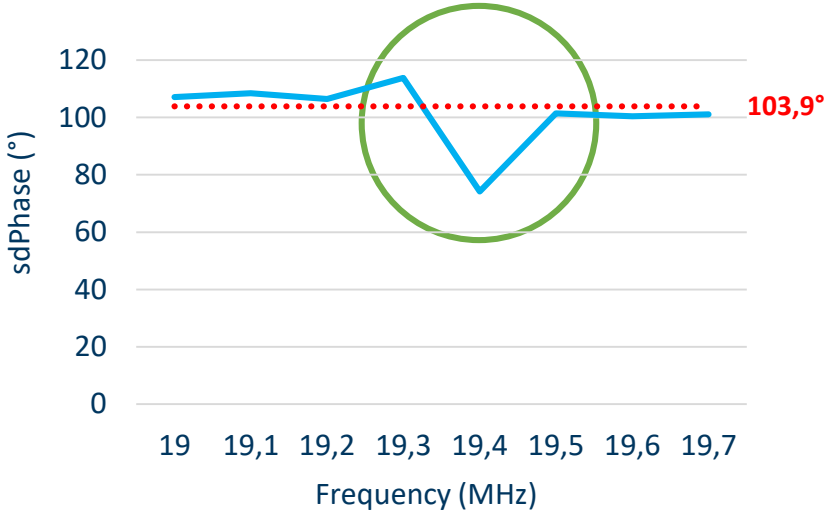
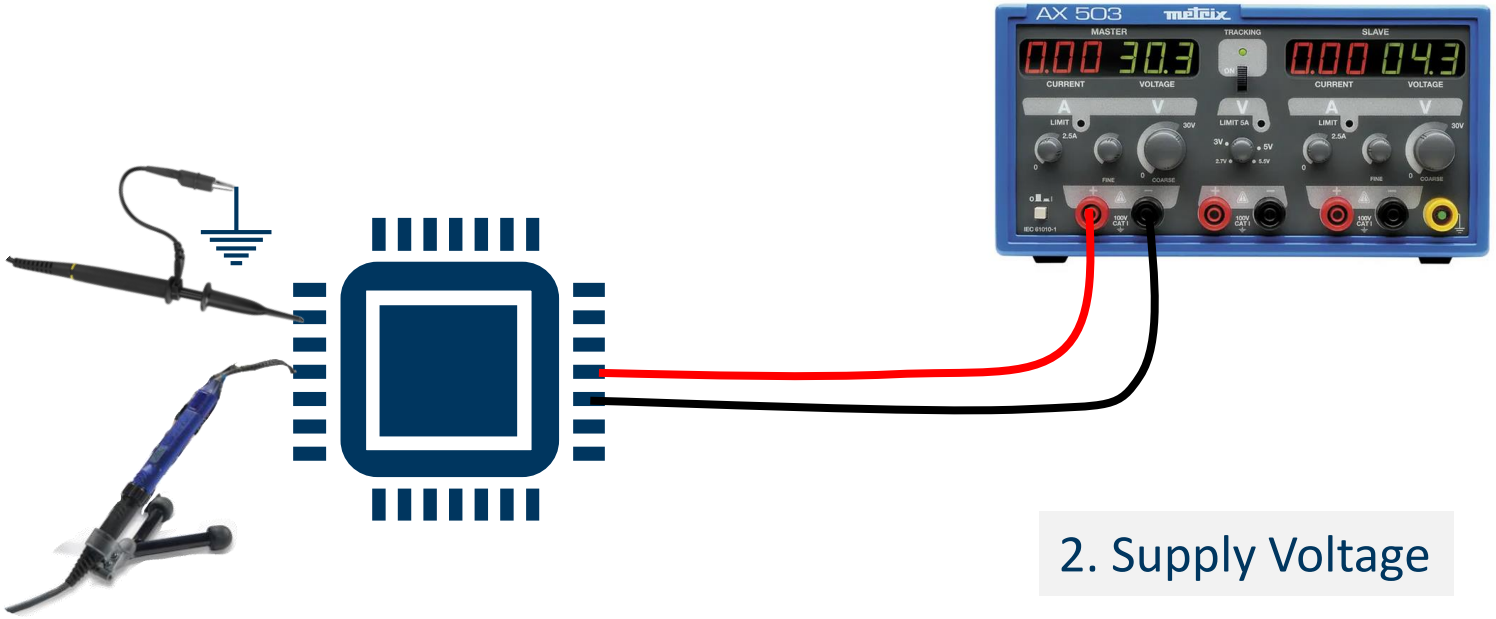


TABLE OF CONTENTS

EXPERIMENTS – *EXTERNAL CAUSES*

Single-ended probes

Differential probes

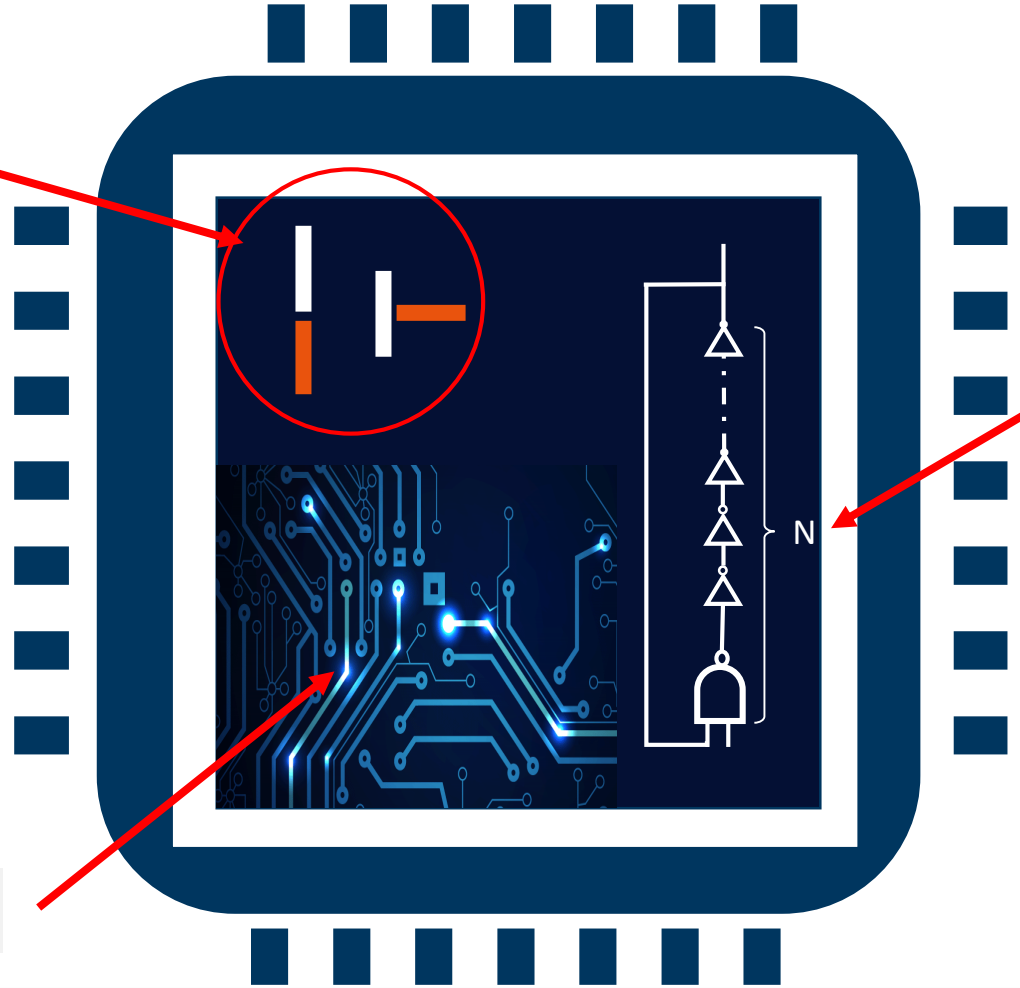


1. Probe type

2. Supply Voltage

EXPERIMENT – *INTERNAL CAUSES*

3. Relative placement

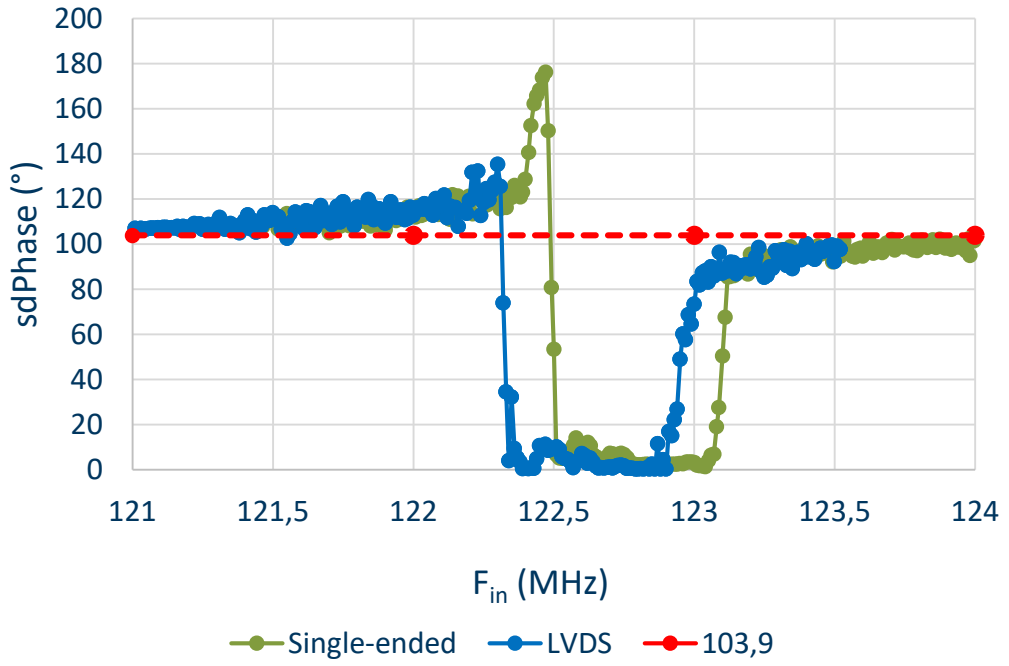


5. # elements in RO

4. Routing paths

EXPERIMENTAL RESULTS – *PROBES TYPE*

- Impact of signal output probe type on locking range



↪ Use of an external oscilloscope

↪ Differential probes are not always available on stock cards

Single-ended probes :

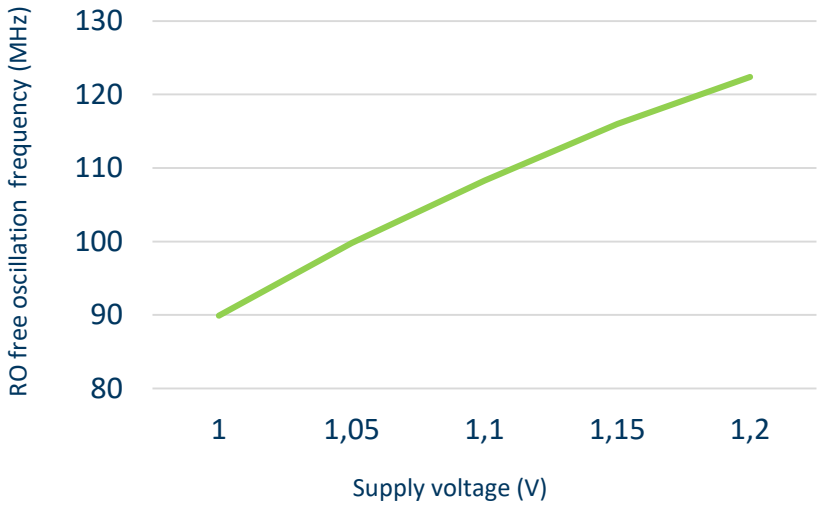
Ring free oscillation frequency : ≈ 122,68 MHz
Total locking range : 810 kHz

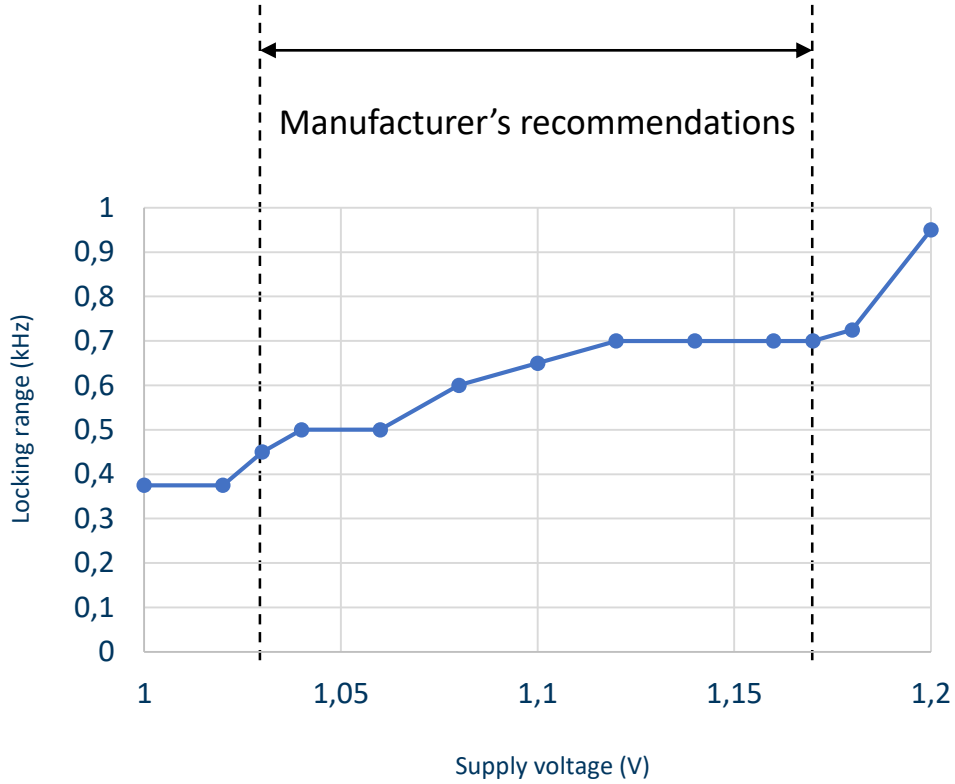
Differential probes :

Ring free oscillation frequency : ≈ 122,78 MHz
Total locking range : 750 kHz

EXPERIMENTAL RESULTS – *SUPPLY VOLTAGE*

- Impact of supply voltage on locking range

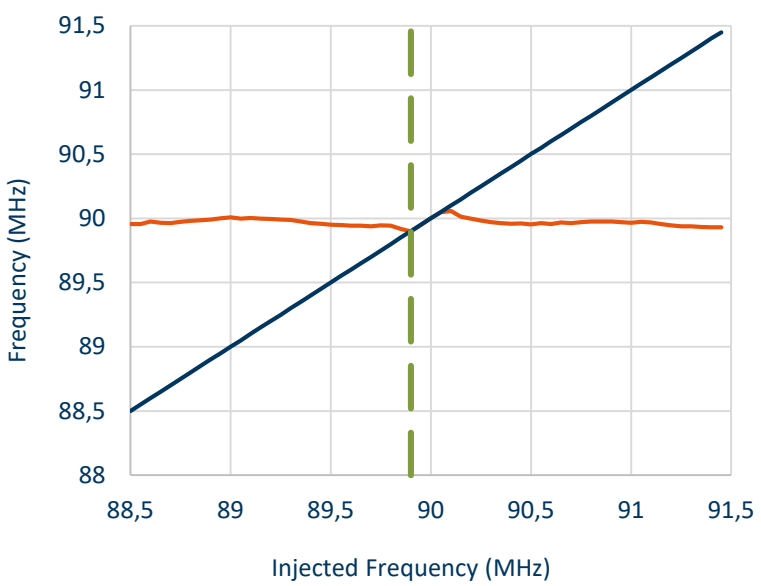




↪ Supply voltage modifies free oscillation frequency of the RO

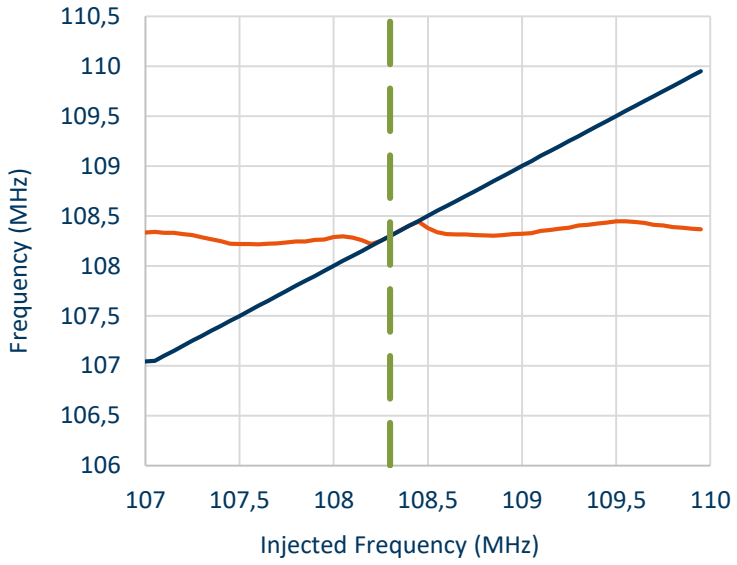
EXPERIMENTAL RESULTS – *SUPPLY VOLTAGE*

- Impact of supply voltage on the locking range

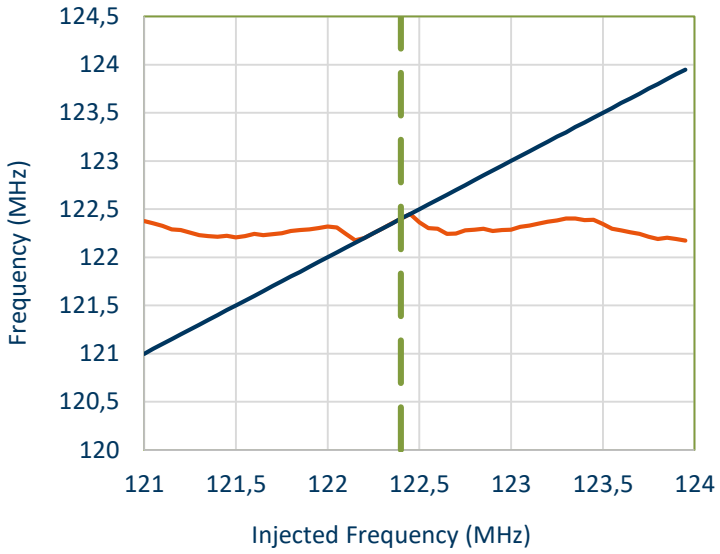


Supply Voltage : 1,0 V

(Outside manufacturer's recommendations)



Supply Voltage : 1,1 V



Supply Voltage : 1,2 V

(Outside manufacturer's recommendations)

F_{RO} (MHz)

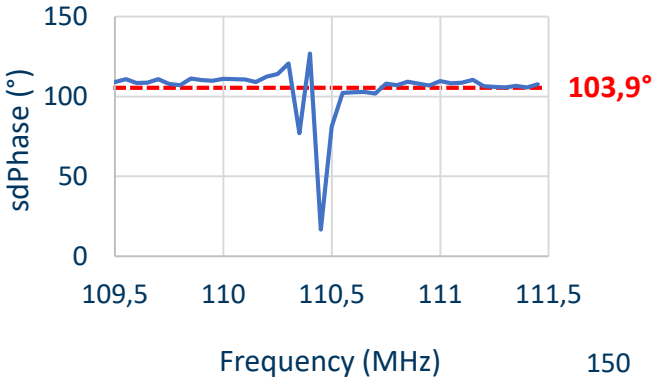
F_{in} (MHZ)

RO free oscillation frequency (MHz)

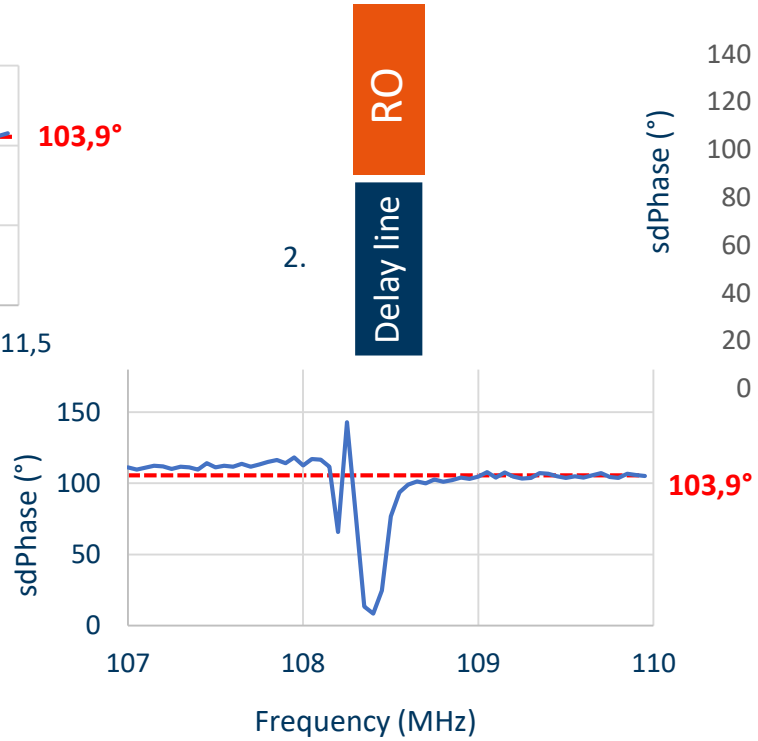
EXPERIMENTAL RESULTS – *RELATIVE PLACEMENTS*

- How relative placement between RO and delay line on FPGA affects locking range?

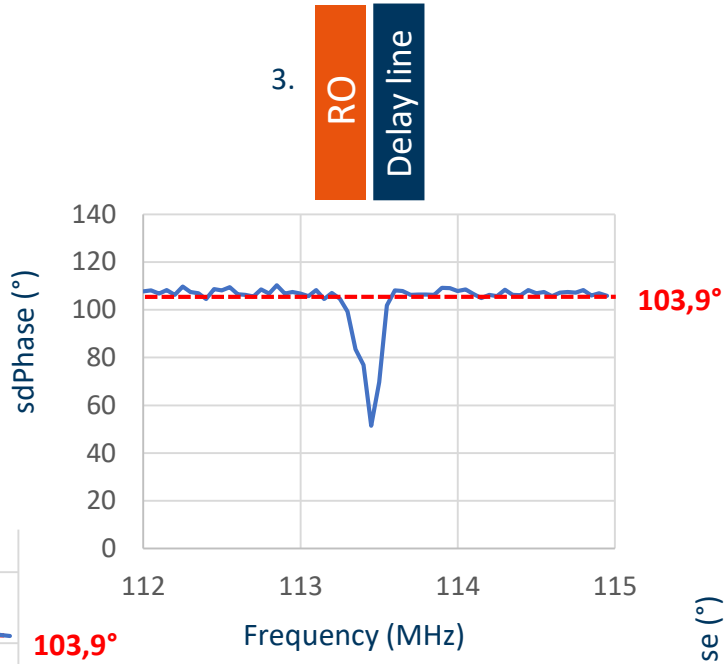
1.



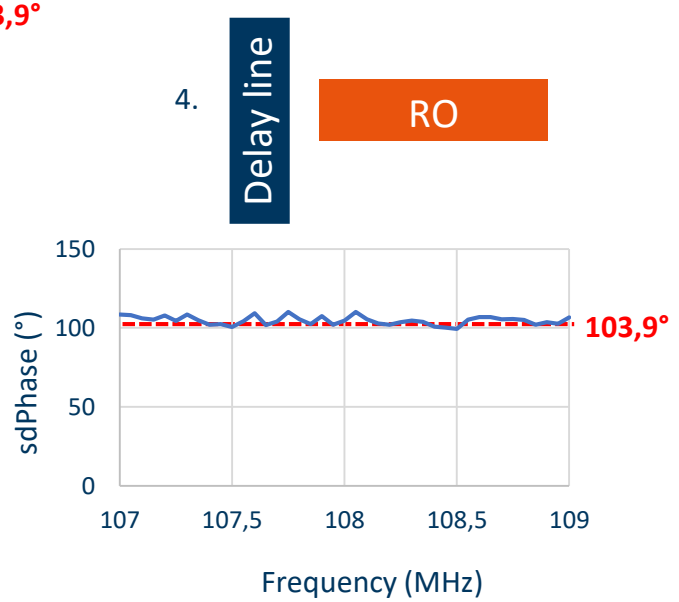
2.



3.



4.

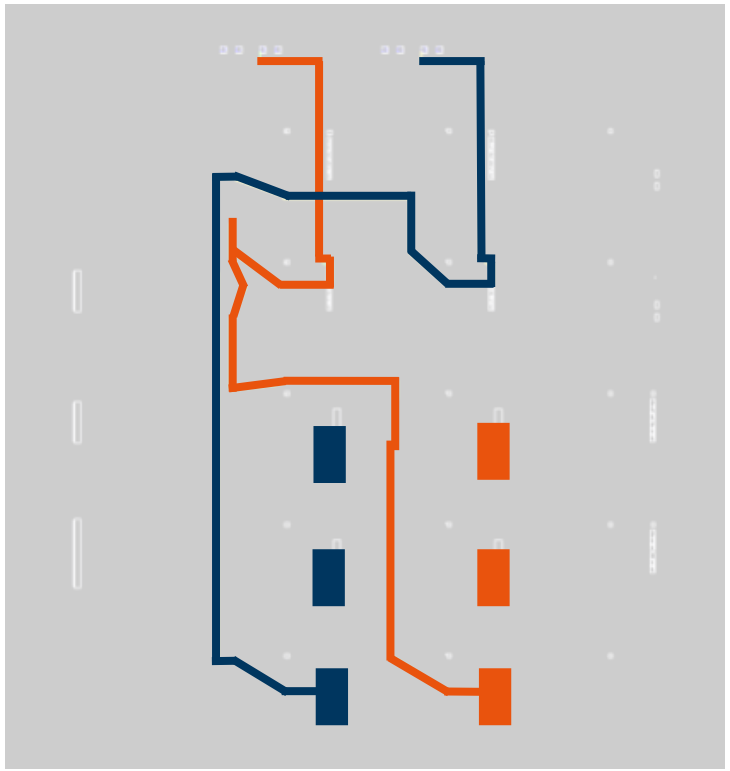


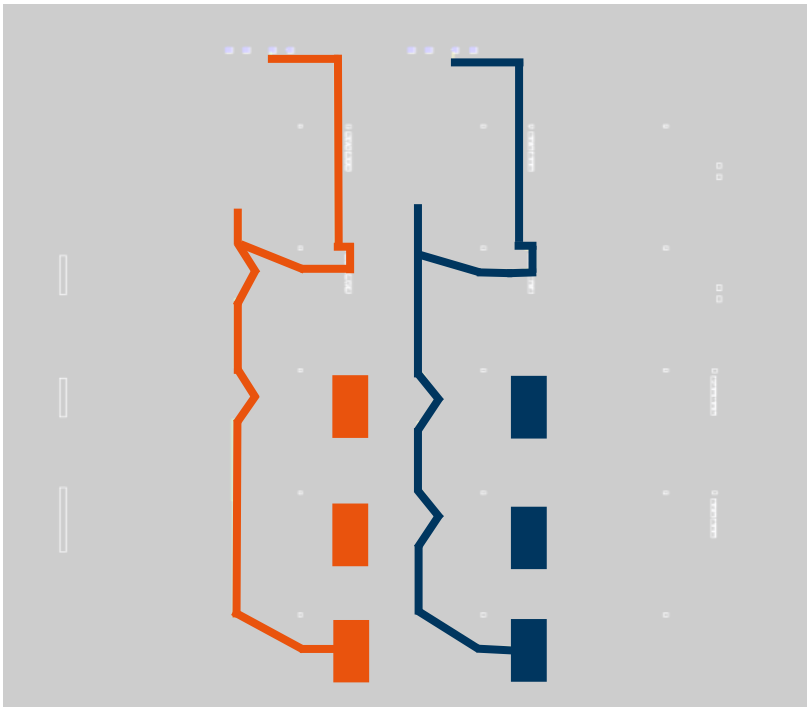
EXPERIMENTAL RESULTS – *ROUTING PATHS*

RO

Delay line

- Do routing paths affect locking range?



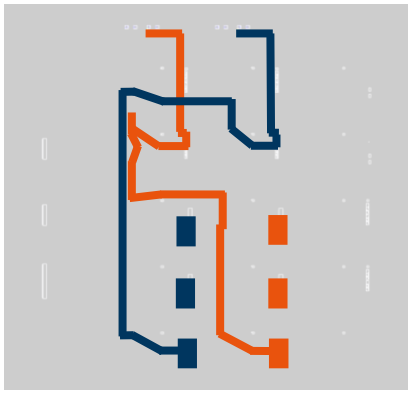


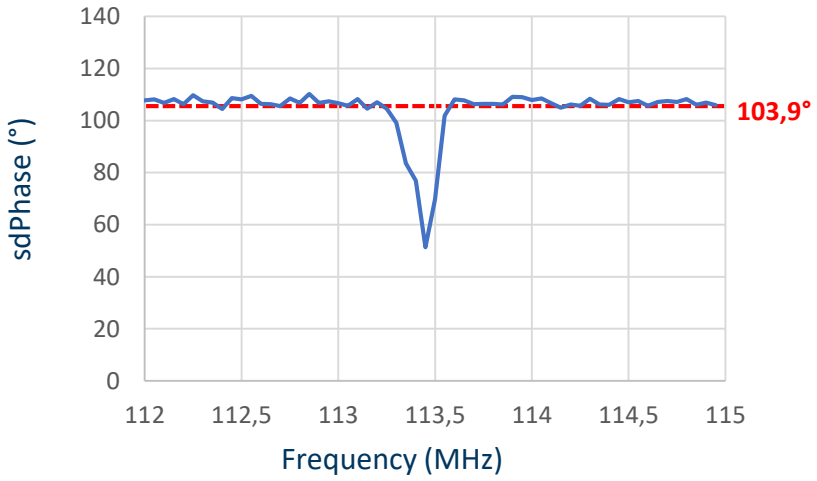
EXPERIMENTAL RESULTS – *ROUTING PATHS*

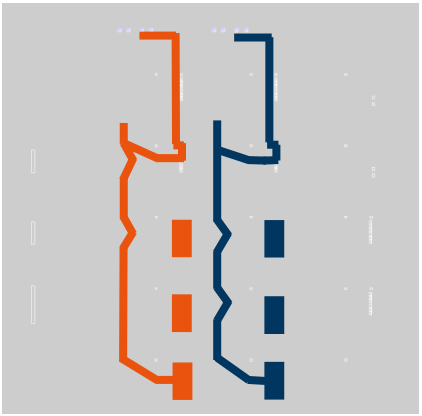
Delay line

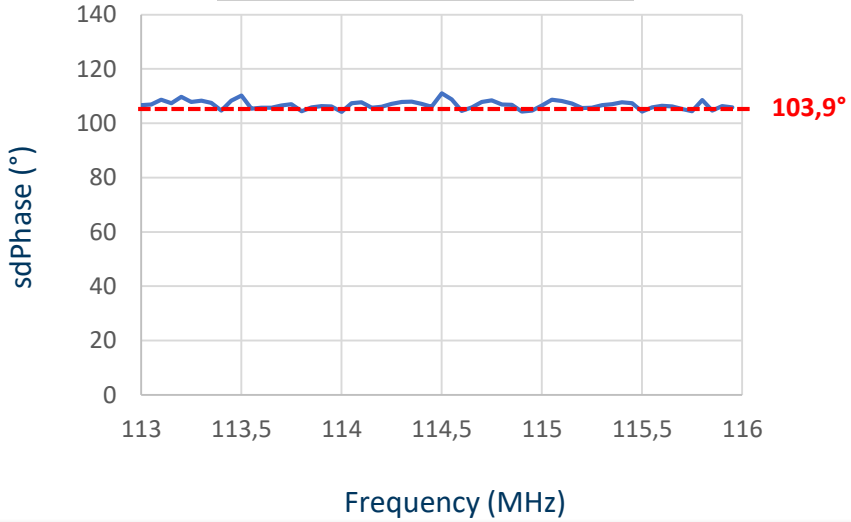
RO

- Do routing paths affect locking range?









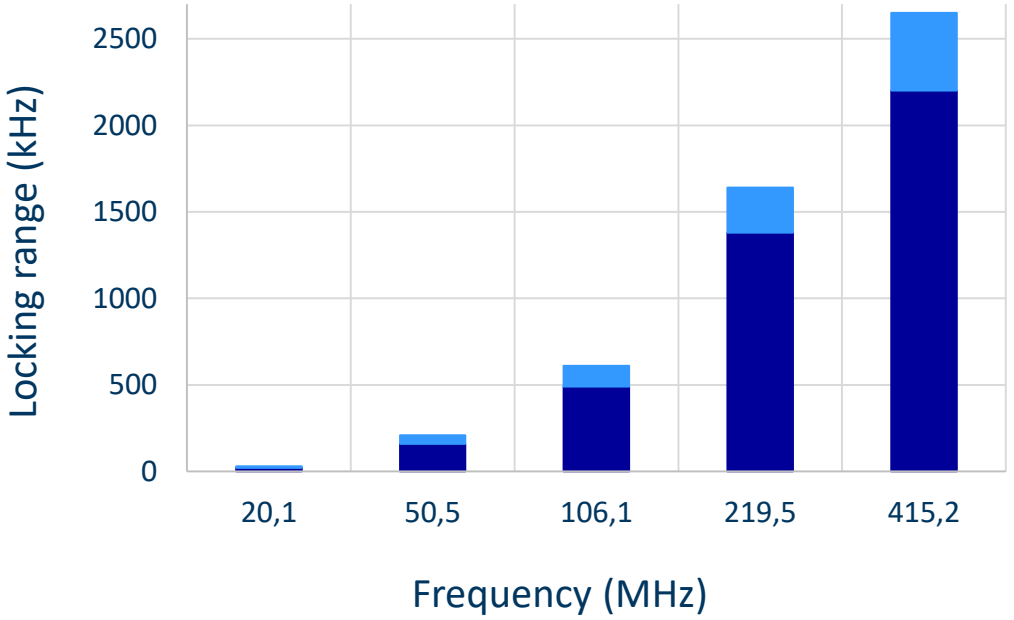
EXPERIMENTAL RESULTS – *# ELEMENT IN RO*

Total lock

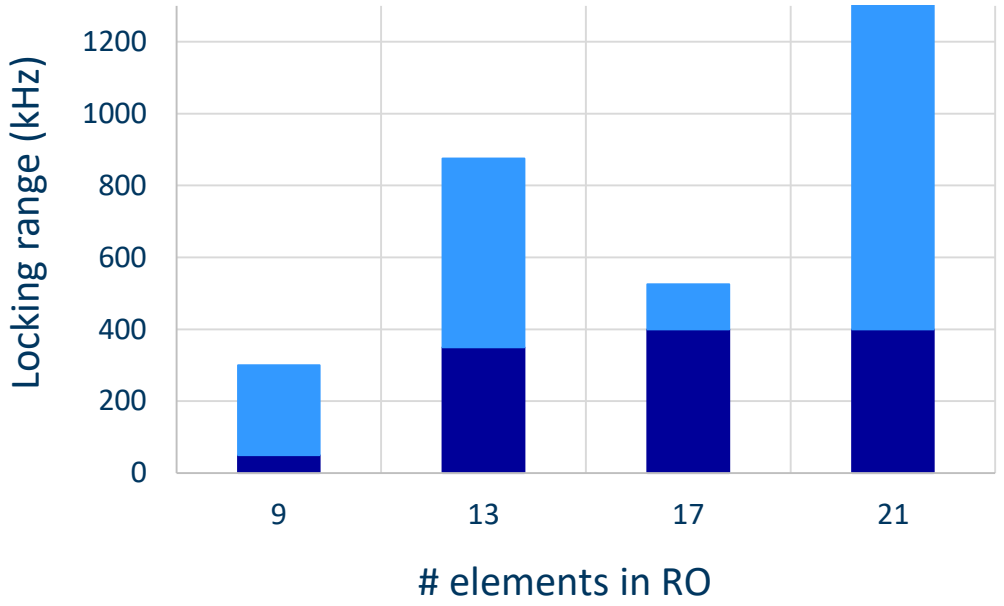
Partial lock

- Impact of number of element composing RO with same frequency

Fixed frequency ≈ $\mathbf{110,4\ MHz}$ $\pm 0{,}3\ MHz$



LOCKING RANGE ACCORDING TO FREQUENCY WITH VARIABLE NUMBER OF ELEMENT IN RO



LOCKING RANGE ACCORDING TO NUMBER OF ELEMENT IN RO WITH SAME FREQUENCY

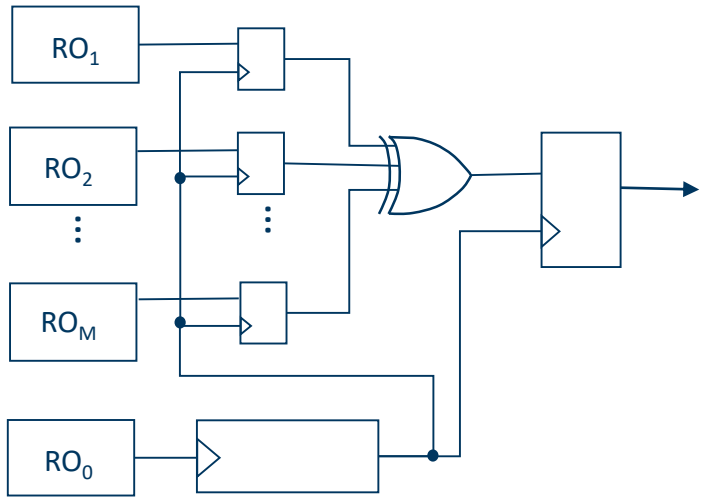
TABLE OF CONTENTS

CONCLUSION

- Locking phenomenon highlighting and its danger for random number generation
- FPGA target : one on which locking can be observed
- Standard deviation of phase difference as a metric

IMPACT ON LOCKING	CAUSE OF LOCKING	RECOMMENDATIONS
High ↓ Least	Routing paths	Avoid common routing paths.
	Ring frequency	The faster ring, the higher chance to lock around nominal frequency.
	Relative placement	Place ROs the farthest you can, or perpendicular from each other.
	Number of element in RO	For a given frequency, ↗ number of delay element + ↘ delay of interconnections ➡ maximize locking
	Supply voltage	As long as lock measurement is performed through a scope, external conditions affect locking.
	Probe types	

FUTURE WORK



TRNG Design

- Total Failure Test
- On line Test
- Jitter measurement method [1]

Are they able to detect locking?

→ ✓ Evaluate speed to detect locking

Evaluate robustness against locking

→ ✗ Create embedded detection methods for locking

[1] Viktor Fischer, David Lubicz. Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG. *Workshop on Cryptographic Hardware and Embedded Systems 2014* (CHES 2014)

Thank you for your attention

Thanks to Maxime JOURNOUD for his unvaluable help in obtaining the various results.

Éloïse DELOLME

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

UNIVERSITÉ DE LYON

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

cnrs

DGA DIRECTION GÉNÉRALE DE L'ARMEMENT

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES