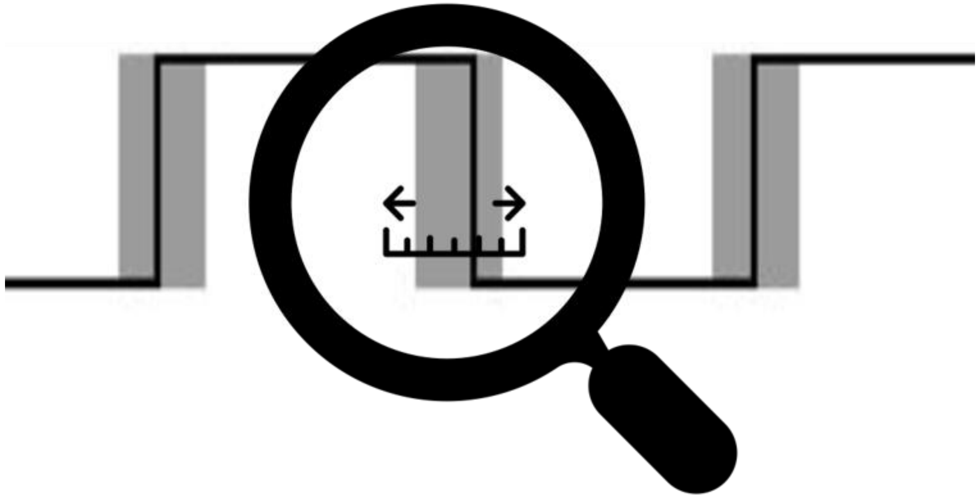


On-board characterization and measurement of clock jitter used as source of randomness by TRNGs

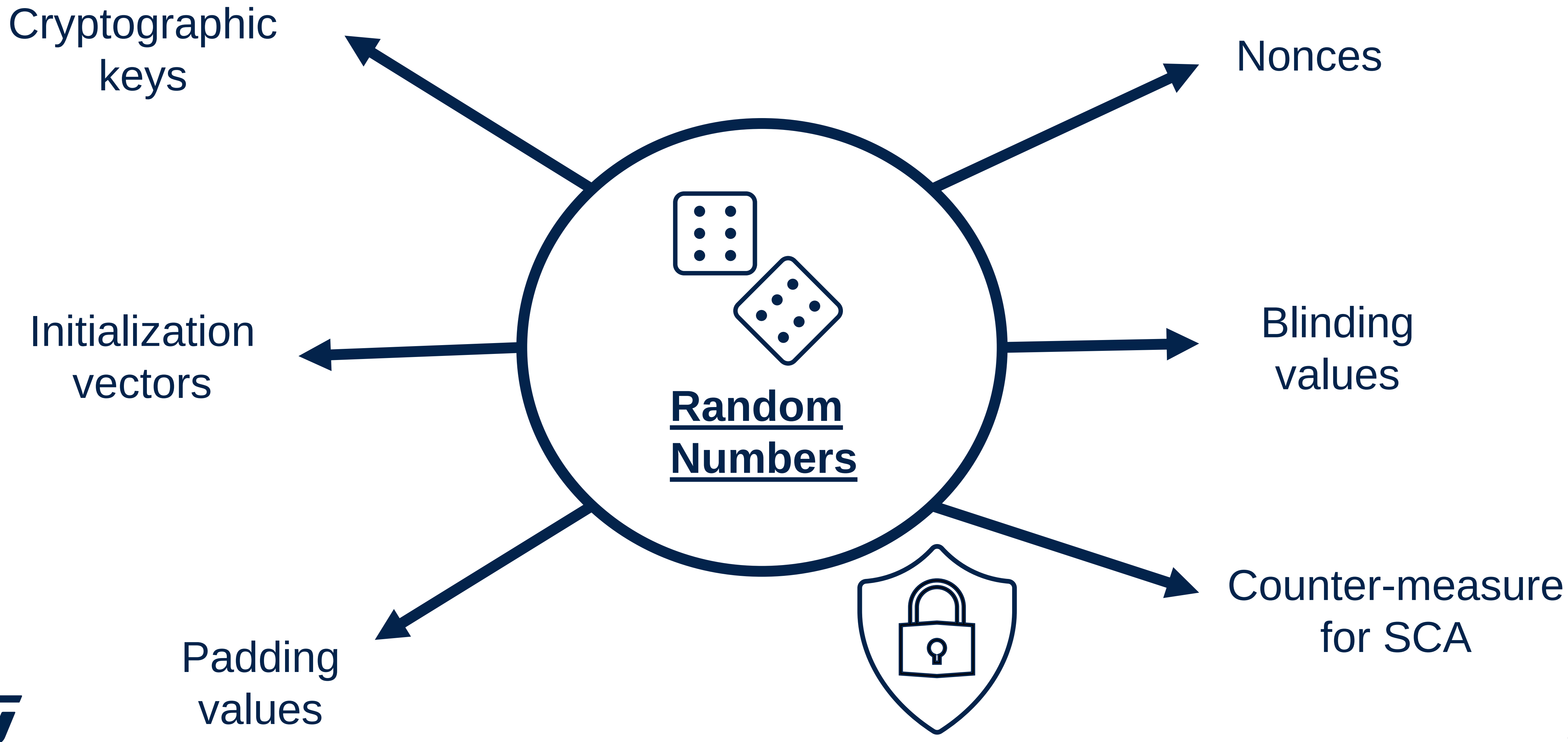
Arturo GARAY

SemSecuElec seminar

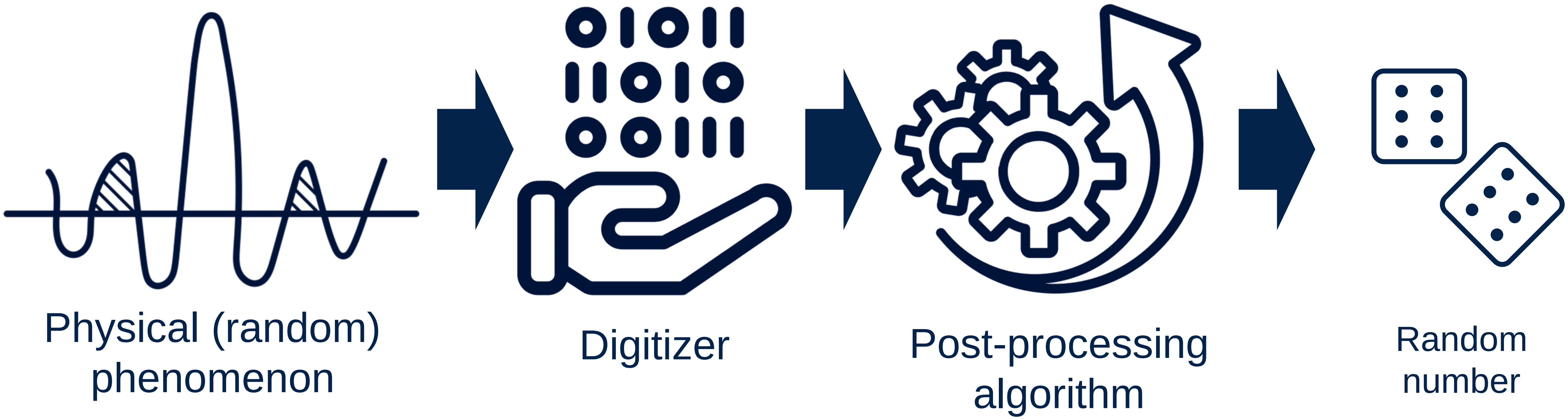
February 28th, 2025

ASSOCIATION NATIONALE RECHERCHE TECHNOLOGIE
life.augmented
LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE
UNIVERSITÉ DE LYON
UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

Random Numbers in Cryptography



True Random Number Generator (TRNG)

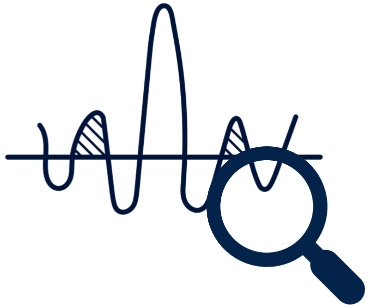


Evaluation of a True Random Number Generator (TRNG)

Current standards

Stochastic model of the TRNG [1]

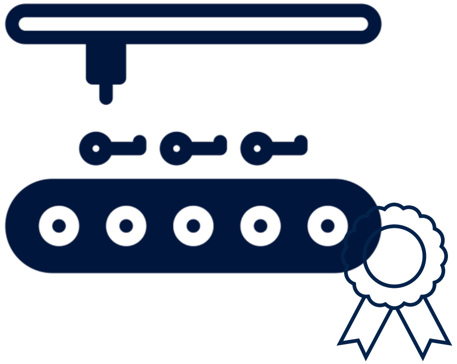
+



Measurement Physical Parameter

H_{min}

Lower min-entropy bound

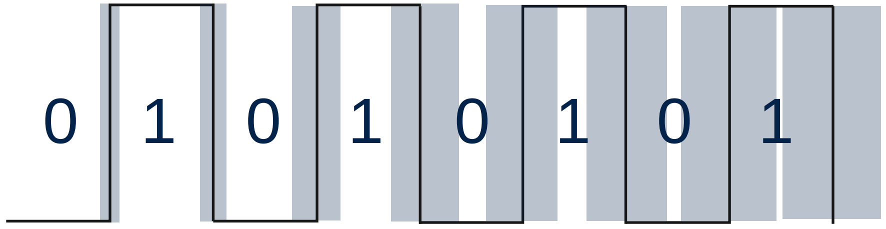


Certified TRNG

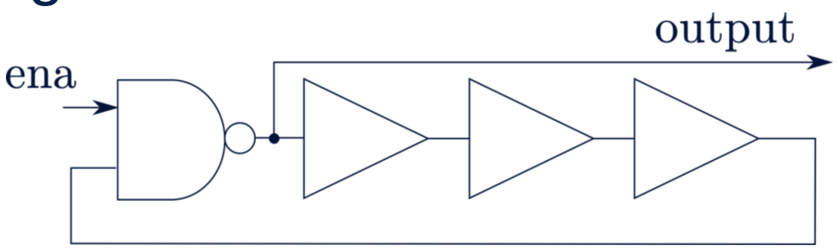
[1] W. Killmann and W. Schindler. A Proposal for: Functionality Classes for Random Number Generators, AIS20/31. 2011

Clock jitter

Clock signal



Ring Oscillator

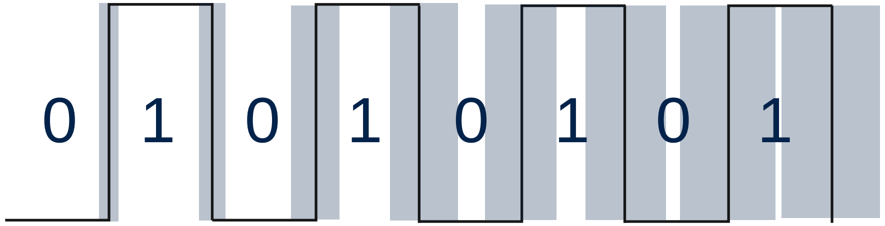


Random periods of the clock signal

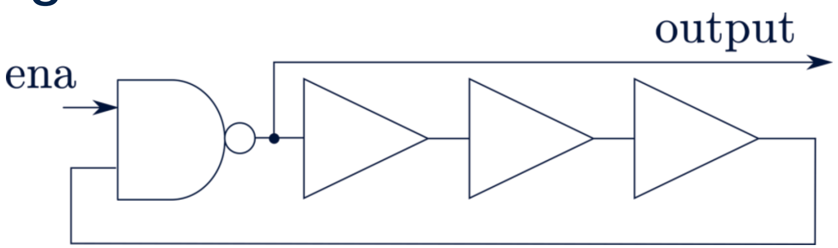
Clock jitter

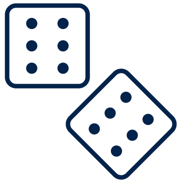
Clock jitter

Clock signal



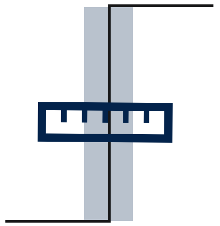
Ring Oscillator



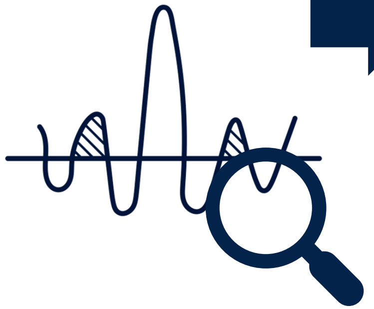


Random periods of the clock signal

Clock jitter

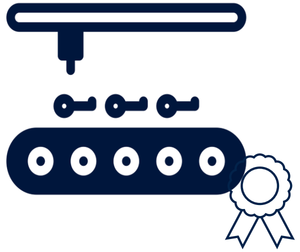


Most TRNGs in the market exploit clock jitter



$$H_{min}$$

Lower min-entropy bound

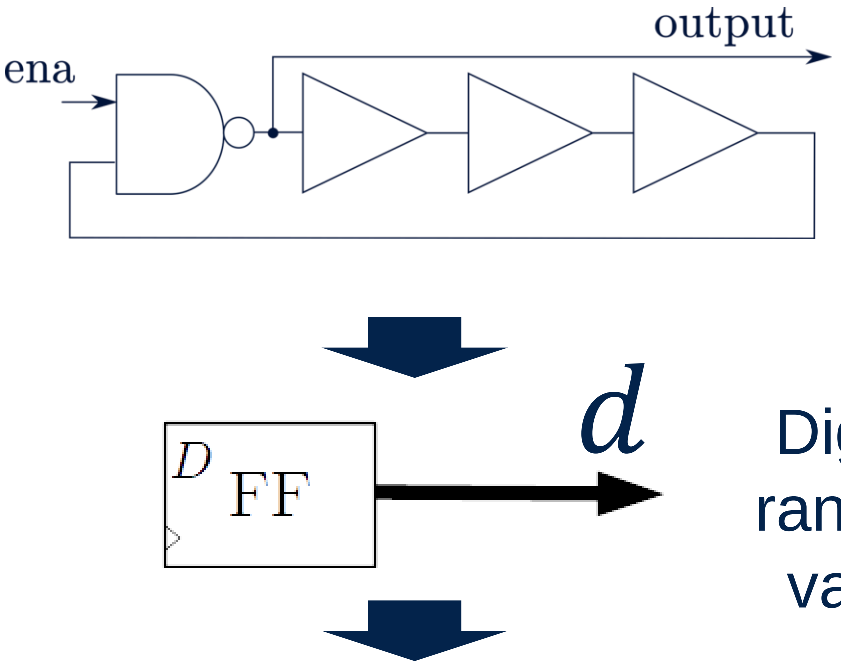


life.augmented

Clock jitter measurement

External
measurements

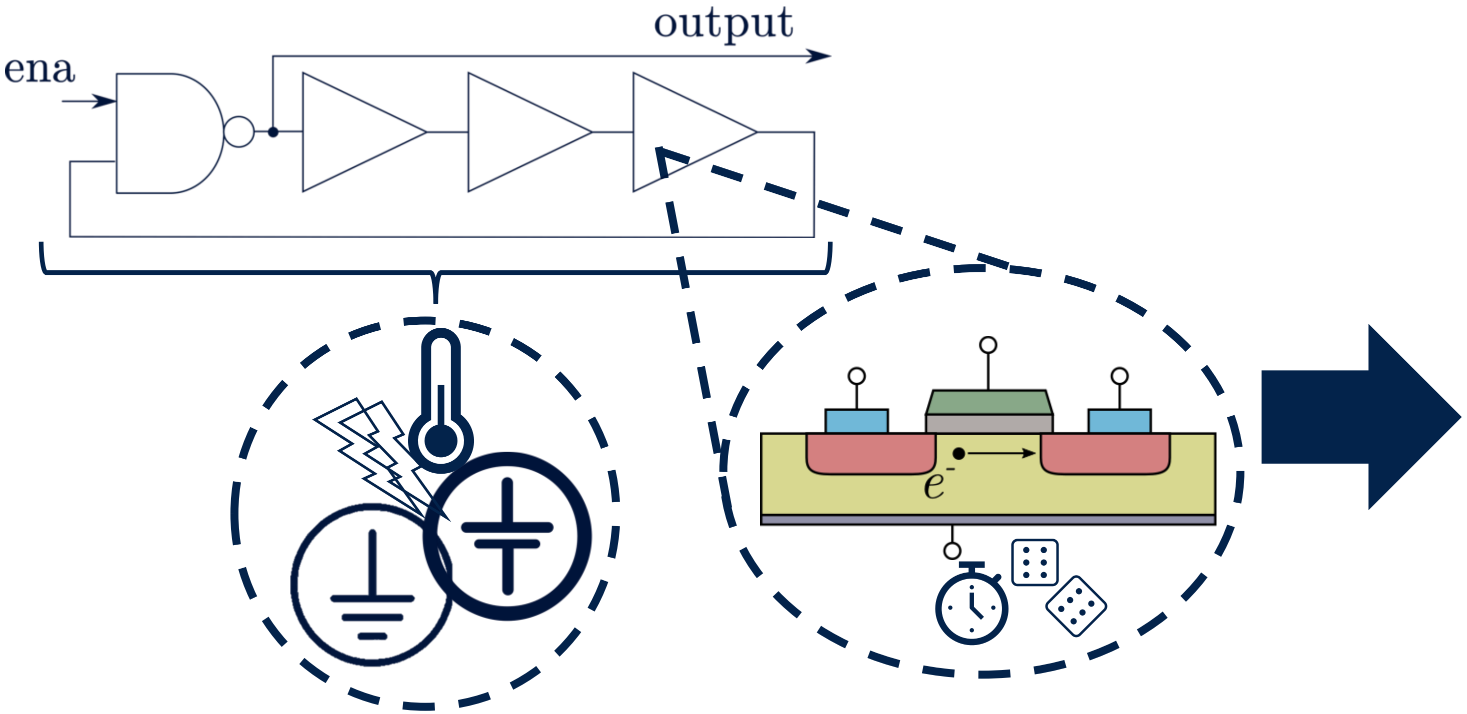
Clock jitter measurement

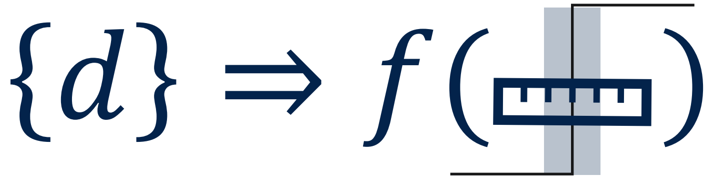


$$\{d\} \Rightarrow f(\;)$$

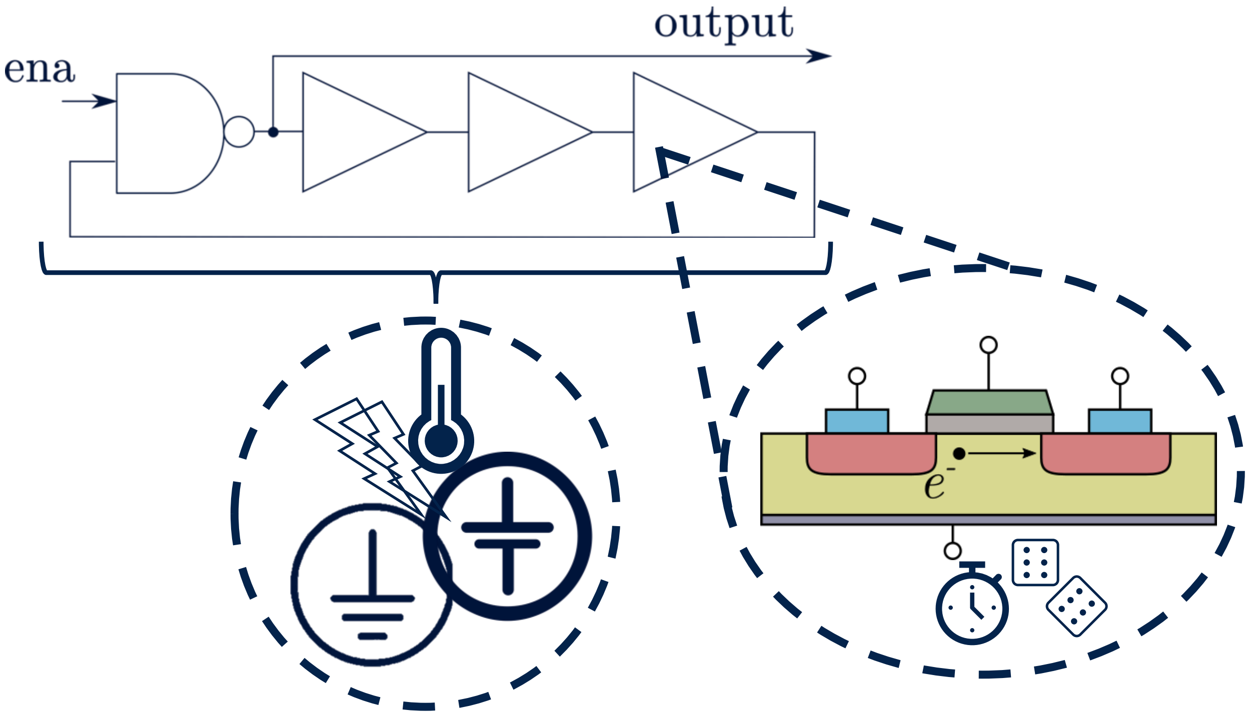
Internal measurements

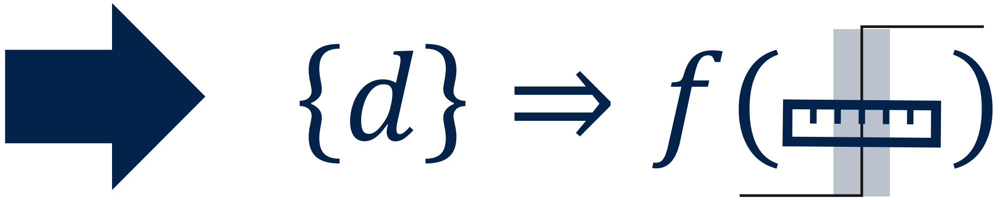
Clock jitter origins





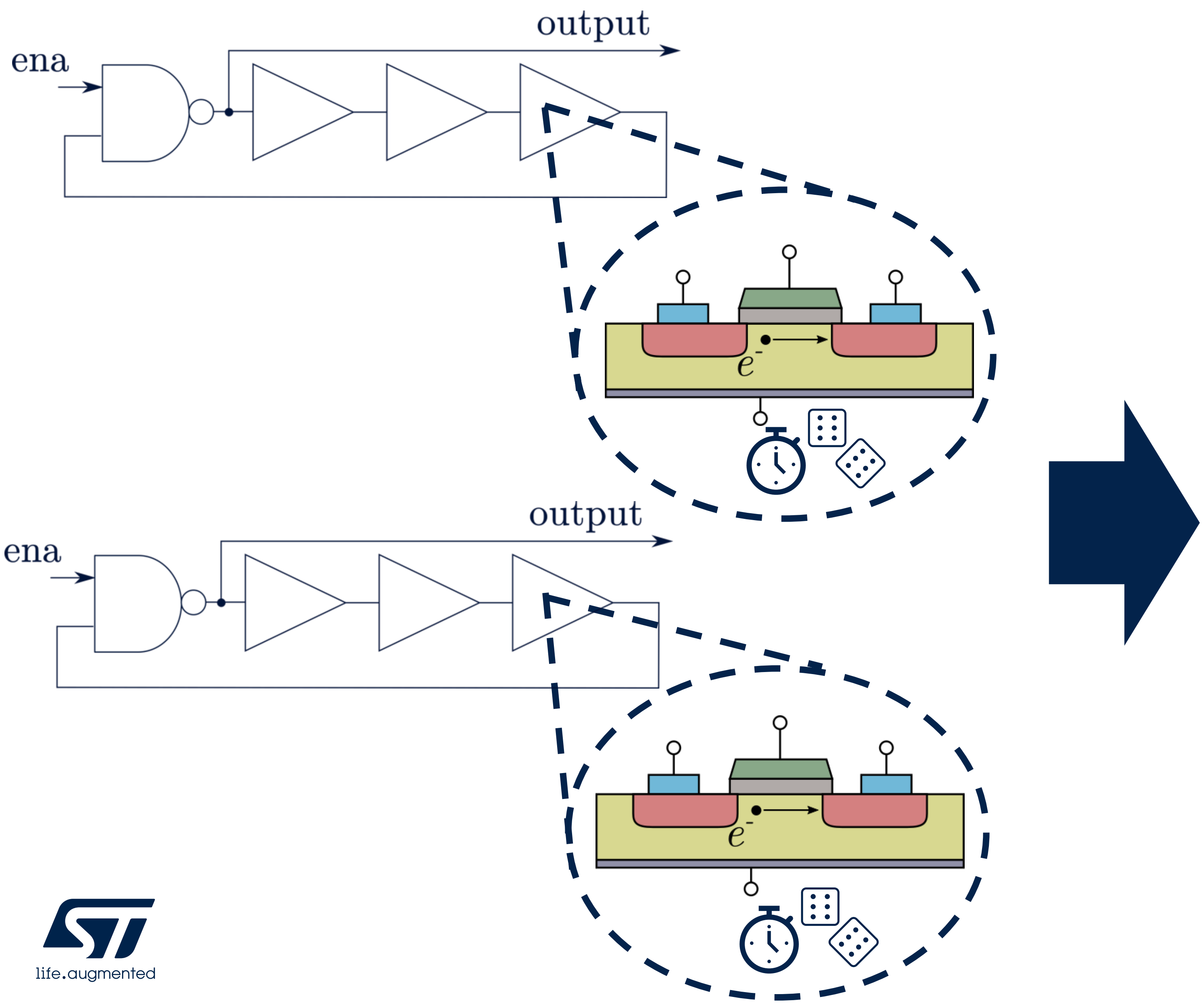
Clock jitter origins





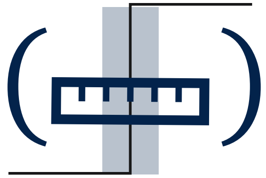
Global noises (manipulable) + Local noises (NOT manipulable)

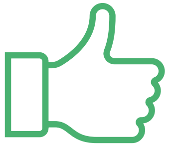
Differential clock jitter measurement



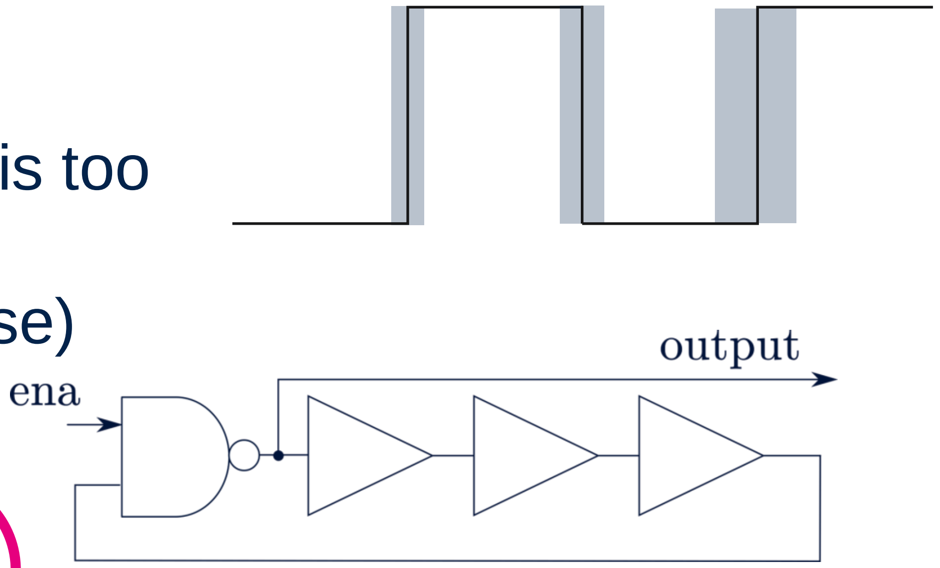
$$\{d\} \Rightarrow f(\ \ )$$

Local noises only



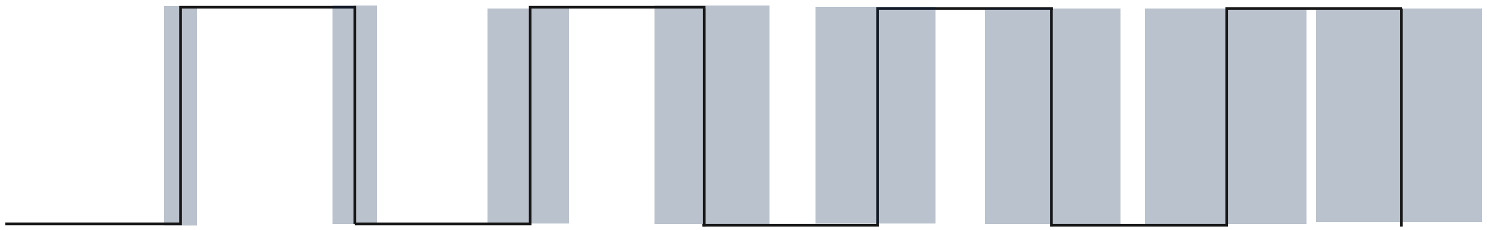


Clock jitter accumulation

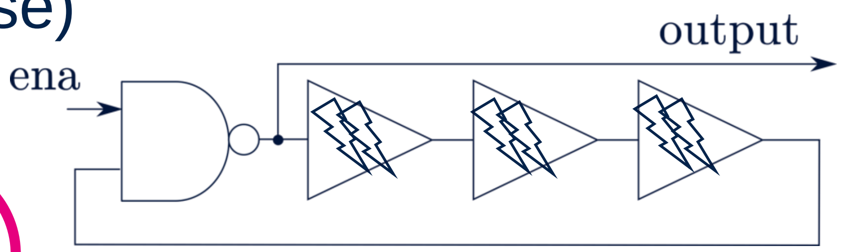


Clock jitter is too small (Imprecise)

Clock jitter accumulation



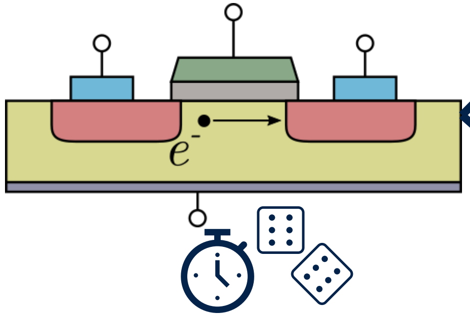
Clock jitter is too small (Imprecise)



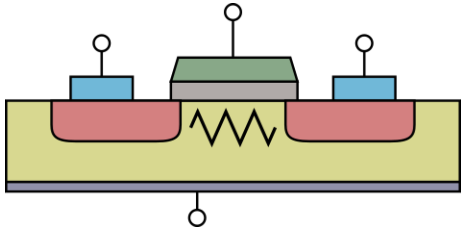
We wait

Clock jitter is bigger (Measurable)

Thermal vs flicker noise

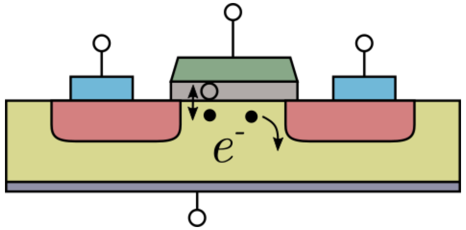


Electronic noises



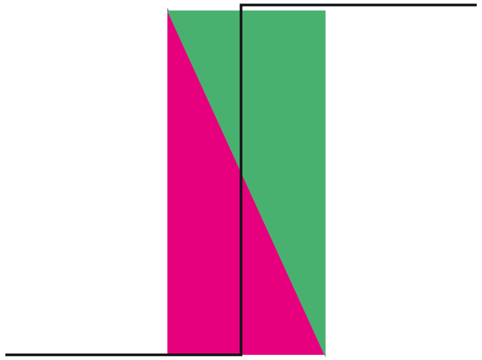
Thermal noise

Considered in the stochastic models



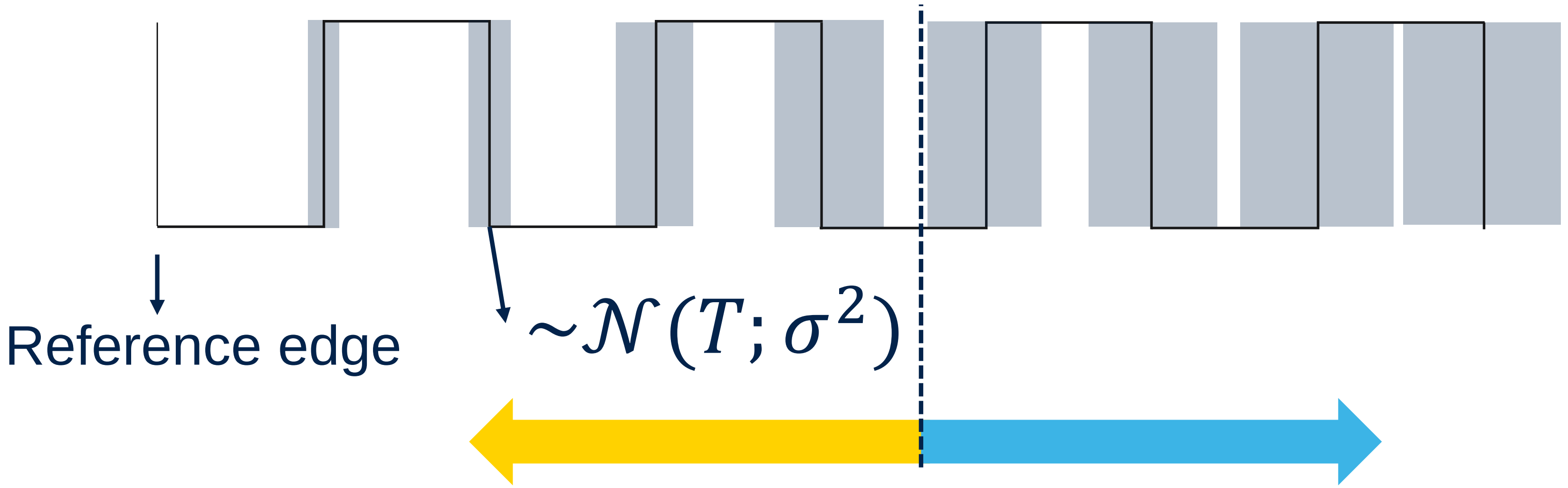
Flicker noise

Leads to unsolved mathematical problems



Distinguish both noises in the total accumulated jitter

Accumulated clock jitter



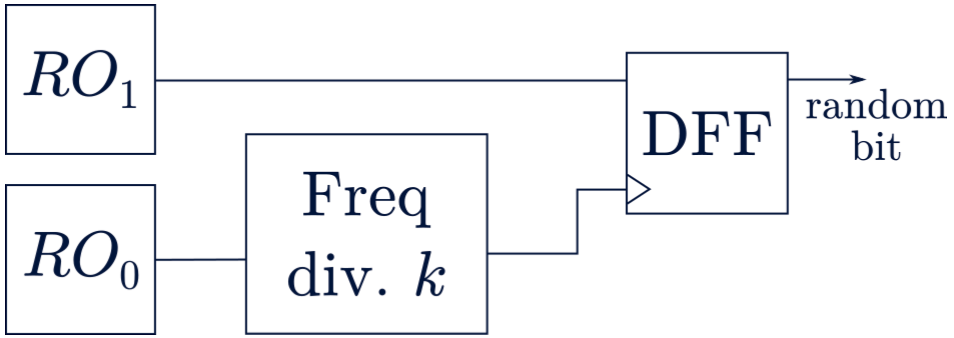
Thermal noise a_{th}

Flicker noise a_{fl}

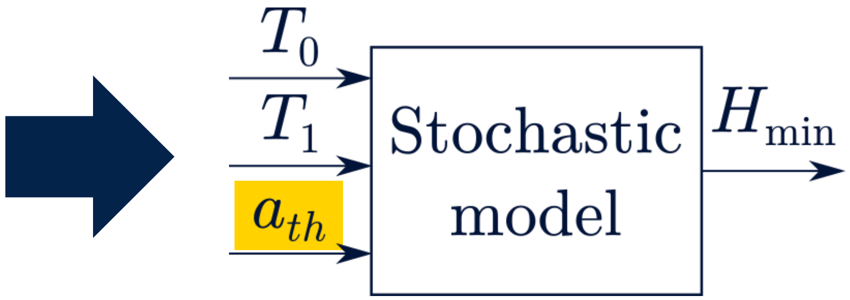
$$\sigma^2(\Delta t) = f(a_{th}, a_{fl})$$

Technology dependent coefficients

Example of the eRO-TRNG



eRO-TRNG



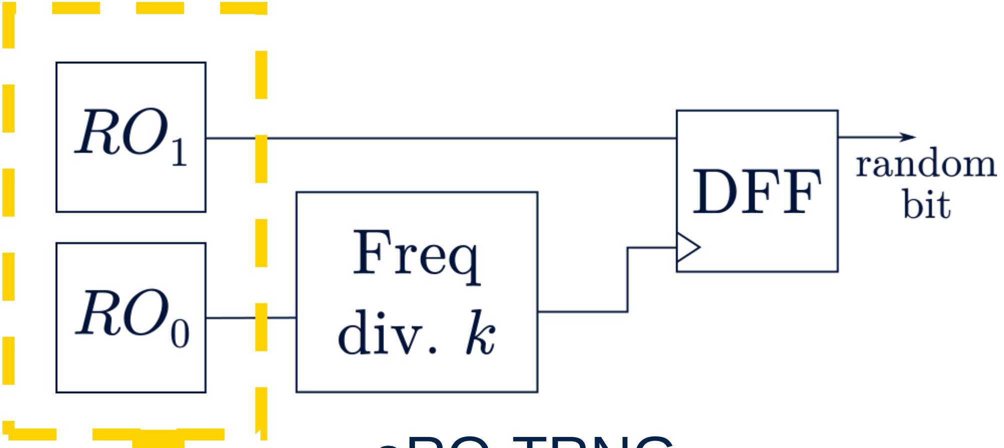
Low min-entropy bound

Parametered model [2]

life.augmented

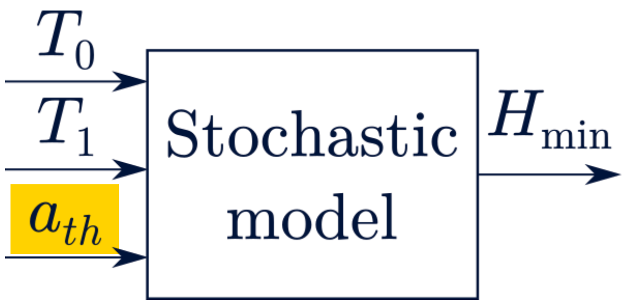
[2] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux. “On the Security of Oscillator-Based Random Number Generators”. (Apr. 2011), pp. 398–425

Example of the eRO-TRNG



eRO-TRNG

Embedded measurement of a_{th}



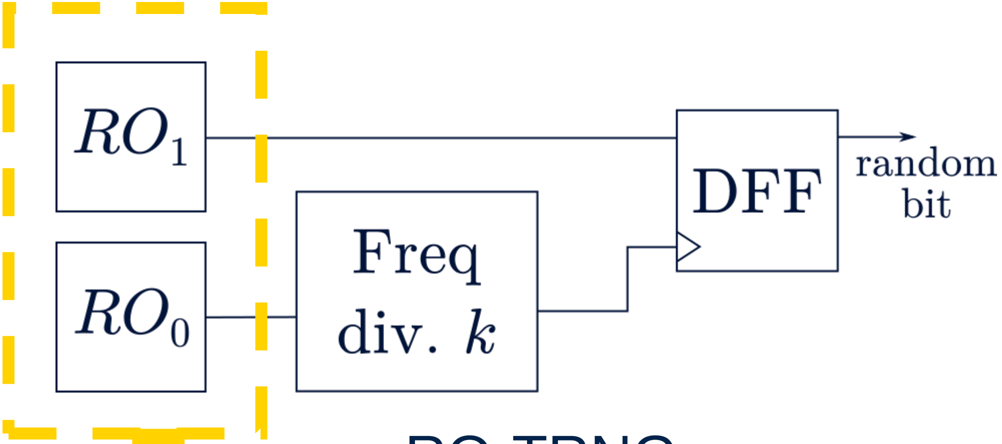
Low min-entropy bound

Parametered model [2]

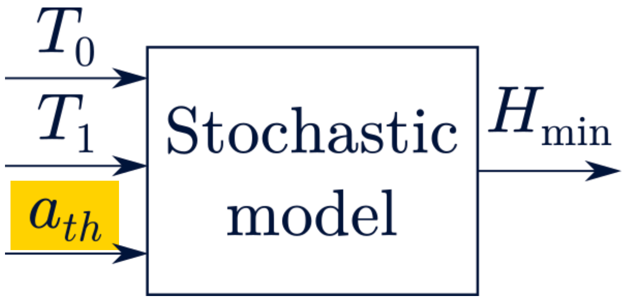
Security evaluation
Guarantee of the TRNG performance

[2] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux. “On the Security of Oscillator-Based Random Number Generators”. (Apr. 2011), pp. 398–425

Example of the eRO-TRNG



eRO-TRNG



Low min-entropy bound

Parametered model [2]

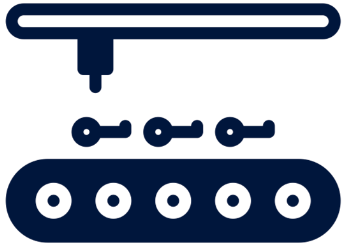
Embedded measurement of a_{th} → Security evaluation Guarantee of the TRNG performance

Overestimation of a_{th} → False security claim of the TRNG, compromising the whole cryptographic system.

[2] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux. “On the Security of Oscillator-Based Random Number Generators”. (Apr. 2011), pp. 398–425

Our objective

The need for true random numbers

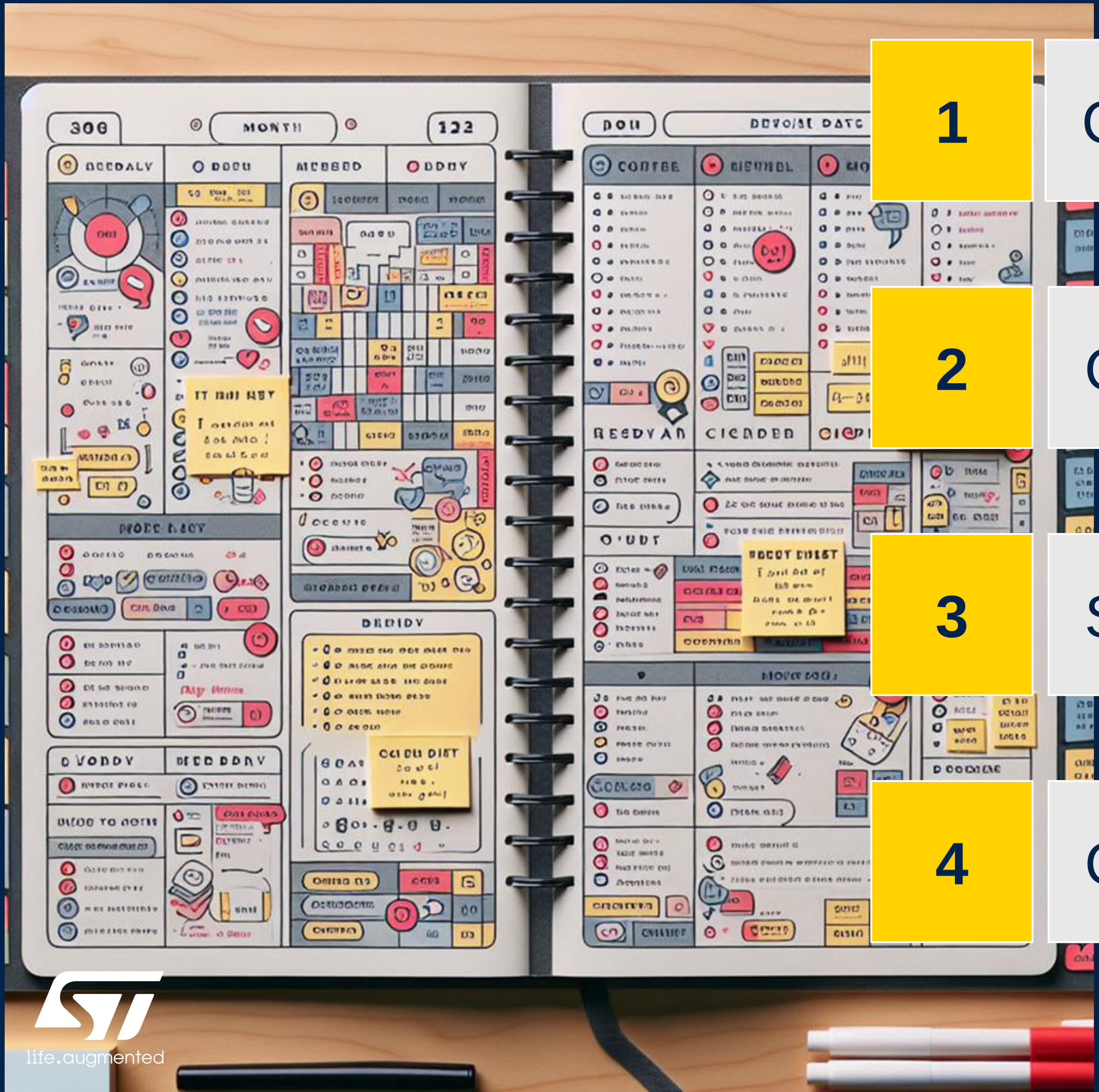


Most TRNGs in the market exploit jittery digital signals

Current standards require the use of a stochastic model to evaluate TRNGs
A measurement of the thermal component of the jitter is required

Develop an embedded differential jitter measurement method of the thermal jitter component

Agenda



1. Comparison of existing methods
2. Our method
3. Studying the impact of flicker noise
4. Conclusions and Perspectives

Agenda – 1) Comparison

a Evaluation procedure

b Case study & Comparison

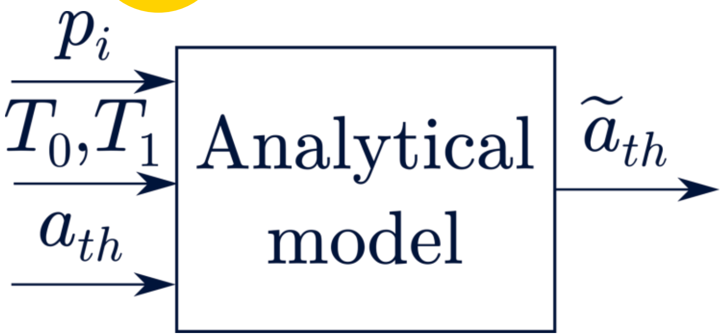
c FPGA implementations

a) Evaluation procedure

life.augmented

The evaluation procedure

1 Modeling



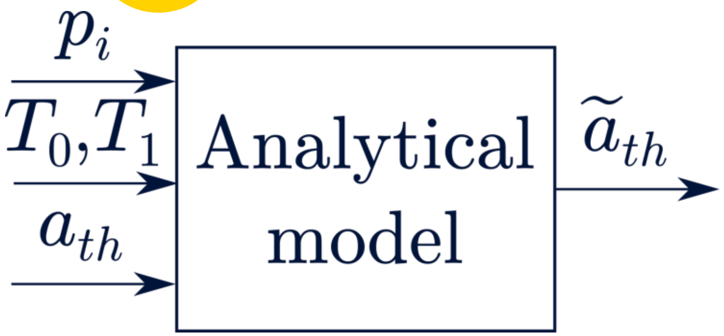
Neglect flicker noise

Clock jitter $a_{th} = 1‰T$

$\sim\mathcal{N}(T; a_{th}^2)$

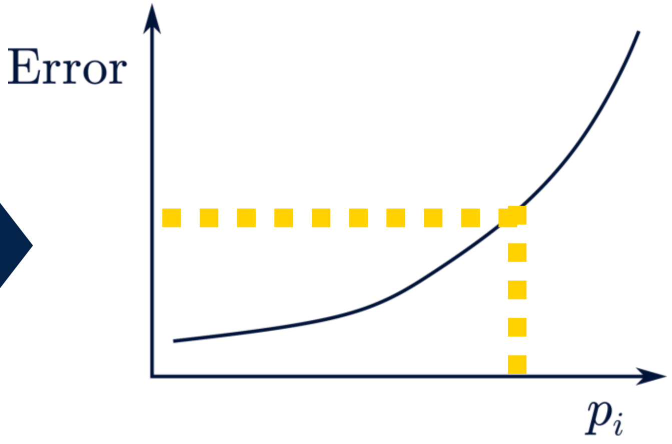
The evaluation procedure

1 Modeling



Neglect flicker noise

Clock jitter $a_{th} = 1‰T$
$\sim\mathcal{N}(T; a_{th}^2)$



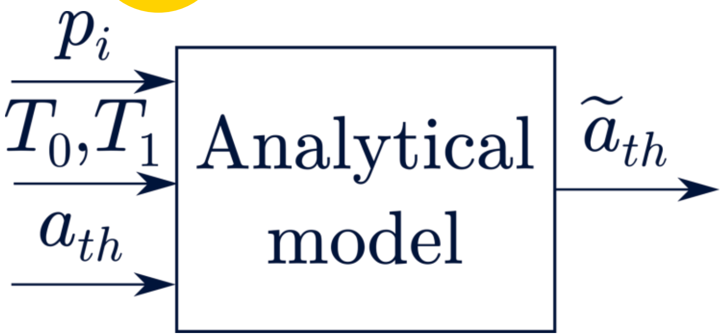
2 Simulation

$$err_{\%} = \frac{|a_{th} - \tilde{a}_{th}|}{a_{th}} . 100$$

life.augmented

The evaluation procedure

1 Modeling

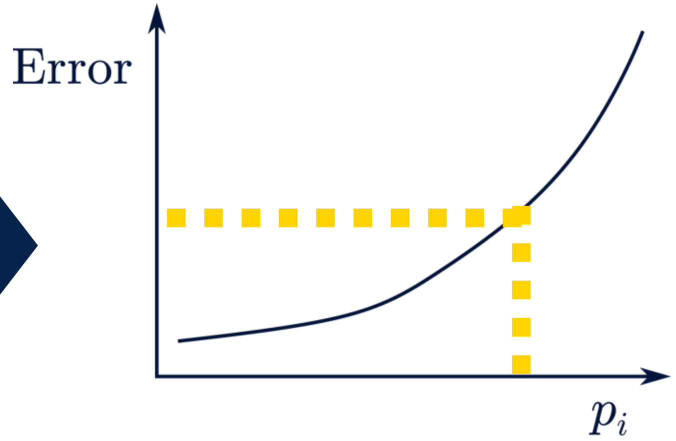


Neglect flicker noise

Clock jitter $a_{th} = 1‰T$

$\sim\mathcal{N}(T; a_{th}^2)$

2 Simulation



$$err_{\%} = \frac{|a_{th} - \tilde{a}_{th}|}{a_{th}} . 100$$

3 Error analysis

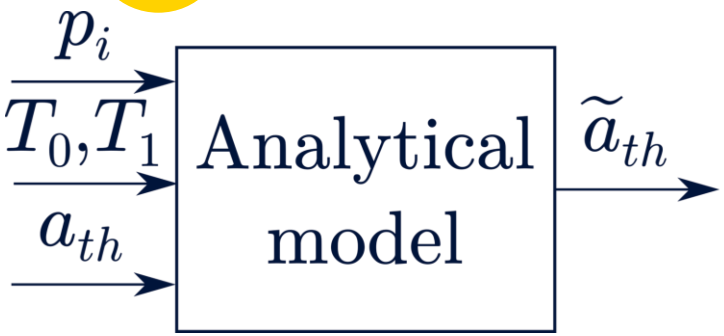
Maximal error < 25%

Average error < 10%

Methods constraints on p_i

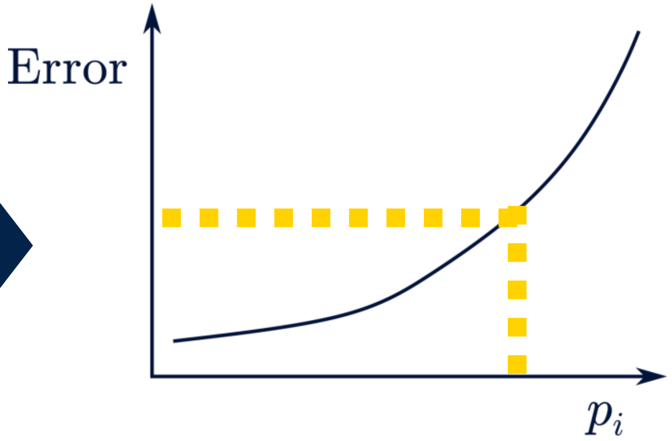
The evaluation procedure

1 Modeling



Neglect flicker noise

Clock jitter $a_{th} = 1‰T$
$\sim\mathcal{N}(T; a_{th}^2)$



2 Simulation

$$err_{\%} = \frac{|a_{th} - \tilde{a}_{th}|}{a_{th}}.100$$

3 Error analysis

Maximal error < 25%

Average error < 10%

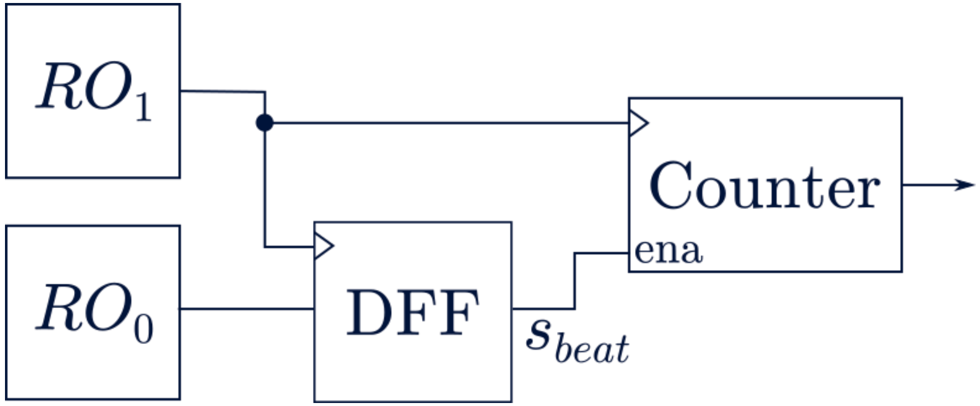
Methods constraints on p_i

4 Hardware experiment

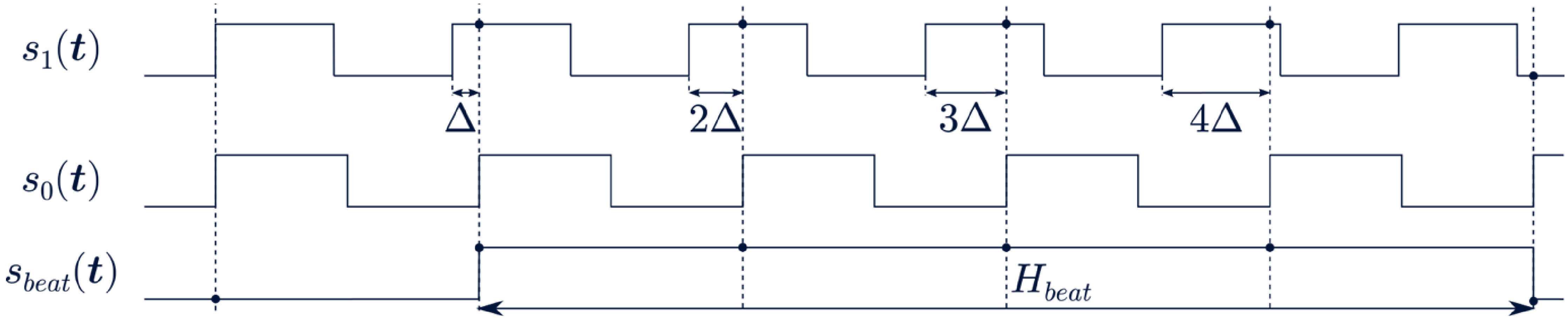
life.augmented

b) Case study

Coherent sampling method [3]

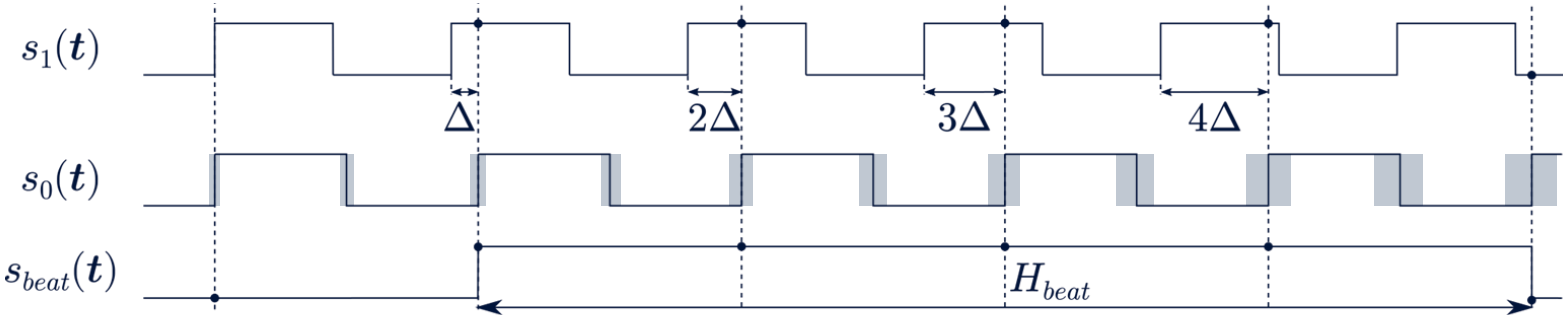


$$\Delta := T_0 - T_1$$



[3] B. Valtchanov, V. Fischer, and A. Aubert. “A Coherent Sampling Based Method for Estimating the Jitter Used as Entropy Source for True Random Number Generators”. In: SAMPTA 2009

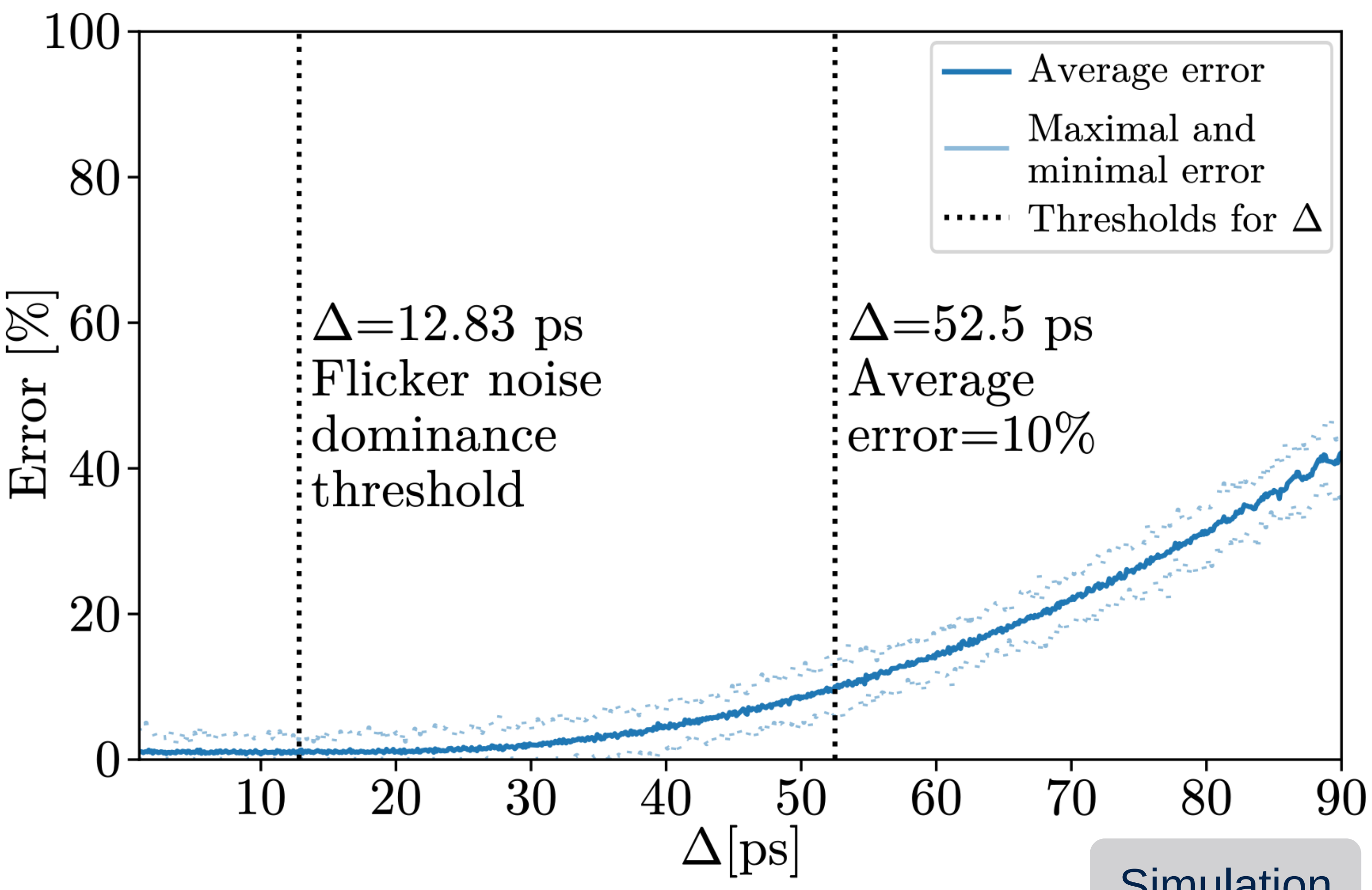
Coherent sampling method



The precision of the method

- Jitter accumulates with time
- Precision of the method depends on Δ
- We control Δ on simulations

Coherent sampling method



Simulation

- Analyse $err_{\%} = f(\Delta)$
- Lower limit → flicker noise influence
  - Greater for more than 300 cycles [4]
- Upper limit → acceptance limit on the error

[4] P. Haddad, Y. Teglia, F. Bernard, and V. Fischer. “On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models”. In: DATE 2014

Coherent sampling method

The interval can be found for any T_1

- If Δ:

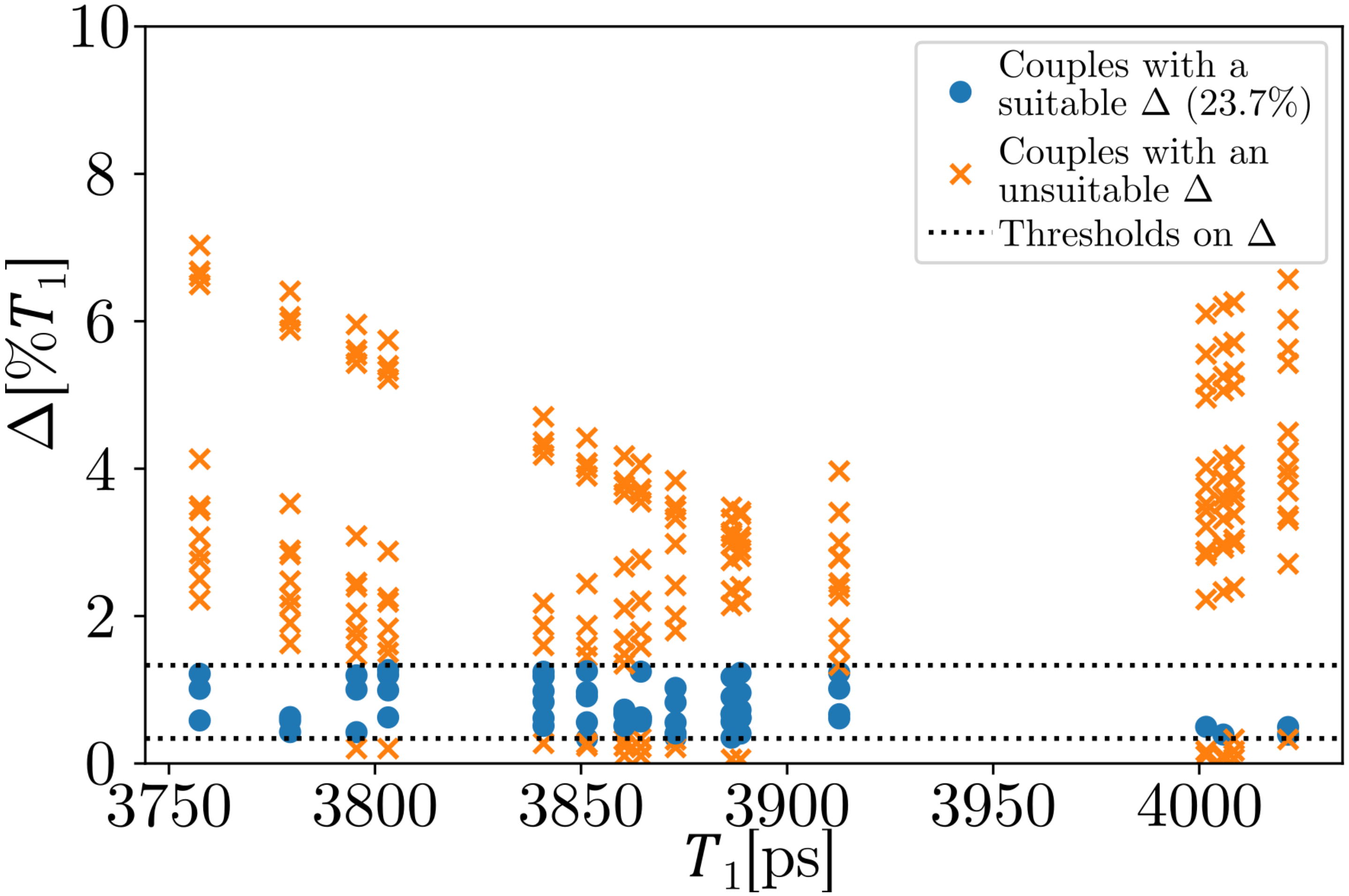
$$\Delta_{i,j} = \frac{|T_i - T_j|}{T_j} 100\% \; ; i \neq j$$

$T_j \rightarrow$ sampled clock ; $T_i \rightarrow$ sampling clock

- Then:

$$0.3\% T_1 < \Delta < 1.4\% T_1$$

Coherent sampling method



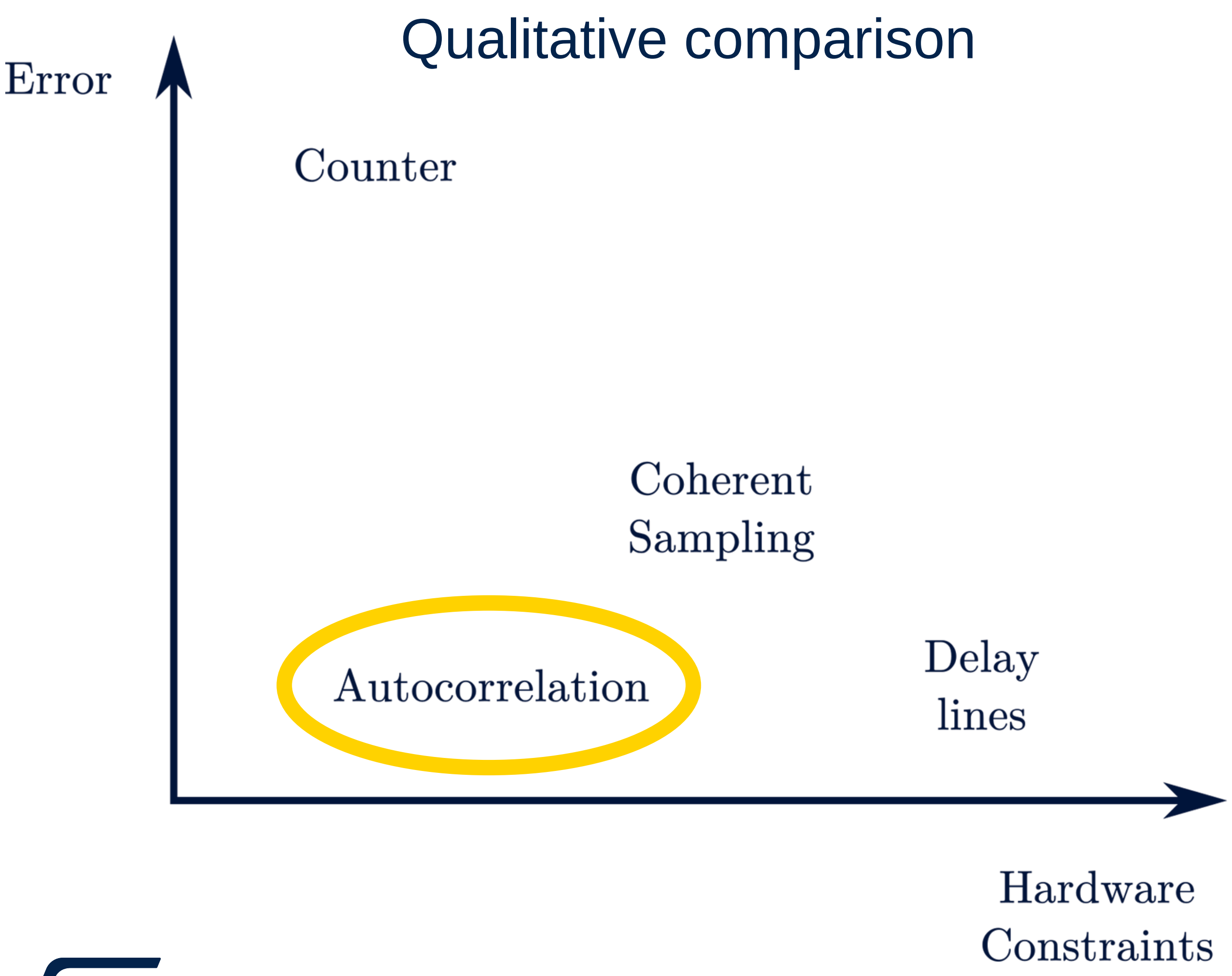
- 16 ROs → 240 pairs of ROs
- 23.7% had a suitable Δ

Result – Coherent sampling method

Critical dependence on Δ

Difficult to implement

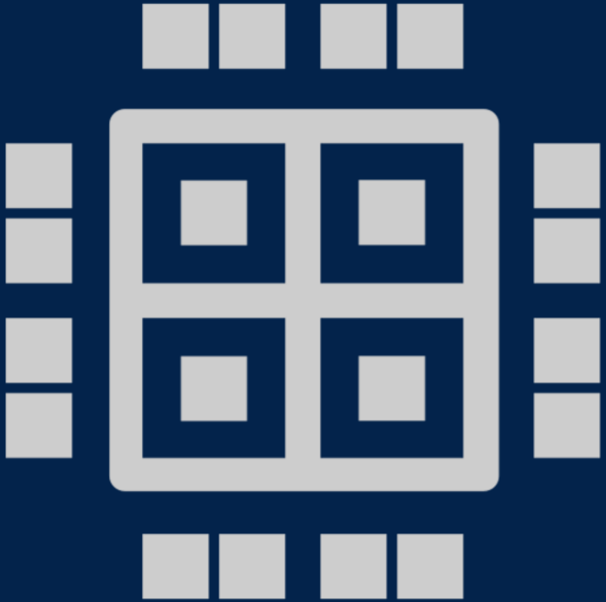
Comparison summary



- The autocorrelation method is ahead of the others
- The rest of them should:
  - Reduce the influence of flicker noise
  - Relax hardware constraints

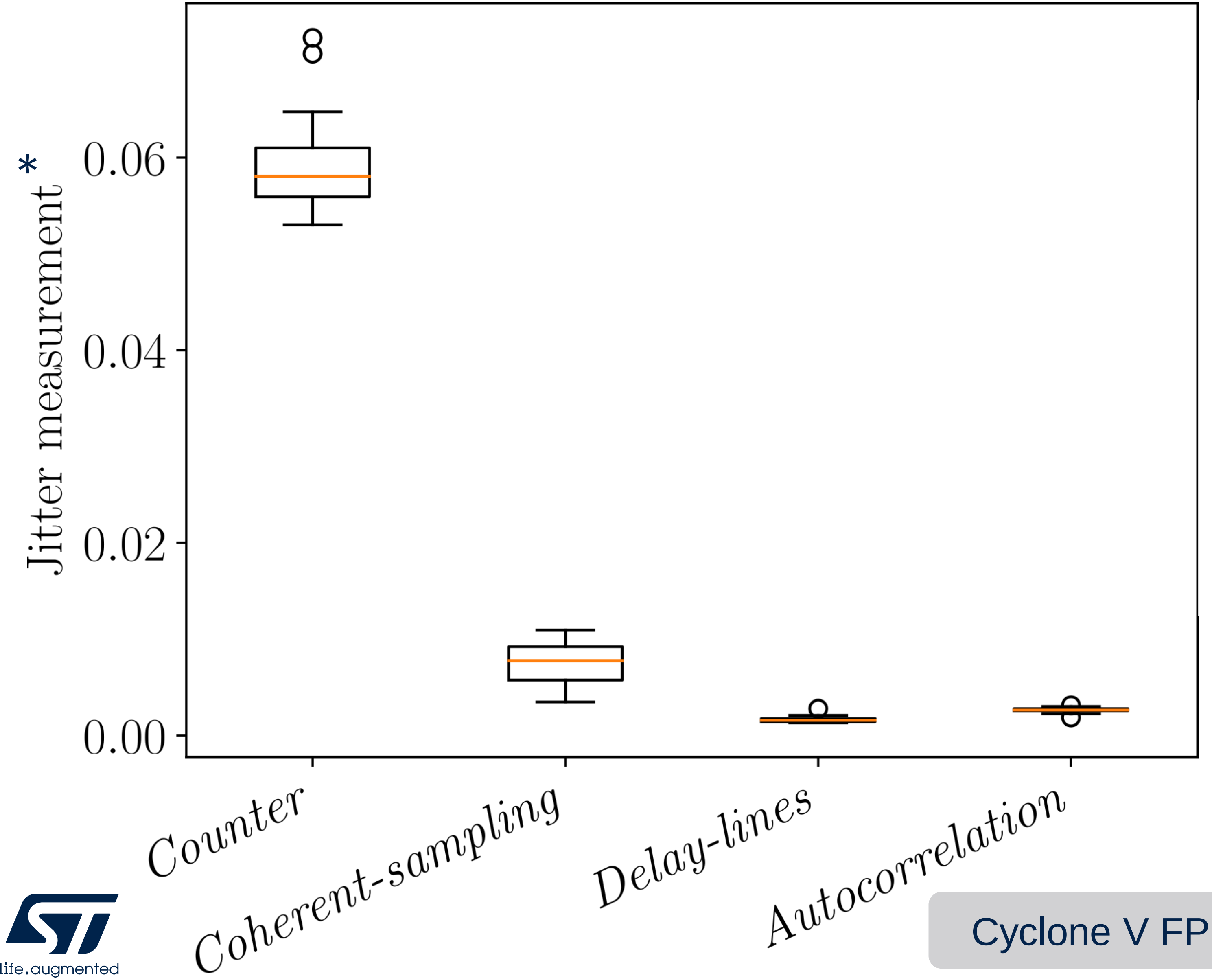
life.augmented

c) FGPA implementations



life.augmented

Comparison in FPGA



- Objective comparison
  - Under the same conditions
  - Same FPGA
- Used The HECTOR project boards

Cyclone V FPGA

$* \frac{a_{th}}{T_1}$

Key points - 1) Comparison

Successfully identified the limits of each method

If inaccurate in simulations ⇒ discard the method

Need a method:

- Low cost
- Precise
  - Hardware independent precision
- Uses **short accumulation times**
  - Reduce flicker noise influence

life.augmented

Agenda - 2) Our method

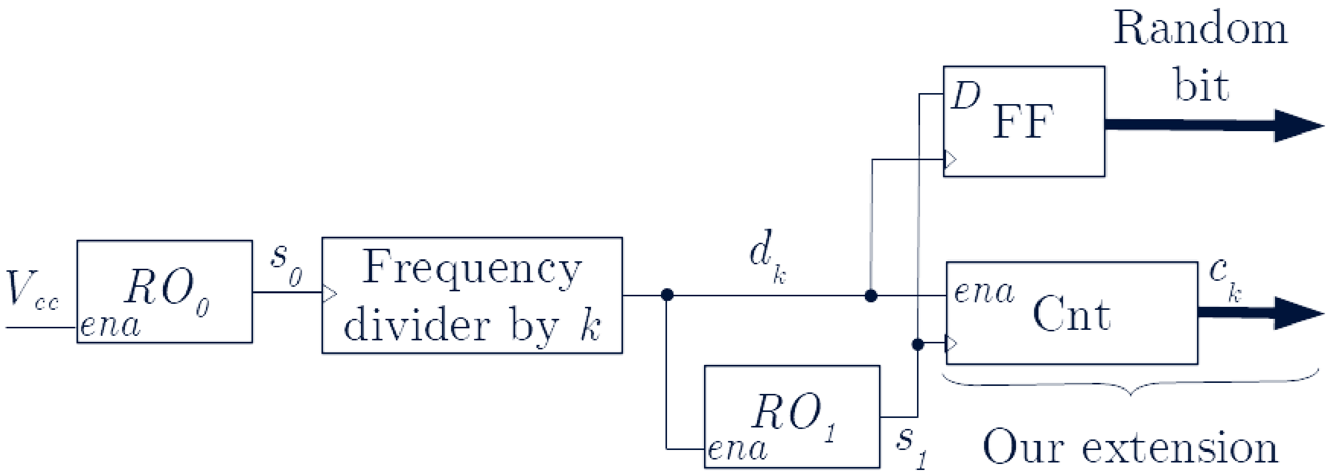
a Principle

b The advantages of our method

c Measurements in hardware

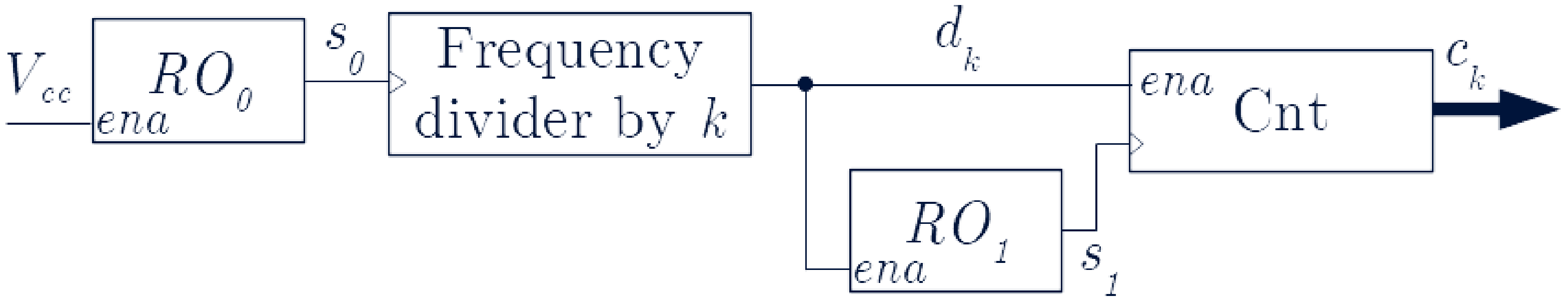
a) Principle

Basic principle

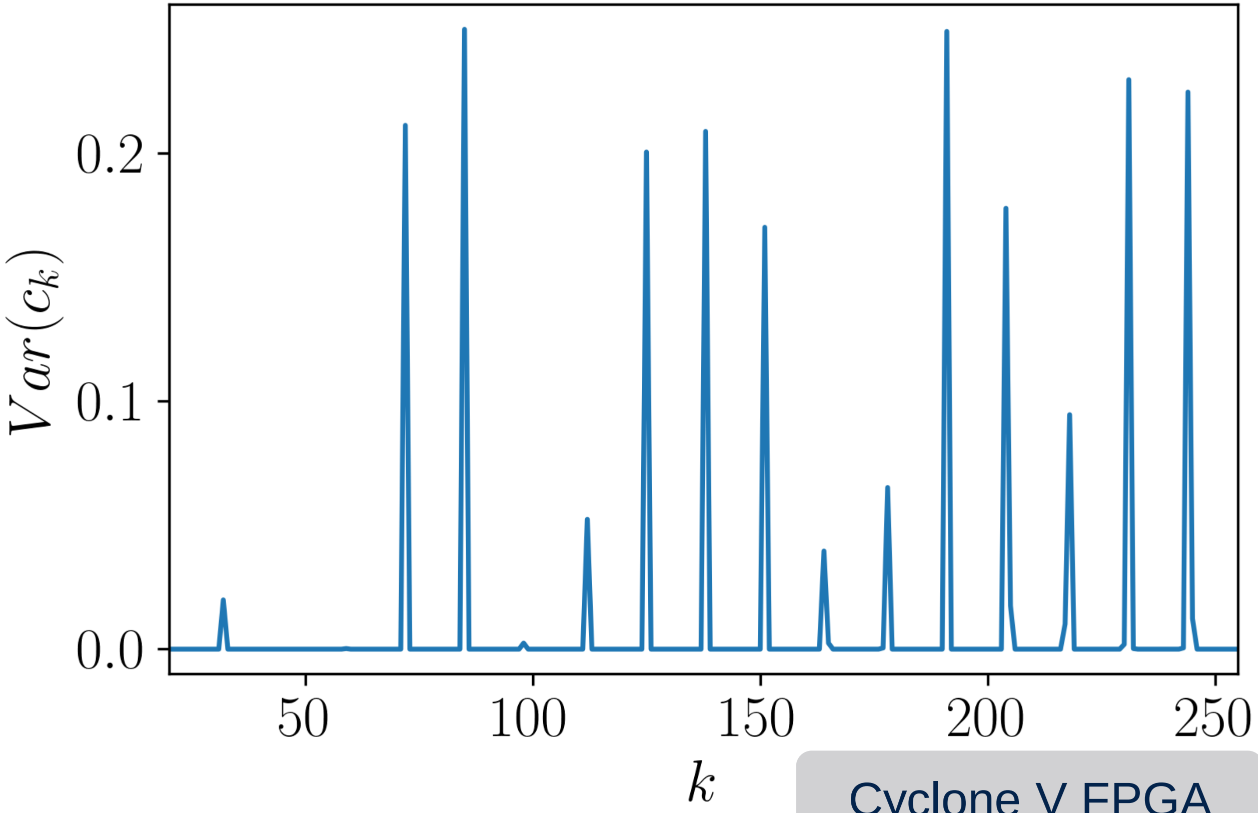


- Count the edges of RO_1
- During d_k (k periods of RO_0)
- Obtain a counter value c_k

Basic principle



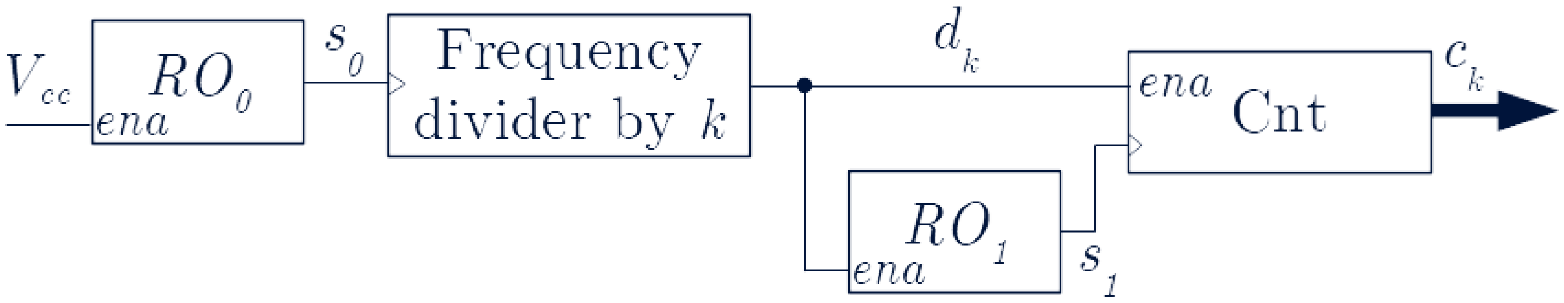
- For a given k a set of counter values may have a non-zero variance
  - The counter values differ of one
  - Caused by clock jitter



Cyclone V FPGA

life.augmented

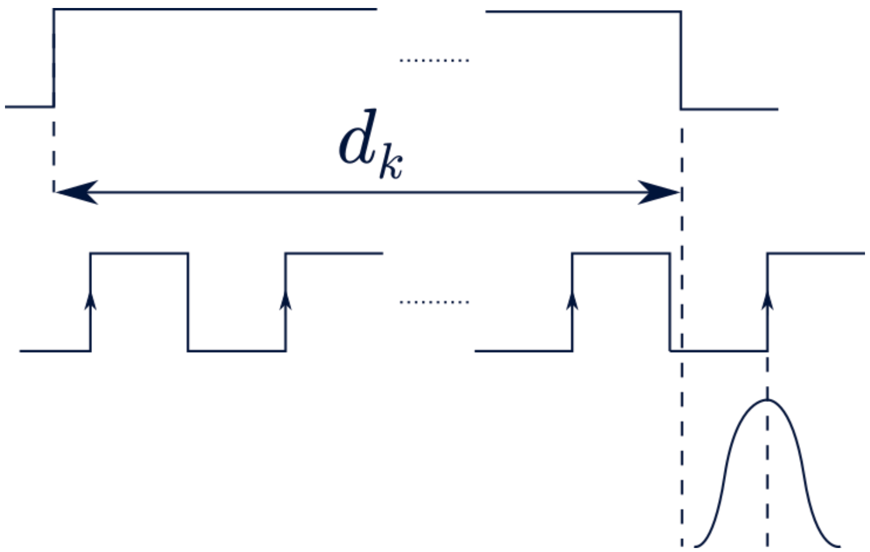
Unexploitable cases

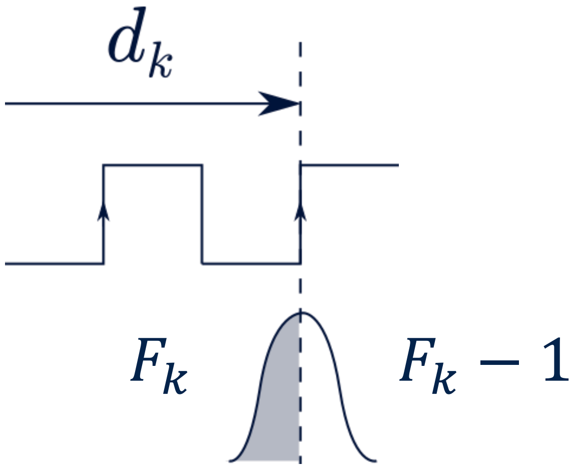


- Let us count the edges of an oscillator during a certain time d_k:

1. Always the same counter value

2. Two different counter values in the same proportion



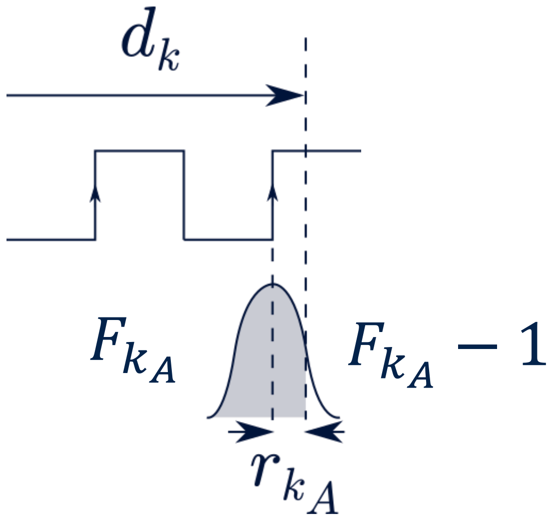


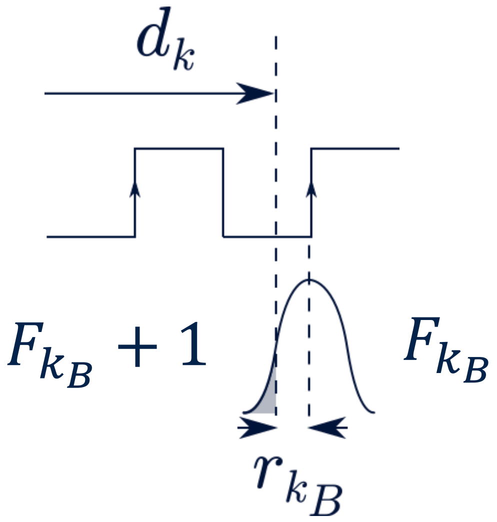
Exploitable cases

On average,

A) d_k arrives After the last edge $k = k_A$

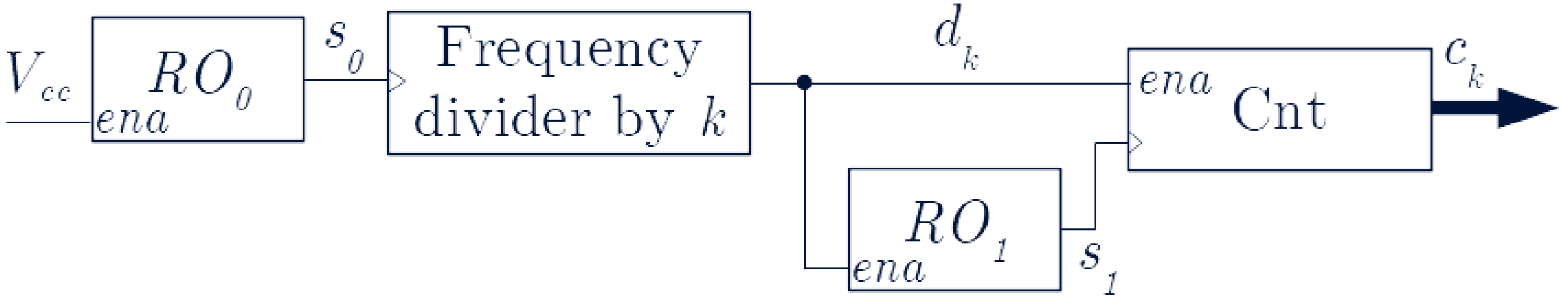
B) d_k arrives Before the last edge $k = k_B$





- The shadowed surfaces $A_k \approx \frac{M_k}{N}$
  - M_k is the amount of counter values equal to one of the different counter values
  - N is very big number, the number of taken samples

life.augmented



1

Vary k

Acquire N counter values for each k

2

Identify cases $k = k_A$ and $k = k_B$

Register k, F_k, M_k

3

Set $k = L$, a very large number

We measure $\frac{c_L}{L} \approx \frac{T_0}{T_1}$

4

Estimate the jitter

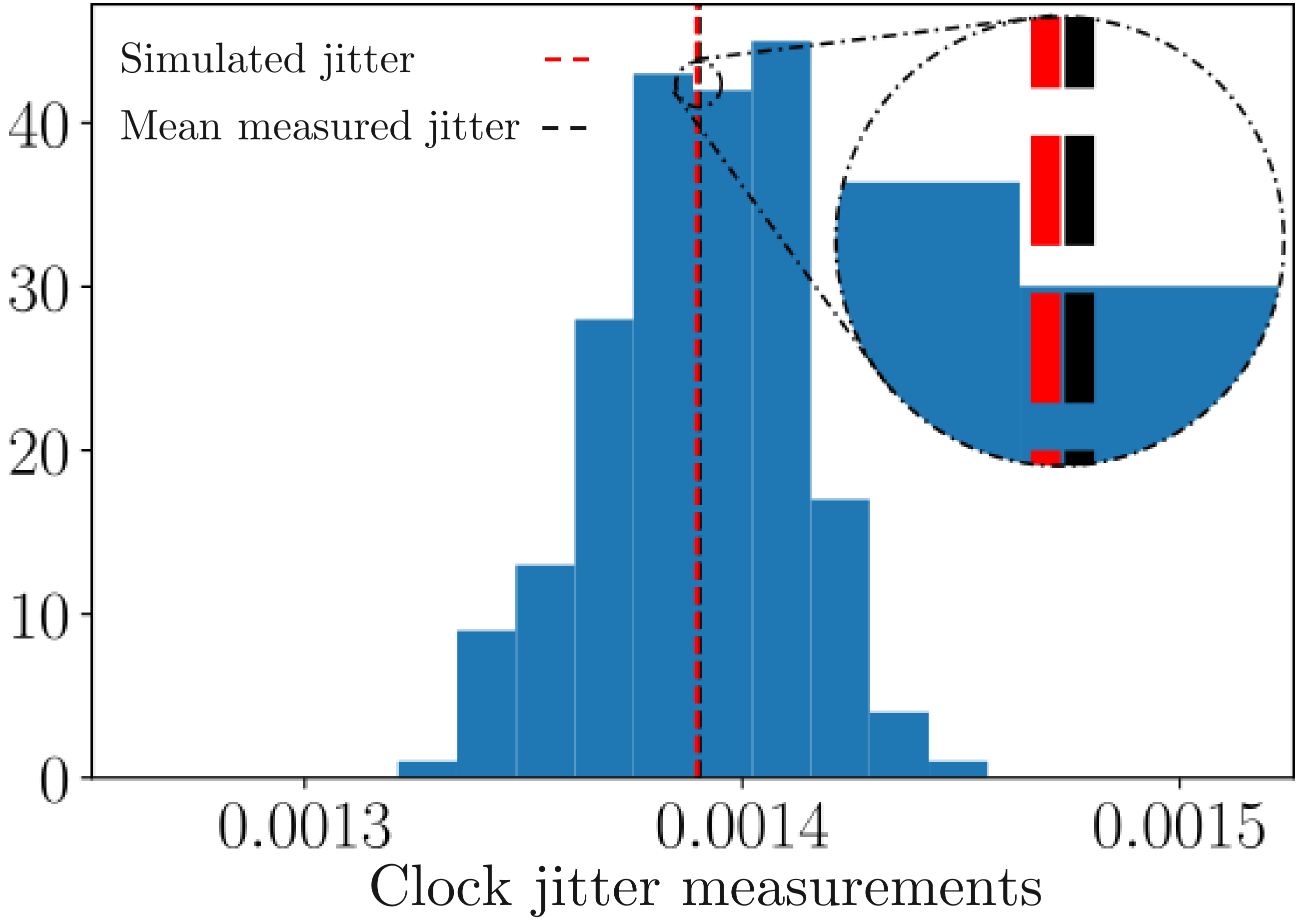
$$\frac{a_{th}}{T_1} \approx \frac{\tilde{a}_{th}}{T_1} = f\left(\frac{c_L}{L}, \frac{M_{k_A}}{N}, \frac{M_{k_B}}{N}, k_A, k_B, F_{k_A}, F_{k_B}\right)$$

life.augmented

b) The advantages of our method

life.augmented

Very precise



Cyclone V FPGA

- We emulated the ROs and simulate thermal noise.
  - 0.04% average error
  - 4.97% maximum error

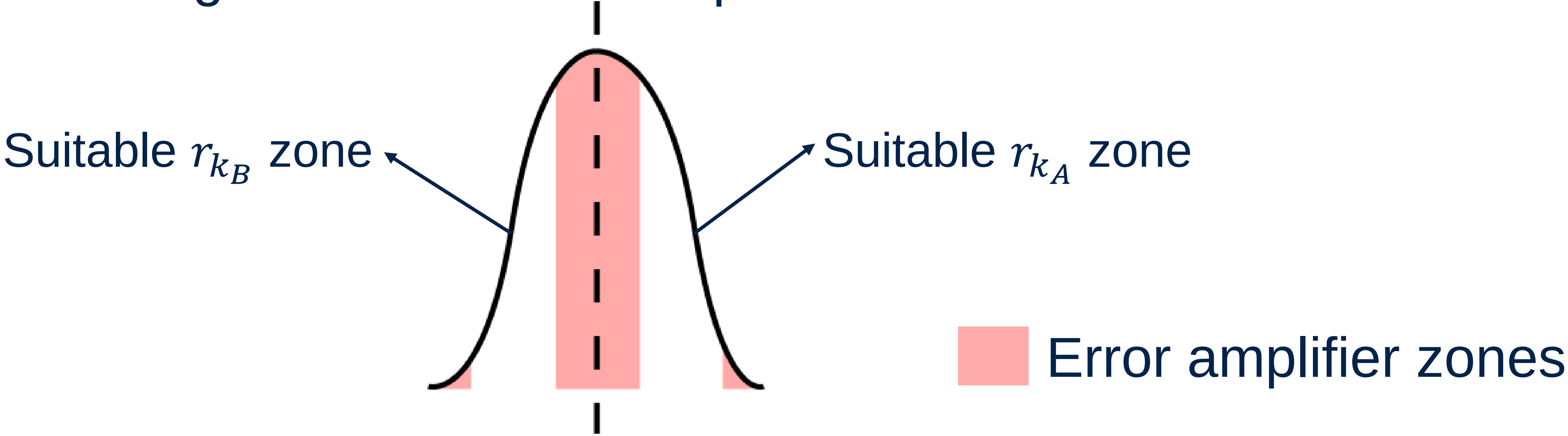
- Different average periods
- Different initial phase shift

Hardware independent precision

Note: $N = 4\,096\,; L = 65\,535$

A bounded error

- The main source of error comes from $\frac{M_k}{N} \approx A_k$
  - We need to get far from the unexploitable cases



  - This error can be bounded through r_{k_A} and r_{k_B}
  - In practice we set N and limit M_{k_A} and M_{k_B}

A bounded error

- The secondary source of error comes from $\frac{c_L}{L} \approx \frac{T_0}{T_1}$
  - Can be bounded by setting a large enough L value
- We can calculate the maximal error bound from those sources, δ_W

$$\frac{1}{1+\delta_W} \cdot \frac{\tilde{a}_{th}}{T_1} \leq \frac{a_{th}}{T_1}$$

- Considering δ_W, we guarantee not to overestimate the jitter
    - Conservative result
  - If $N = 4\,096; L = 65\,535; |k_A - k_B| \leq 16 \Rightarrow \delta_W$ < 10.8%

Parametrizable measurement run-time

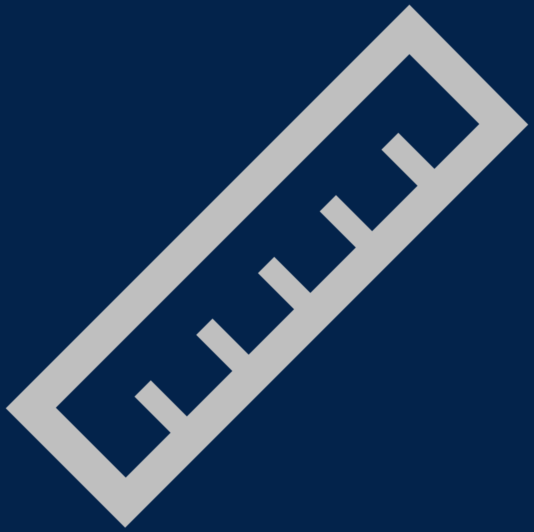
- The measurement run-time is a function of N
- Lower $N \Rightarrow$ faster measurements $\Rightarrow$ bigger δ_W
- The error bound is still controlled

Low flicker noise impact

- The method can exploit very small k
  i.e., very short accumulation times
- Smaller $k \Longrightarrow$ lower flicker influence

life.augmented

c) Measurement in hardware



life.augmented

Measurement results

FPGA	k_A	k_B	$\tilde{a}_{th}/T_1$	δ_W	$\frac{1}{1+\delta_W} \cdot \frac{\tilde{a}_{th}}{T_1}$
Cyclone V	112	99	0.9425‰	9.76%	0.8586‰
Spartan 6	117	102	1.087‰	10.58%	0.9836‰
SmartFusion 2	115	103	0.9491‰	9.31%	0.8683‰

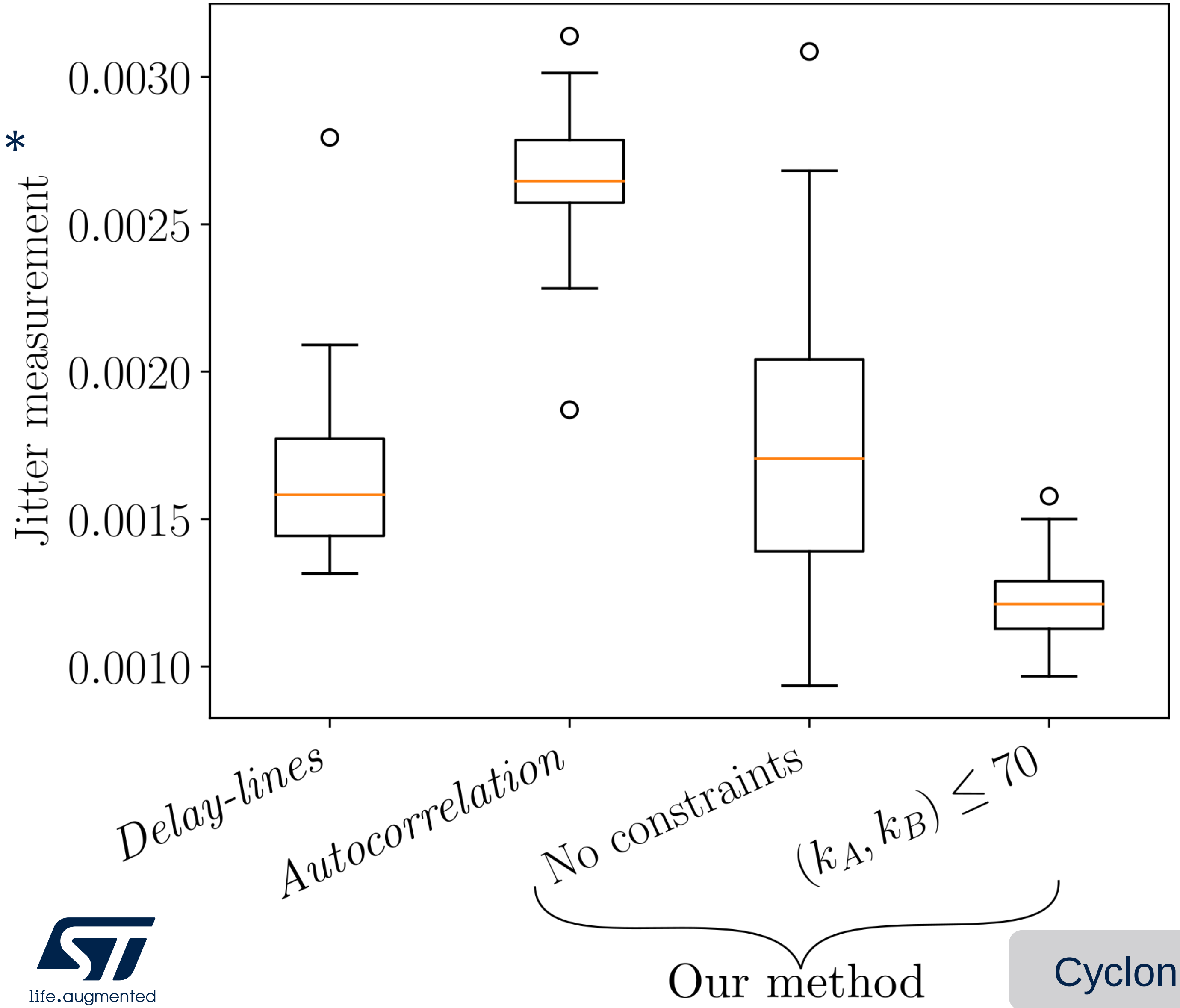
→ Conservative approximate

- Repeatable results in different FGPAs
- Usually, $k_A; k_B \approx 100$ but it is possible to find $k_A; k_B \approx 50$
- In real measurements in FPGAs $\delta_W \approx 10\%$

Note: $N = 4\,096\,; L = 65\,535$

life.augmented

Comparison with other methods in FPGA



- Objective comparison
  - Under the same conditions
  - Same FPGA
- Used The HECTOR project boards
- Our measure using short accumulation times:
  - More precision
  - Less flicker noise influence

Cyclone V FPGA

$* \frac{a_{th}}{T_1}$

life.augmented

Comparison with other methods - in an FPGA

	Autocorrelation	Delay chain	Our method
Total run-time (in cycles of RO_0)	$1.2\ 10^5$	$1.7\ 10^5$	$6\ 10^5$
Area (ALMs)	266	1759	260
Power consumption (mW)	9.9	20.9	8.8

- in an ASIC

	Autocorrelation	Coherent sampling	Our method
Accumulation period (k)	325	89	**10**
$\tilde{a}_{th}/_{T}$ (‰)	3.46	1.04	**0.42**

Key points - 2) Our method

Our method is the **best** option yet

- Bounded and hardware independent error
- Reduces the influence of flicker noise the most
- Easy to implement

Are we really exempt of flicker noise influence?

Agenda - 3) Studying the impact of flicker noise

a Jitter characterization - Background

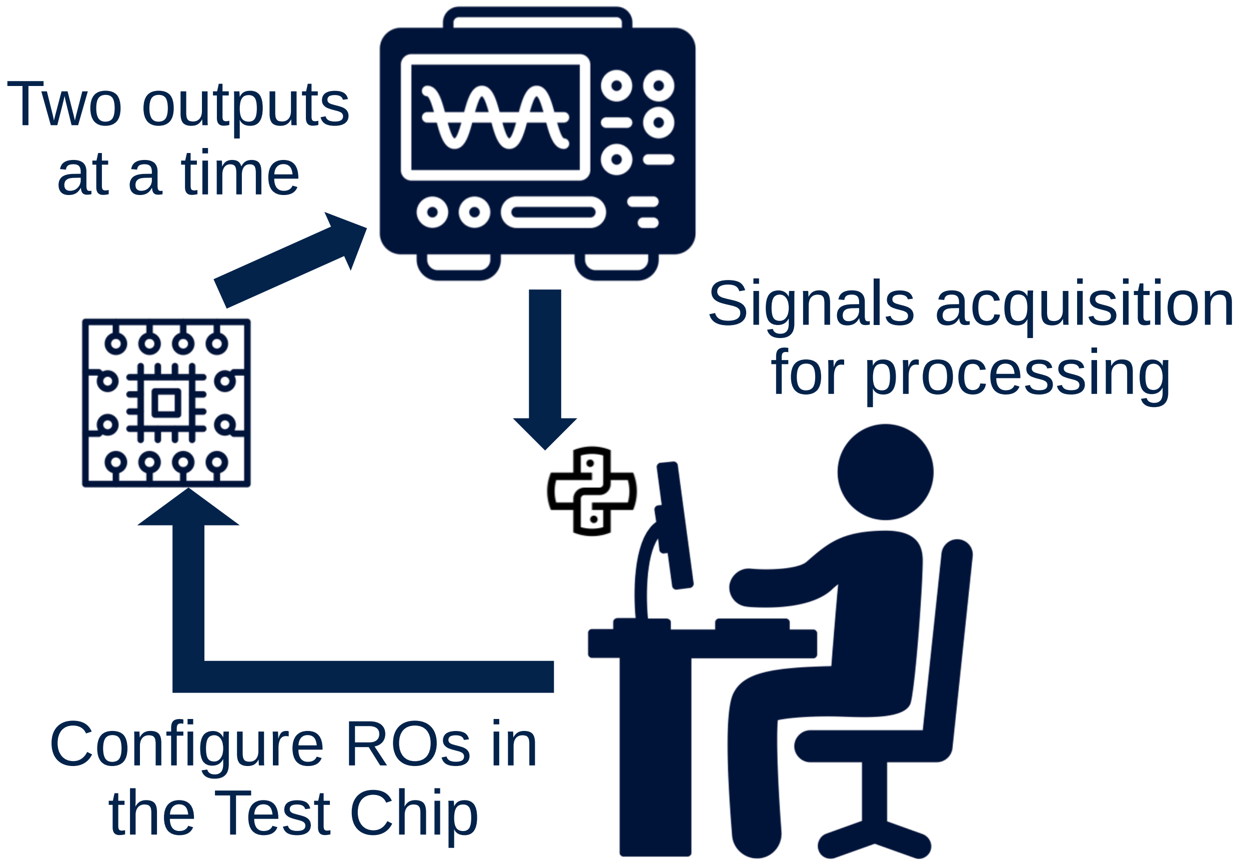
b Our method and flicker noise

life.augmented

a) Jitter characterization - Background

life.augmented

The set-up



- Pair of oscillators at 39MHz
- Set up the oscilloscope at 40GS/s
- Acquire the ROs outputs

Characterize the noise components of the jitter using the acquired traces

life.augmented

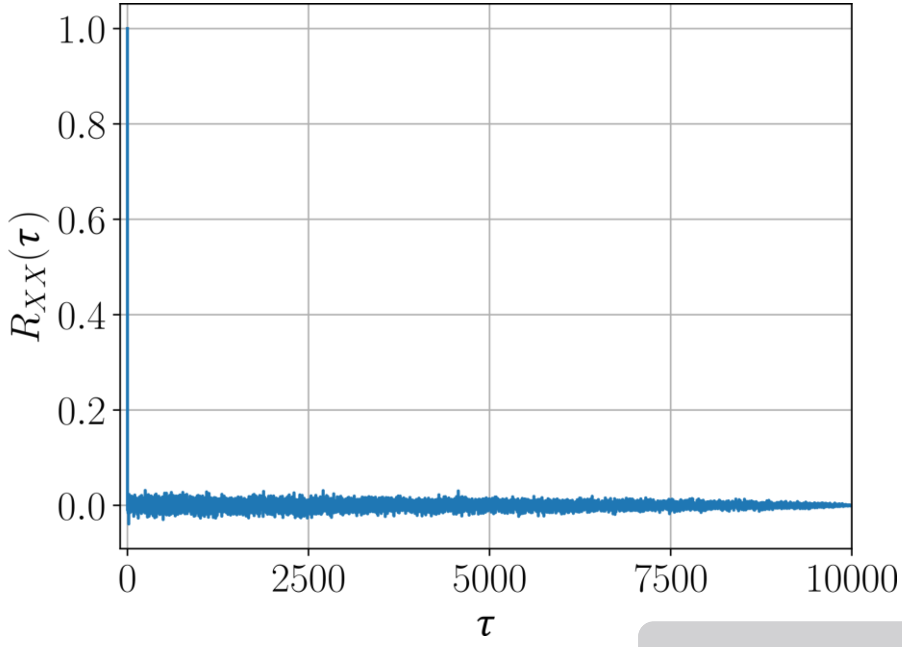
Autocorrelation

- A measurement of how a signal resembles to itself after being shifted of τ

$$R_{xx}(\tau) = \lim_{T\to\infty} \int_{-T/2}^{T/2} x(t)x(t+\tau)dt$$

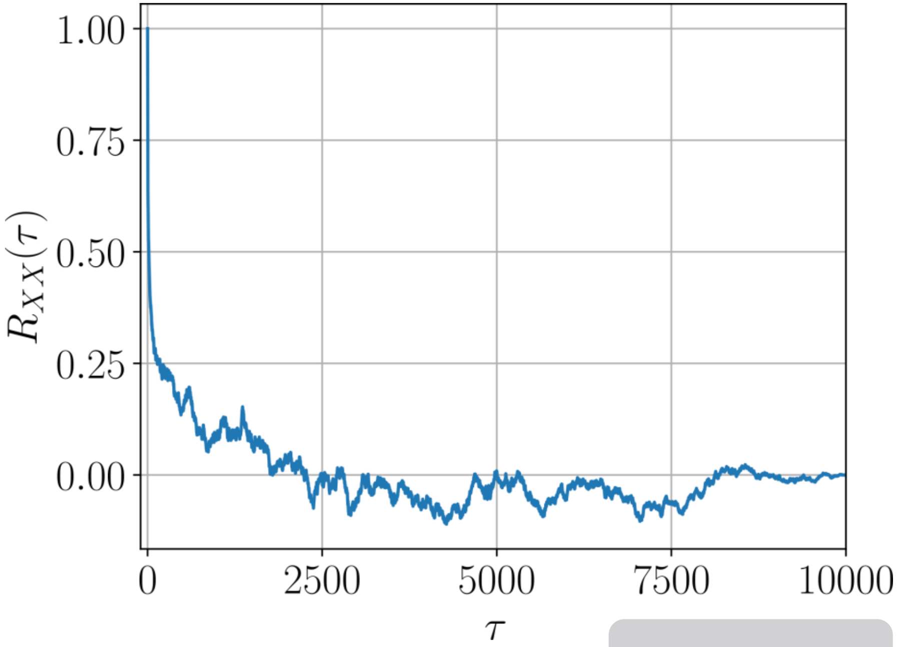
- Different shape depending on the frequency components a signal

Thermal noise



Simulation

Flicker noise



Simulation

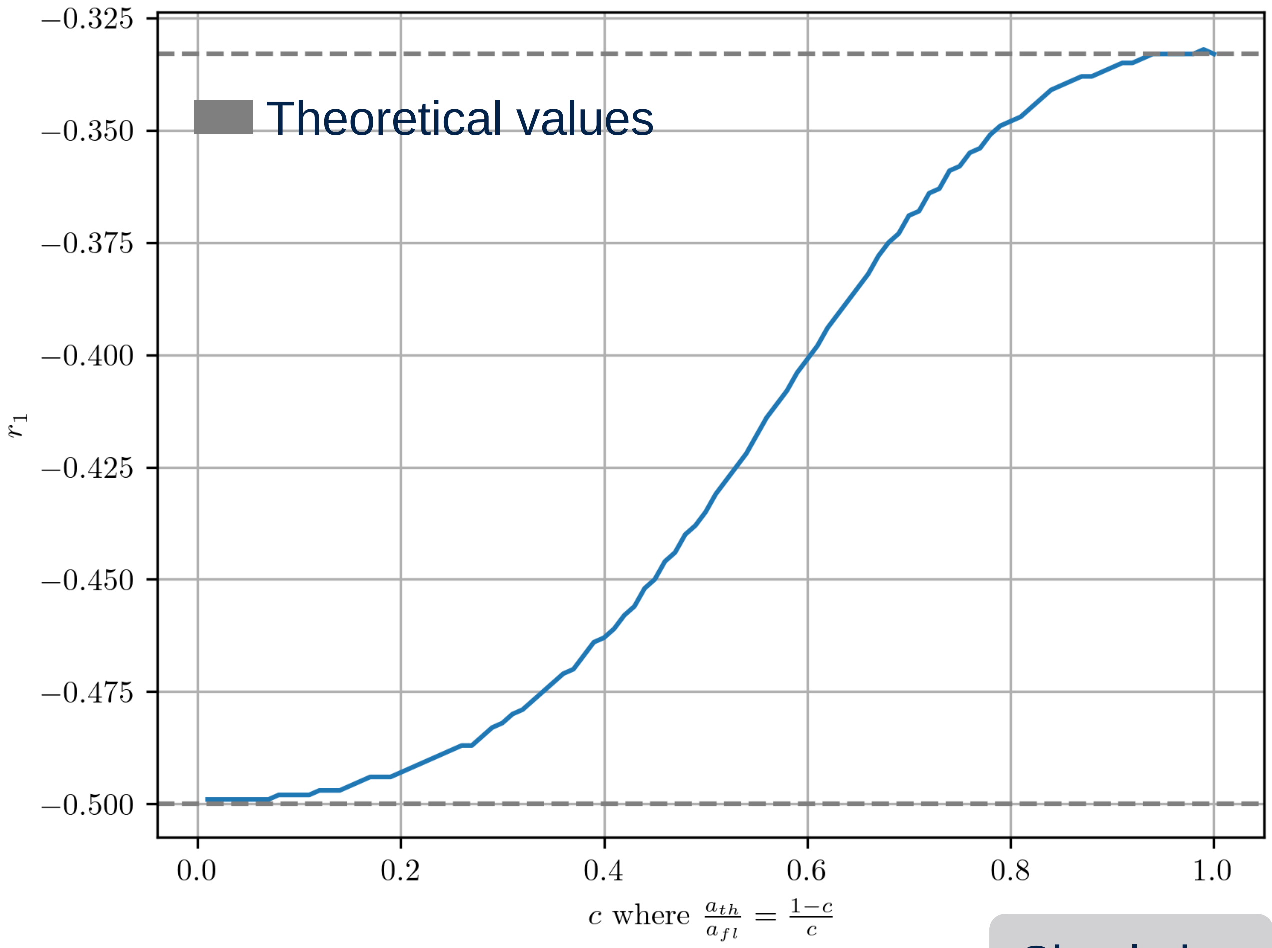
Autocorrelation

- We can use the lag 1 statistic autocorrelation to

identify the governing noise type [8]

$$r_1 = -1/3 \Rightarrow \text{"Pure" } flicker\ noise$$
$$r_1 = -1/2 \Rightarrow \text{"Pure" } thermal\ noise$$

- From the Test-Chip we measured: $\boldsymbol{r_1 = -0.337}$

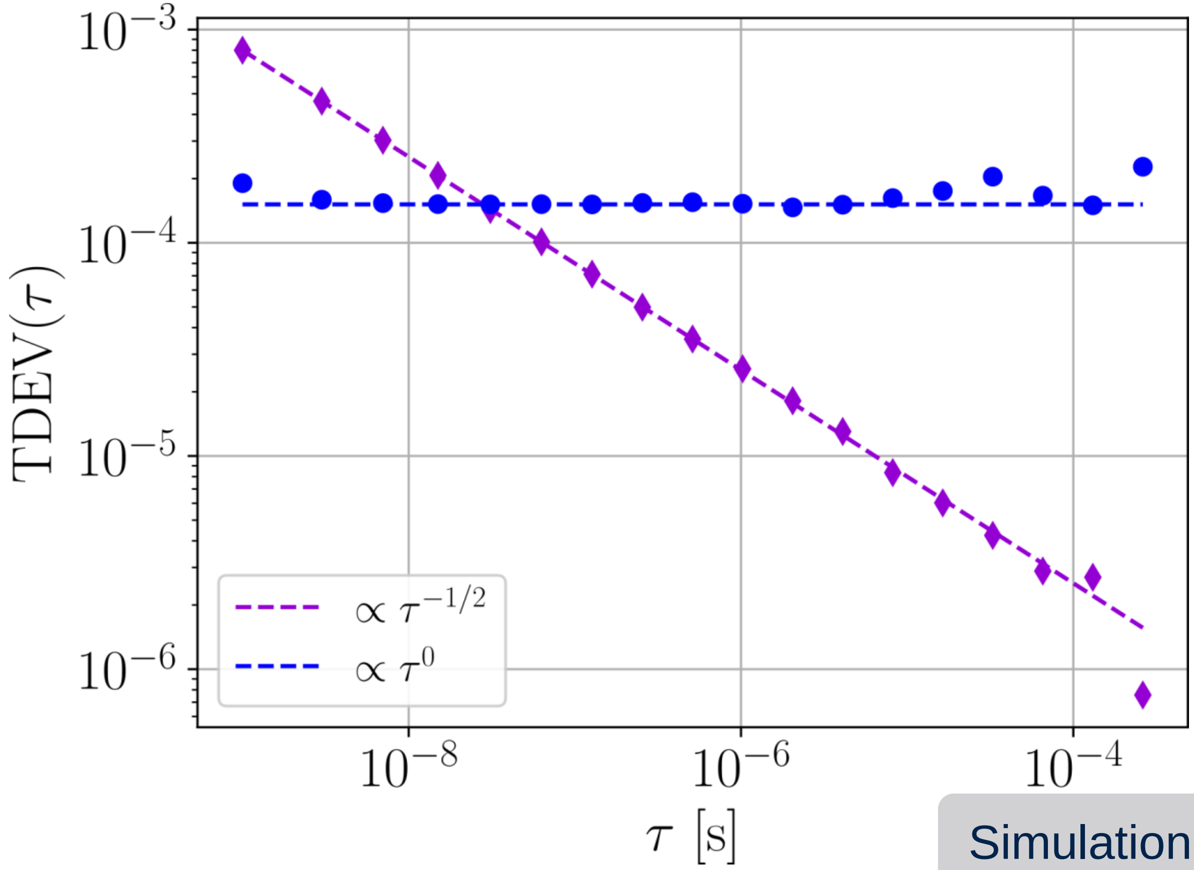


Simulation

[8] W. Riley and D. Howe. Handbook of Frequency Stability Analysis. Tech. rep. NIST SP 1065. Gaithersburg, MD: National Institute of Standards and Technology, July 2008.

Time Allan variance - illustration

$$TDEV(\tau) \propto \tau^{\alpha}$$



Simulation

Each α corresponds to a noise source [9]

$\alpha = {}^{-1}/_{2}$ White noise

$\alpha = 0$ Flicker noise

[9] F. Vernotte. “Stabilité temporelle et fréquentielle des oscillateurs : modèles”. In: vol. RE1. June 2006, R680/1–R680/10.

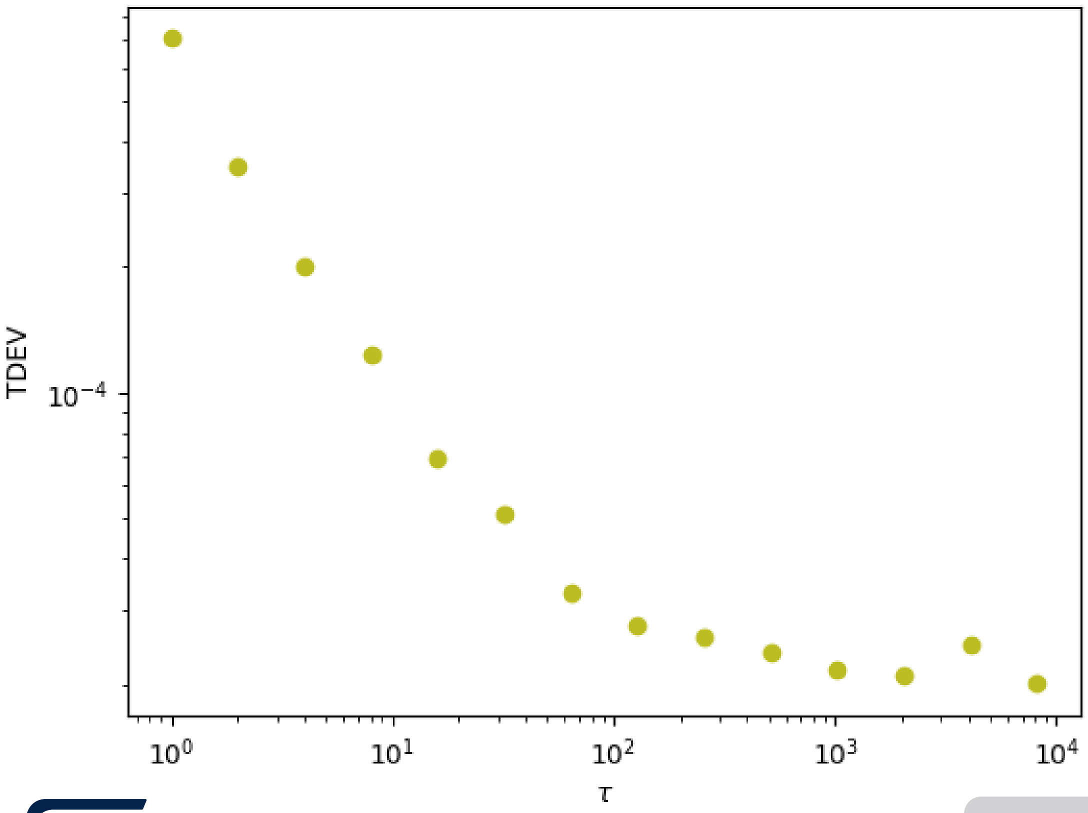
Time Allan variance - results

$$\frac{a_{th}}{T_1} = f[TDEV(\tau)]$$

Thermal dominance

Flicker dominance

$$\frac{a_{fl}}{T_1} = f[TDEV(\tau)]$$



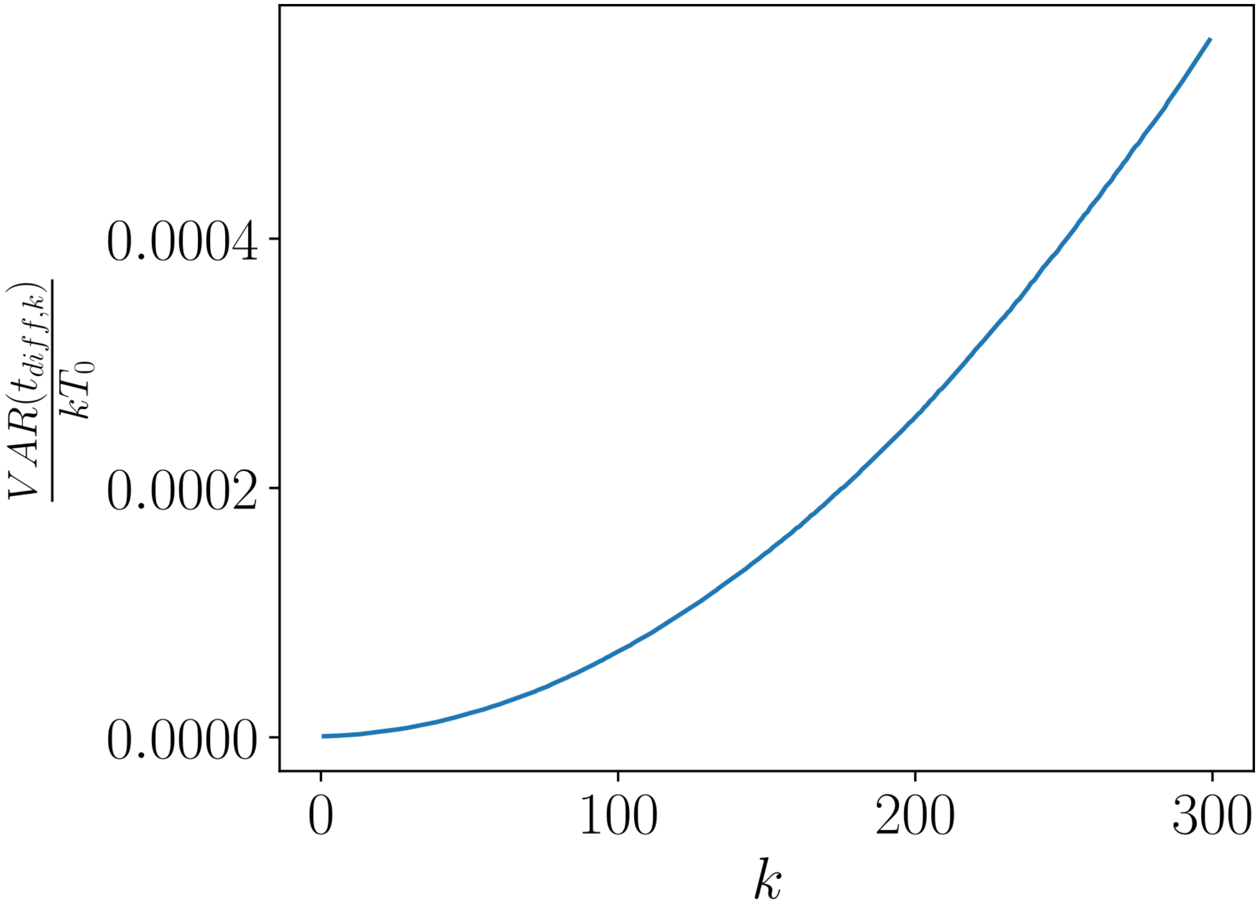
ASIC

From the Test-Chip we measured:

$$\tilde{a}_{th}/T = 0.75‰$$

Curve fitting method

$$\sigma^2(k) = a_q + a_{th}^2 k + a_{fl}^2 k^2$$



- Shadowed thermal jitter component
  - Earlier by the quantization error
  - Later by the flicker component

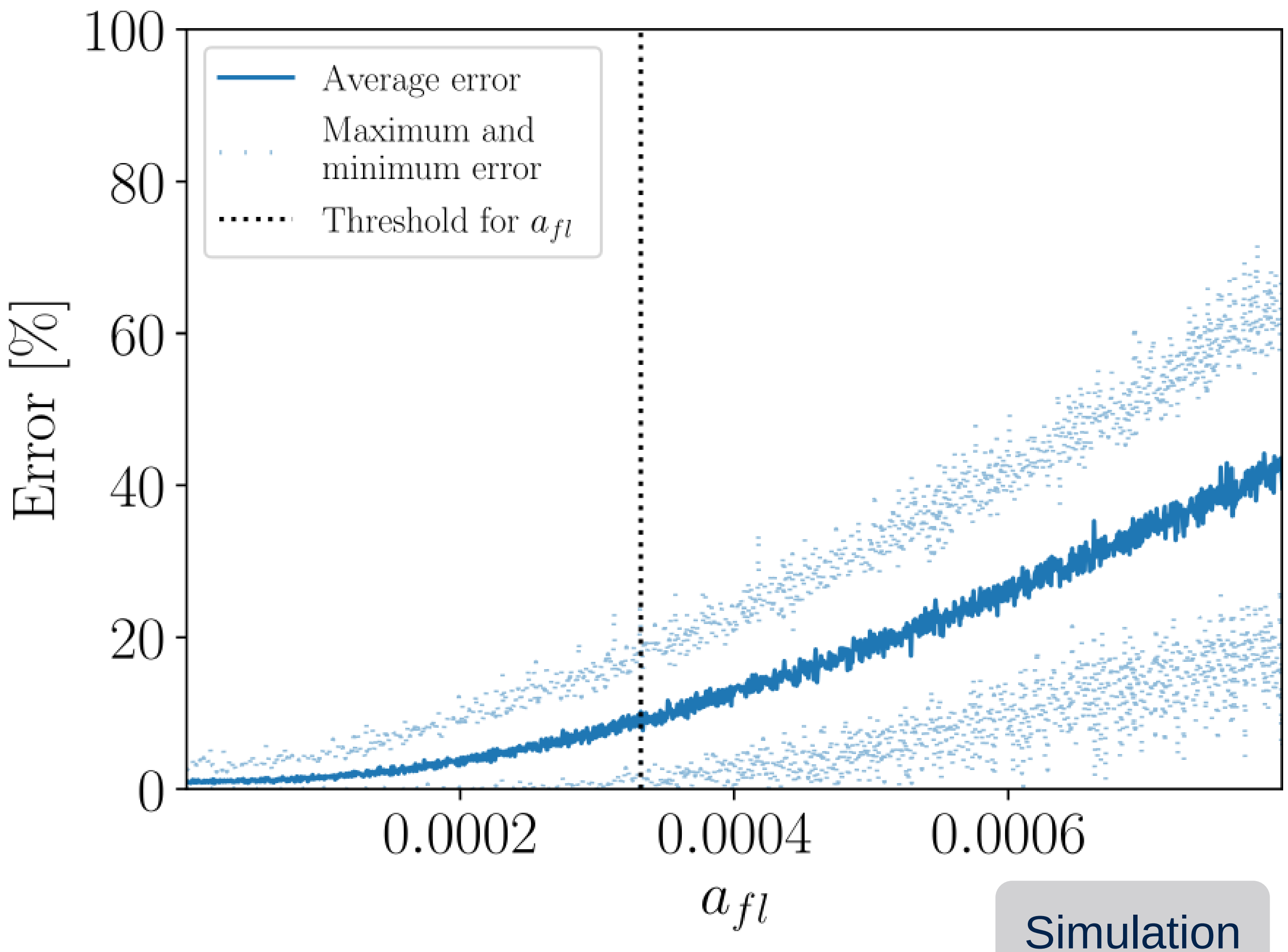
- From the Test-Chip we measured:
  $\tilde{a}_{th}/_T = \mathbf{0.35‰}$

ASIC

[10] L. Benea, M. Carmona, F. Pebay-Peyroula, and R. Wacquez. “On the Characterization of Jitter in Ring Oscillators using Allan variance for True Random Number Generator Applications”. In: DSD 2022

life.augmented

Curve fitting method - Error



Simulation

- Dependence on a_{fl}
- On simulations and using our criteria, we conclude:

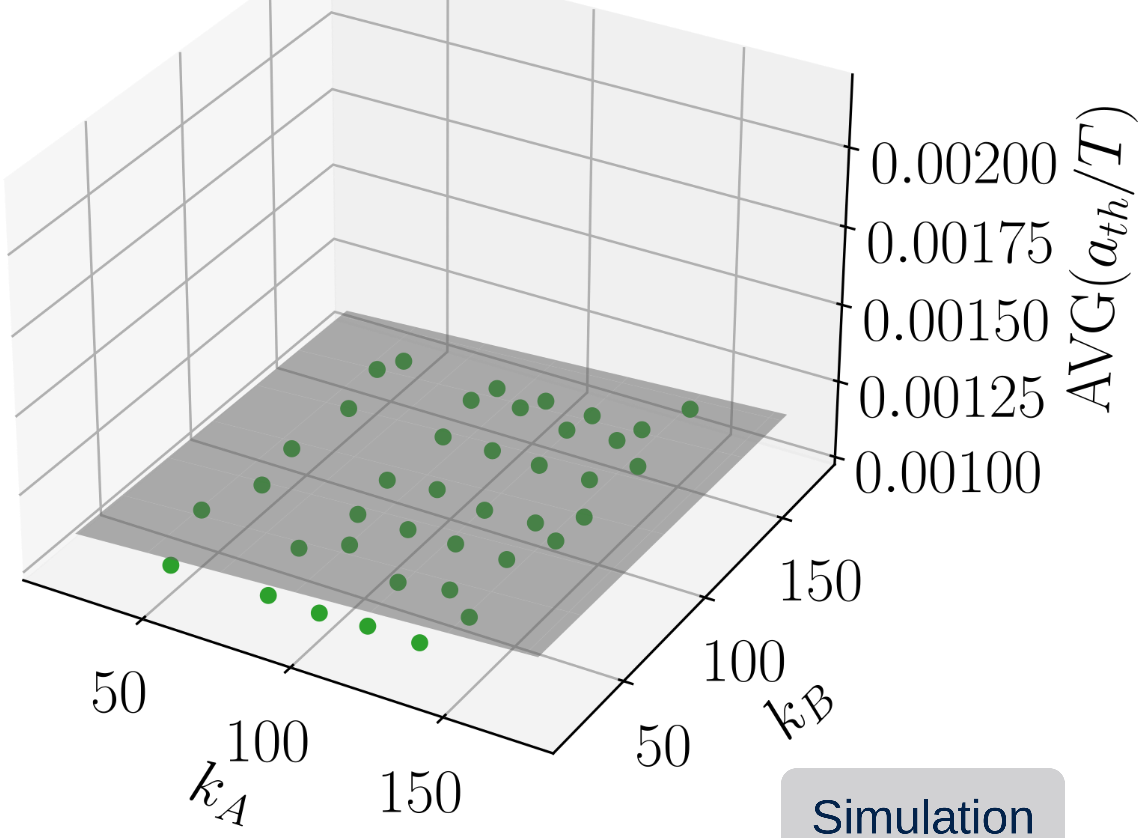
$$a_{th}/a_{fl} > 2.41$$

life.augmented

b) Our method and flicker noise

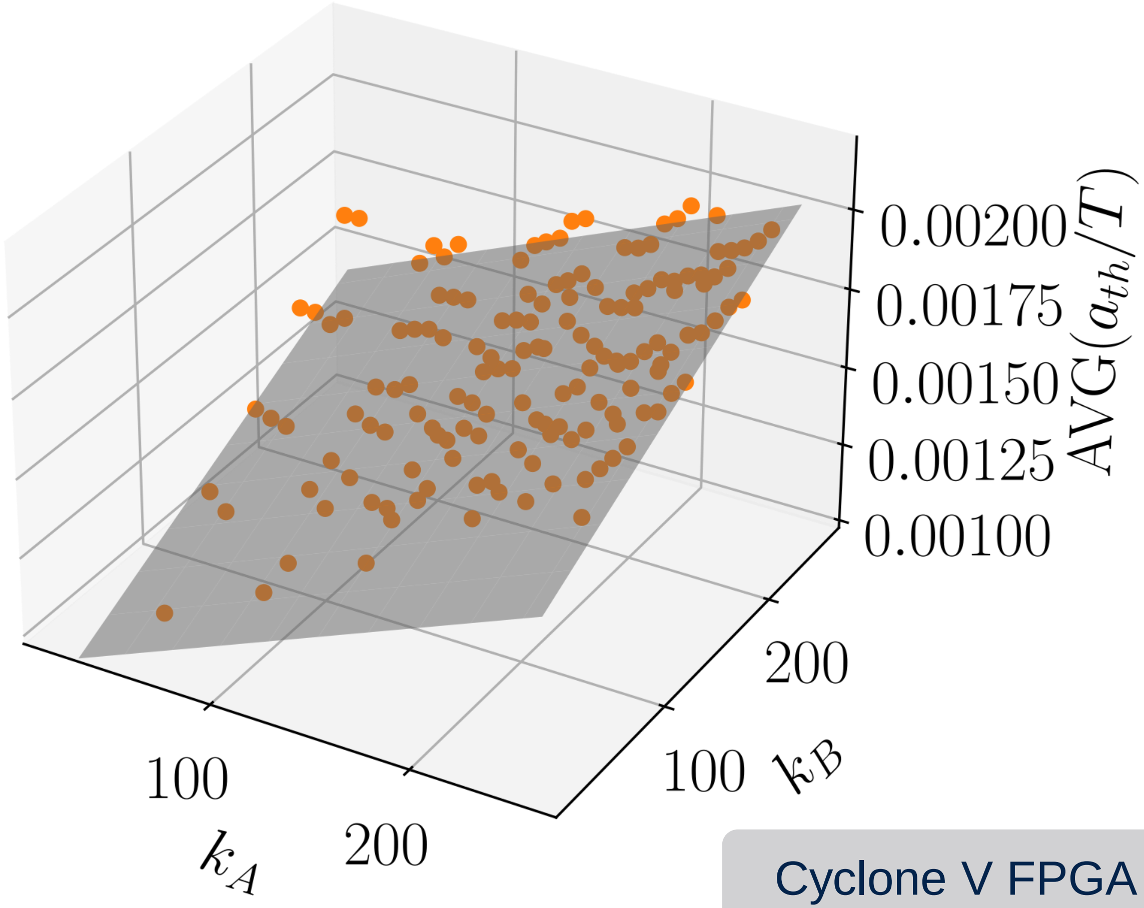
Simulations vs. reality – our method

Measurements in Simulation with thermal noise (ideal behavior)



Simulation

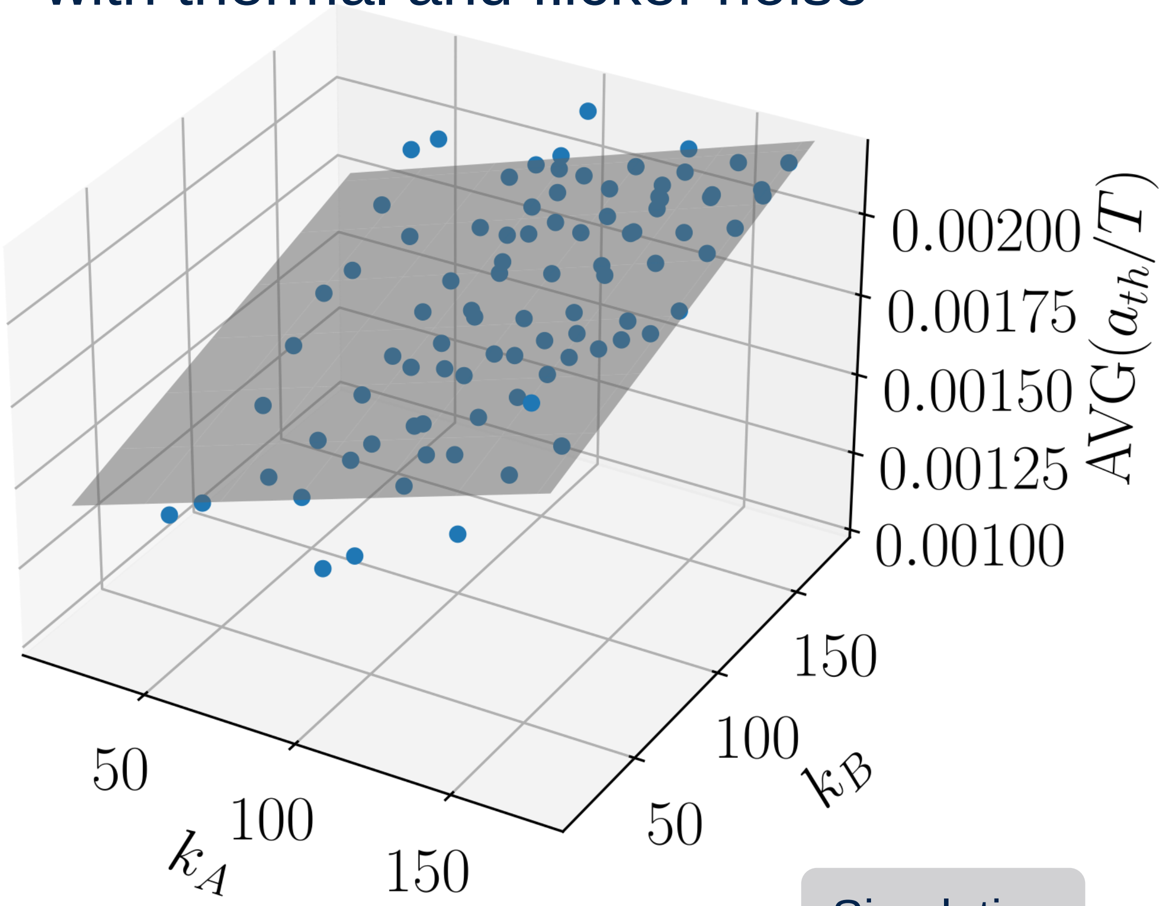
Measurements in FPGA (real behavior)



Cyclone V FPGA

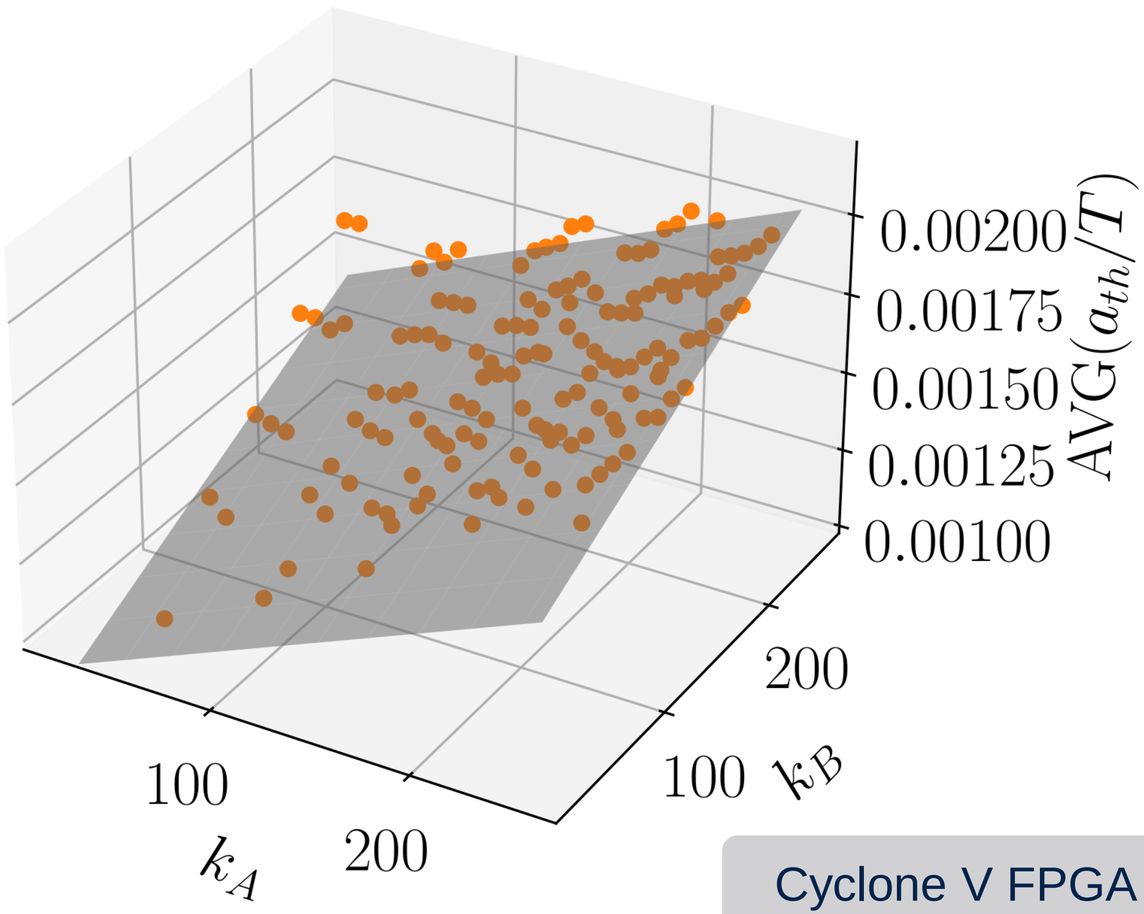
Simulations vs. reality – our method

Measurements in Simulation
with thermal and flicker noise



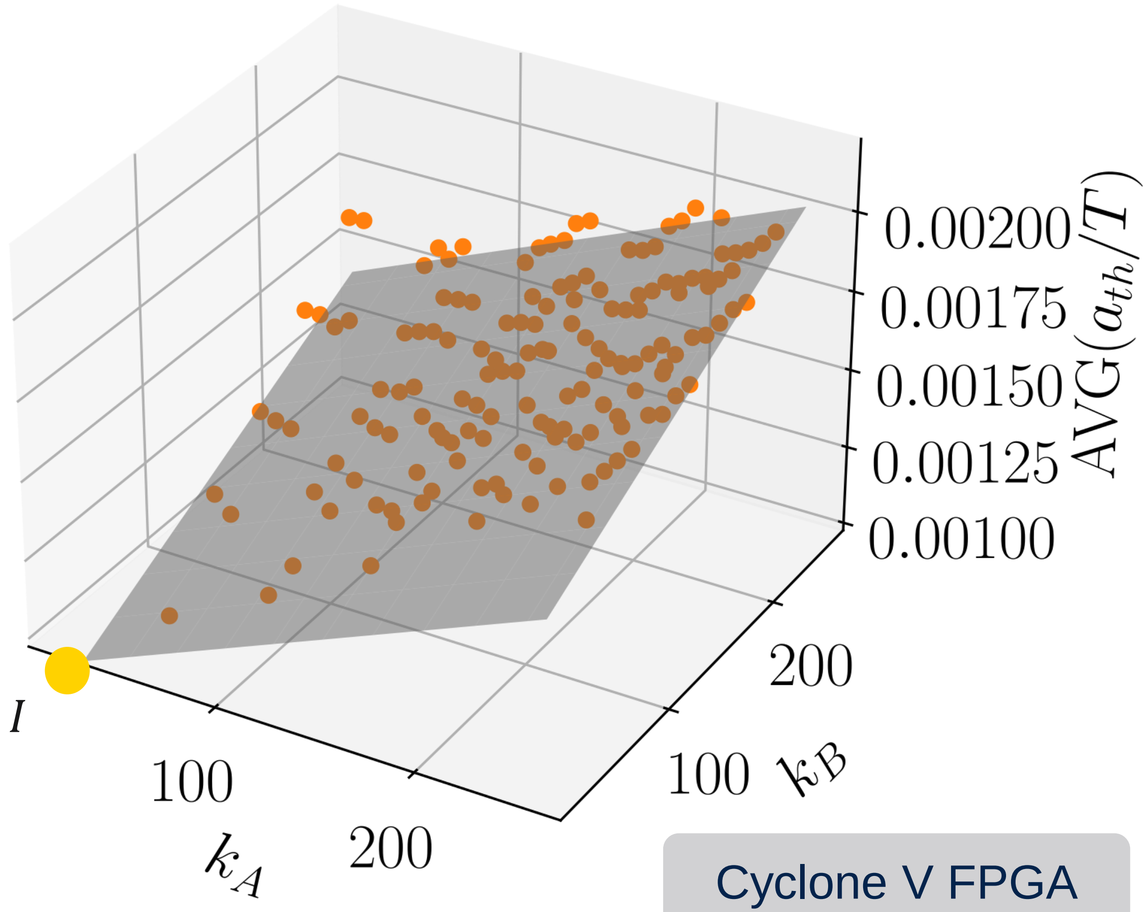
Simulation

Measurements in FPGA



Cyclone V FPGA

An estimation of the thermal coefficient

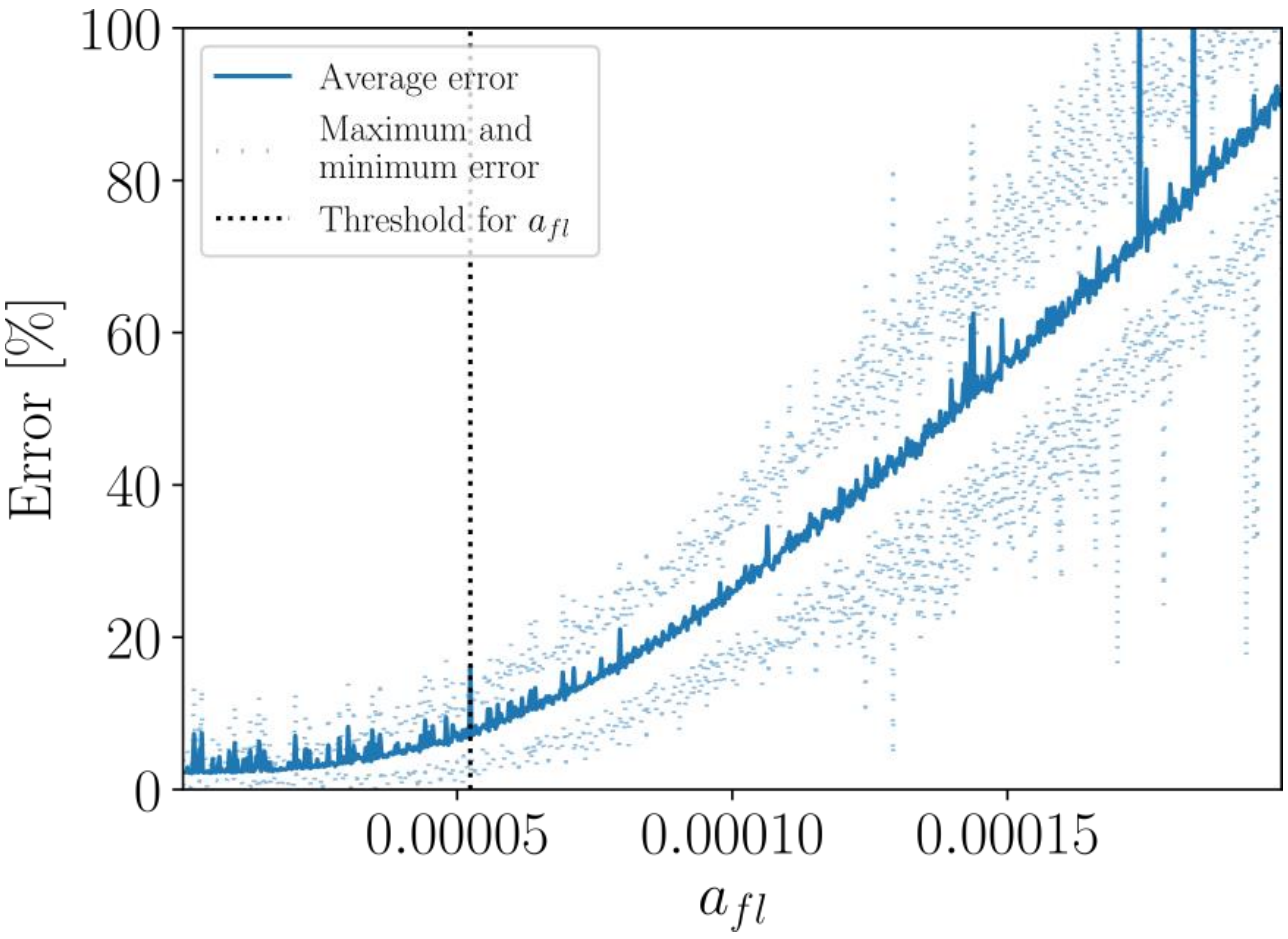


Cyclone V FPGA

- I intersection of the regressed plane to the origin
- I is a good approximation of a_{th}
- From the Test-Chip we measured:

$$\tilde{a}_{th}/T = \mathbf{0.42‰}$$

An estimation of the thermal coefficient - Error



- Dependence on a_{fl}
- I is a good approximation of a_{th}
  - if $a_{fl} \ll a_{th}$ (analytically confirmed)
- Using our criteria

$$a_{th}/a_{fl} > \mathbf{14.28}$$

Key points - 3) Studying the impact of flicker noise

Most characterizing methods require **external measurements**

Flicker noise seems to govern very fast

We must **prioritize** short jitter accumulation times

Our method can be used, if we **have knowledge of the proportion** $\boldsymbol{a_{th}/a_{fl}}$

life.augmented

Conclusions

We have **successfully** developed and embedded differential jitter measurement method that uses short jitter accumulation times

Flicker noise might shadow our measurements, we need to characterize clock jitter into its noise components

Perspective

- Find a characterizing method adapted to our needs
- Deducing the jitter coefficients from the physical characteristics of a transistor

life.augmented

Bibliography

[1] W. Killmann and W. Schindler. A Proposal for: Functionality Classes for Random Number Generators, AIS20/31. 2011

[2] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux. “On the Security of Oscillator-Based Random Number Generators”. (Apr. 2011), pp. 398–425

[3] B. Valtchanov, V. Fischer, and A. Aubert. “A Coherent Sampling Based Method for Estimating the Jitter Used as Entropy Source for True Random Number Generators”. In: SAMPTA 2009

[4] P. Haddad, Y. Teglia, F. Bernard, and V. Fischer. “On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models”. In: DATE 2014

[5] B. Valtchanov, A. Aubert, F. Bernard, and V. Fischer. “Modeling and observing the jitter in ring oscillators implemented in FPGAs”. In: DDECS 2008

[6] B. Yang, V. Rozic, M. Grujic, N. Mentens, and I. Verbauwhede. “On-chip jitter measurement for true random number generators”. In: AsianHOST 2017

[7] V. Fischer and David Lubicz. “Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG”. In: CHES 2014

[8] W. Riley and D. Howe. Handbook of Frequency Stability Analysis. Tech. rep. NIST SP 1065. Gaithersburg, MD: National Institute of Standards and Technology, July 2008

[9] F. Vernotte. “Stabilité temporelle et fréquentielle des oscillateurs : modèles”. In: vol. RE1. June 2006, R680/1–R680/10

[10] L. Benea, M. Carmona, F. Pebay-Peyroula, and R. Wacquez. “On the Characterization of Jitter in Ring Oscillators using Allan variance for True Random Number Generator Applications”. In: DSD 2022

Our technology starts with You

Find out more at www.st.com

© STMicroelectronics - All rights reserved.
ST logo is a trademark or a registered trademark of STMicroelectronics International NV or its affiliates in the EU and/or other countries.
For additional information about ST trademarks, please refer to www.st.com/trademarks.
All other product or service names are the property of their respective owners.

life.augmented