Short Accumulation Time based method for precise jitter measurement

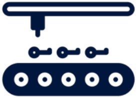
Florent BERNARD, Arturo MOLLINEDO GARAY, Nathalie BOCHARD, Viktor FISCHER

<florent.bernard@univ-st-etienne.fr>

Université Jean Monnet
Laboratoire Hubert curien
SESAM team

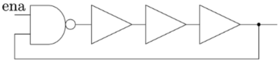
ECW - Workshop TRNG & PUF by DGA

TRNG

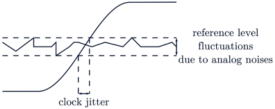


TRNGs are used to generate the inputs of cryptographic systems

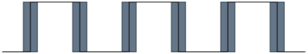
A randomness source is required



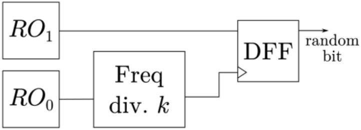
Ring oscillators are easily implementable in digital circuits



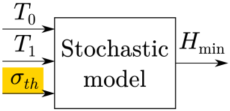
These fluctuations are an inevitable random phenomena



TRNG Evaluation



eRO-TRNG



Lower bound entropy

Parametered model

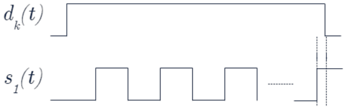
Online and embedded measurement of σ_{th} → Security evaluation Guarantee of the TRNG performance

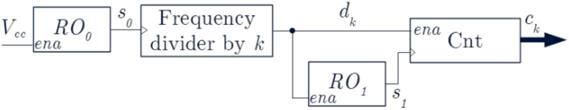
Outline

1. Short Accumulation Time Method
2. Precision of the method, Error Analysis and Conservative Approach
3. From Simulation to reality : Hardware implementation and results (and future work)

Basic principle

- Define a set of (short) accumulation times : $k \in \{10, \ldots, 250\}$
- For each k in this set, repeat the experiment N times





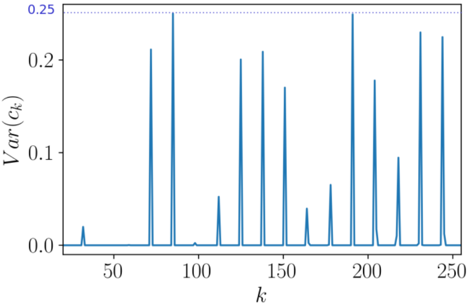
For a given k

- c_k is always 0.

or

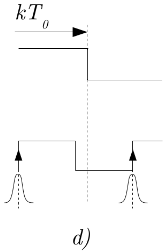
- c_k values differ of only 1.

This phenomenon is caused by the clock jitter.



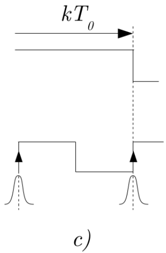
Position of the last rising edge : different cases

Two unexploitable cases :



$Var(c_k) = 0$

- c_k has only one constant value
- No information on the jitter can be retrieved

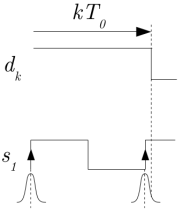


$Var(c_k) = 0.25$

- c_k has exactly two (perfectly balanced) outcomes
- No information on the jitter can be either retrieved

Position of the last rising edge : different cases

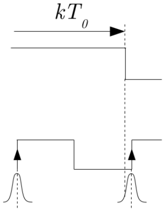
Two very interesting cases (experimentally easy to identify) :



a)

$0 < Var(c_k) < 0.25$

- c_k has exactly two (unbalanced) outcomes $F_{k_A} - 1$ and F_{k_A}
- The end of the measurement window falls more likely **after** the last rising edge.
- $\#\{F_{k_A} - 1\}$<$\#\{F_{k_A}\}$

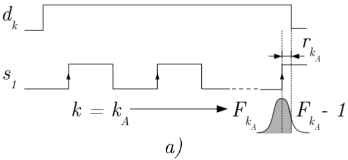


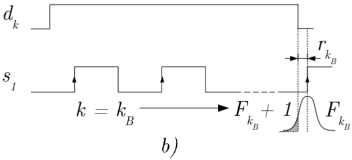
b)

$0 < Var(c_k) < 0.25$

- c_k has exactly two (unbalanced) outcomes F_{k_B} and $F_{k_B} + 1$
- The end of the measurement window falls more likely **before** the last rising edge.
- $\#\{F_{k_B}\}$>$\#\{F_{k_B} + 1\}$

Exploiting cases a) and b) to measure the jitter



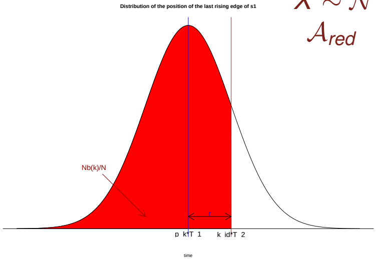


$$\boxed{\varphi_0 + T_1 \cdot (F_{k_A} - 1) + \underbrace{r_{k_A}}_{\gtrsim 0} = k_A \cdot T_0}$$

$$\boxed{\varphi_0 + T_1 \cdot F_{k_B} - \underbrace{r_{k_B}}_{\gtrsim 0} = k_B \cdot T_0}$$

From Counter values to jitter estimation

In case a) :

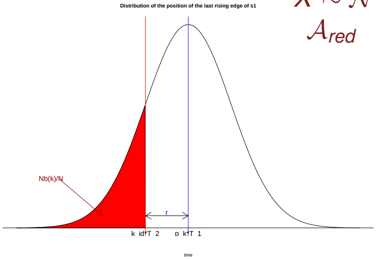


$$X \sim \mathcal{N}(\mu, \sigma) \text{ and } Y \sim \mathcal{N}(0,1)$$

$$\begin{aligned}
\mathcal{A}_{red} &= Pr(X \leq r_{k_A} + \mu) \\
&= Pr\left(\frac{X-\mu}{\sigma} \leq \frac{r_{k_A}}{\sigma}\right) \text{ where } \sigma = \sqrt{F_{k_A}}\sigma_1 \\
&= Pr\left(Y \leq \frac{r_{k_A}}{\sigma}\right) = \Phi\left(\frac{r_{k_A}}{\sigma}\right) \\
&\simeq \frac{M_{k_A}}{N}
\end{aligned}$$

$$\Rightarrow \boxed{r_{k_A} \simeq \Phi^{-1}\left(\frac{M_{k_A}}{N}\right)\sqrt{F_{k_{k_A}}}\sigma_1}$$

In case b) :



$$X \sim \mathcal{N}(\mu, \sigma) \text{ and } Y \sim \mathcal{N}(0,1)$$

$$\begin{aligned}
\mathcal{A}_{red} &= Pr(X \leq \mu - r_{k_B}) \\
&= Pr\left(\frac{X-\mu}{\sigma} \leq \frac{-r_{k_B}}{\sigma}\right) \text{ where } \sigma = \sqrt{F_{k_B}+1}\sigma_1 \\
&= Pr\left(Y \leq \frac{-r_{k_B}}{\sigma}\right) = \Phi\left(\frac{-r_{k_B}}{\sigma}\right) \\
&\simeq \frac{M_{k_B}}{N}
\end{aligned}$$

$$\Rightarrow \boxed{r_{k_B} \simeq -\Phi^{-1}\left(\frac{M_{k_B}}{N}\right)\sqrt{F_{k_B}+1}\sigma_1}$$

From Counter values to jitter estimation (2)

Equations

- Case a) : $\varphi_0 + T_1 \cdot (F_{k_A} - 1) + r_{k_A} = k_A \cdot T_0$
- Case b) : $\varphi_0 + T_1 \cdot F_{k_B} - r_{k_B} = k_B \cdot T_0$
- $r_{k_A} \simeq \Phi^{-1}\left(\frac{M_{k_A}}{N}\right)\sqrt{F_{k_A}}\sigma_1$
- $r_{k_B} \simeq -\Phi^{-1}\left(\frac{M_{k_B}}{N}\right)\sqrt{F_{k_B}+1}\sigma_1$

Jitter estimation from experimental data under reasonnable assumptions

If φ_0 remains constant during the measurement process, if we have both case a) and case b) in our experiment, and if $\frac{c_L}{L} \approx \frac{T_0}{T_1}$ then :

$$\frac{\sigma_1}{T_1} \simeq \frac{\widetilde{\sigma}_1}{T_1} = \frac{(k_A - k_B)\frac{c_L}{L} - (F_{k_A} - F_{k_B} - 1)}{\Phi^{-1}\left(\frac{M_{k_A}}{N}\right)\sqrt{F_{k_A}} - \Phi^{-1}\left(\frac{M_{k_B}}{N}\right)\sqrt{F_{k_B}+1}}$$

Outline

1. Short Accumulation Time Method
2. Precision of the method, Error Analysis and Conservative Approach
3. From Simulation to reality : Hardware implementation and results (and future work)

Error upper bound

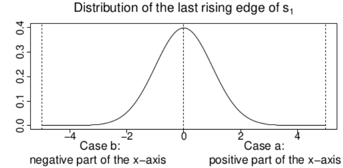
Upper bound of the relative error

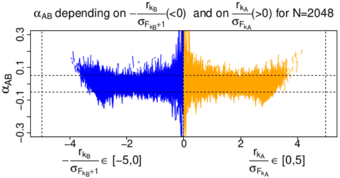
$$\left|1-\frac{\widetilde{\sigma_1}}{\sigma_1}\right| \leq \sqrt{\frac{\max(F_{k_A}, F_{k_B}+1)}{\min(F_{k_A}, F_{k_B}+1)}}\left(|\alpha_{0,1}|+|\alpha_{AB}|+|\alpha_{0,1}\cdot\alpha_{AB}|\right)$$

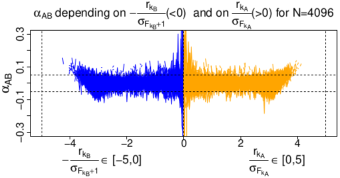
where

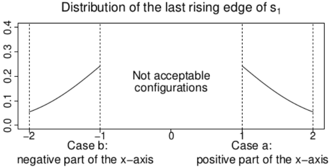
- $\alpha_{AB} := \frac{\Phi^{-1}(\mathcal{A}_{k_B})-\Phi^{-1}\left(\frac{M_{k_B}}{N}\right)-\left(\Phi^{-1}(\mathcal{A}_{k_A})-\Phi^{-1}\left(\frac{M_{k_A}}{N}\right)\right)}{\Phi^{-1}\left(\frac{M_{k_A}}{N}\right)-\Phi^{-1}\left(\frac{M_{k_B}}{N}\right)}$, represents the relative error made in the approximation of the areas $\mathcal{A}_{red}$: $\mathcal{A}_{k_A}$ in case a) and $\mathcal{A}_{k_B}$ in case b) by $\frac{M_{k_A}}{N}$ and $\frac{M_{k_B}}{N}$.
- $\alpha_{0,1} := \frac{(k_A-k_B)\cdot\left(\frac{T_0}{T_1}-\frac{c_L}{L}\right)}{(k_A-k_B)\cdot\frac{T_0}{T_1}-(F_{k_A}-F_{k_B}-1)}$, represents the relative error made in the approximation of $\frac{T_0}{T_1}$ by $\frac{c_L}{L}$

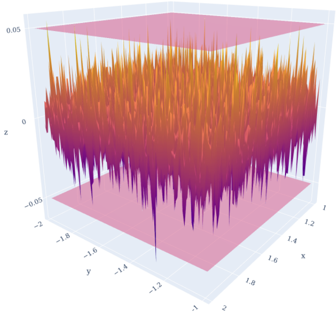
Evaluation of α_{AB} and choice of the method parameters



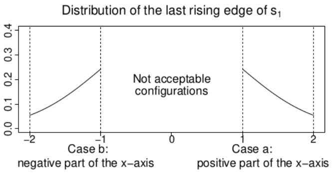


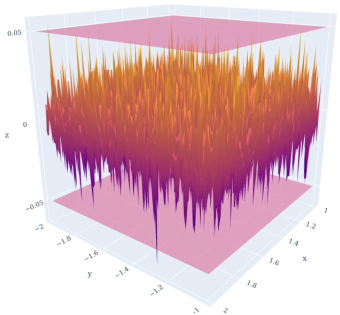






Evaluation of α_{AB} and choice of the method parameters





By choosing,

- $N = 4096$
- $Var(c_k) \in [0.0222; 0.1335] \Leftrightarrow$
$$\begin{cases} 3446 \leq M_{k_A} \leq 4003 \\ 93 \leq M_{k_B} \leq 650 \end{cases}$$

we can guarantee that $\alpha_{AB} \leq 0.05$

If there is not enough configurations, one can relax some constraints and still evaluate the error accordingly.

1. https://src.koda.cnrs.fr/labhc/code4publications/2024-tches-lcpj-measurement-method

LABORATOIRE Hubert CURIEN UMR • CNRS • 5516 • ST-ETIENNE

Evaluation of α_{01} and choice of the method parameters

Error due to the approximation of $\frac{T_0}{T_1}$ by $\frac{c_L}{L}$ for big L ($L = 65536$ for instance)

$$|\alpha_{0,1}| \leq \frac{2|k_A - k_B|}{L \cdot r_{min} \cdot \frac{\sigma_1}{T_1}(\sqrt{F_{k_A}} + \sqrt{F_{k_B}+1})}, \text{ where :}$$

- r_{min} comes from α_{AB} (set to 1 for example to get $\alpha_{AB} \leq 0.05$)
- The bigger $\frac{\sigma_1}{T_1}$, the smaller $\alpha_{0,1}$ (order of magnitude : $\frac{\sigma_1}{T_1} \approx \frac{0.5}{1000}$)

Sufficient condition to guarantee $\alpha_{0,1} \leq 0.05$

Assuming $F_{k_A} \approx F_{k_B} \approx 100$ (short accumulation times) :

$$|k_A - k_B| \leq \frac{0.05 \cdot L \cdot r_{min} \cdot \frac{\sigma_1}{T_1}(\sqrt{F_{k_A}} + \sqrt{F_{k_B}+1})}{2} \approx 16$$

Again, if this condition is too restrictive, one can accept more configurations while still being able to compute an upper bound on the error.

Upper bound of the error and conservative approach

- Under the following conditions (easy to chek experimentally) :
  - $N = 4096$
  - $|k_A - k_B| \leq 16$
  - $3446 \leq M_{k_A} \leq 4003$ and $93 \leq M_{k_B} \leq 650$
  - $F_{k_A} \approx F_{k_B} \approx 100$ (short accumulation time)

Upper bound of the error

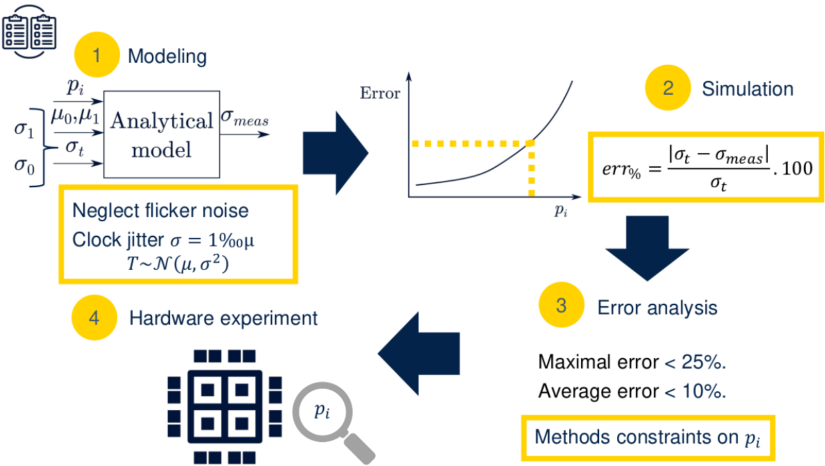
$$\left|1 - \frac{\widetilde{\sigma_1}}{\sigma_1}\right| \leq \underbrace{\sqrt{\frac{\max(F_{k_A}, F_{k_B}+1)}{\min(F_{k_A}, F_{k_B}+1)}}}_{\approx\sqrt{\frac{116}{100}}<1.1} \left(\underbrace{|\alpha_{0,1}|}_{0.05} + \underbrace{|\alpha_{AB}|}_{0.05} + \underbrace{|\alpha_{0,1}\cdot\alpha_{AB}|}_{0.0025}\right) < \underbrace{12.3\%}_{\delta_W}$$

- This upper bound is not too big and can be used to give a . . .

. . .conservative estimation of $\frac{\sigma_1}{T_1}$

$$\frac{\sigma_1}{T_1} \geq \underbrace{\frac{1}{1+\delta_W}\frac{\widetilde{\sigma_1}}{T_1}}_{\text{conservative estimation}}$$

Jitter Measurement Methods : evaluation procedure

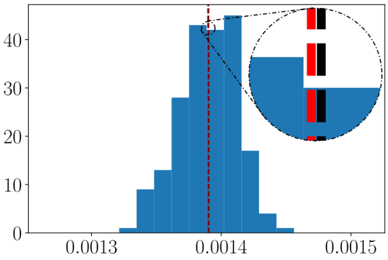


2

2. A. Garay, F. Bernard, V. Fischer, P. Haddad and U. Mureddu. An evaluation procedure for comparing clock jitter measurement methods. CARDIS 2023

Simulation results for the Short Accumulation Time Method

- Experiment :
  - Pick two random periods : T_0 and T_1 (close two each other according to the differential principle).
  - Pick a random jitter (between 0.5‰ and 1.5‰).
  - Repeat 100 times the jitter meaurement based on the Short Accumulation Time Method with previous constraints.
- Results ($T_0 = 7462$ps, $T_1 = 7940$ps, $\frac{\sigma_1}{T_1} = 1.39$‰)



- black dashed line : average measured value equal to 1.387‰,
- red dashed line : injected jitter $\frac{\sigma_1}{T_1} = 1.39$‰,
- average error is 0.04% and the maximum error is 4.97% $<$ 12.3%.

More simulation results

k_A	k_B	F_{k_A}	F_{k_B}	$M_{(k_A,N)}$	$M_{(k_B,N)}$	c_L/L	$\widetilde{a}_{th}/T_1$	$\alpha_{0,1}$	α_{AB}	δ_W	$\left\|1-\frac{\widetilde{a}_{th}}{a_{th}}\right\|$
86	**70**	**81**	**65**	**3 993**	**599**	**0.93977**	**1.390‰**	**1.08%**	**0.94%**	**2.25%**	**0.14%**
169	170	159	159	3 868	136	0.93977	1.391‰	-0.04%	-0.11%	0.15%	0.07%
252	253	237	237	3 814	322	0.93977	1.348‰	-0.04%	-3.19%	3.24%	3.15%
53	253	50	237	3 589	322	0.93977	1.510‰	-12.37%	-2.46%	33.03%	8.46%
252	70	237	65	3 814	599	0.93977	1.235‰	10.47%	-0.62%	21.14%	11.27%

- For each case more precise values (than the upper bound) of the errors can be computed
- Two unsuitable couples such that $|k_A - k_B| > 16$ are presented (in grey) to show that $\delta_W > 12.3\%$
- For the three suitable couples, their stringent upper bound are far below the worst-case (very conservative) upper bound of 12.3%
- Even if this not the couple that gives the lowest error, the best couple is highlighted in bold for its shortest accumulation time (compatible with the thermal noise dominance assumption)

Outline

1. Short Accumulation Time Method
2. Precision of the method, Error Analysis and Conservative Approach
3. From Simulation to reality : Hardware implementation and results (and future work)

Validation of stability assumptions

- Measurement time :
  $t_m = T_0 \left(N \left(k_{max} \frac{k_{max}+1}{2} + l_c\right) + L + l_c\right) \approx 3\ s$
- φ_0 and $\frac{T_0}{T_1}$ are assumed to be stable during the measurement time
- Stabilization of the board temperature :
  we let the oscillators run freely for 10 minutes before the measurements
- φ_0, T_0 and T_1 were measured using a LeCroy WaveRunner 9254M oscilloscope at a 40 GS/s sampling rate for a period of 10s (3 times greater than the method measurement time).

Results

- φ_0 : mean 0.6 ns and standard deviation of 1.9 ps
- T_0 : mean 7.32 ns and standard deviation 4.4 ps
- T_1 : mean 7.9 ns and standard deviation 4.8 ps

Hardware results in FPGA and comparison with the S-o-A

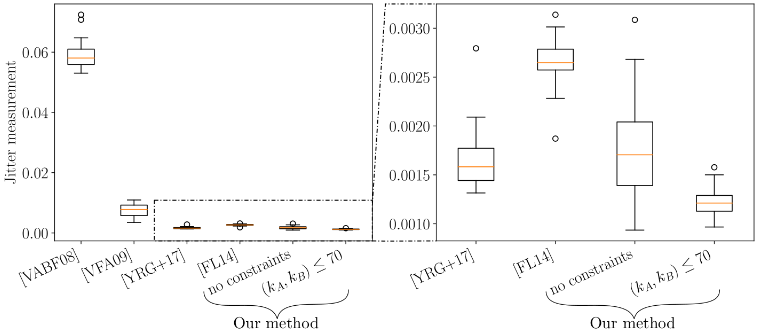
Ring oscillators at ≈125MHz

Measurement method	Accumulation time	Result	
		$\widetilde{a_{th}}/_T$ [‰]	$\widetilde{a_{th}}$ [ps]
Counter method	≈ 200.000 periods	58.6	468.8
Coherent sampling method	≈ 400 periods	7.47	60.1
Autocorrelation of distant samples	≈ 300 periods	2.61	20.88
Short accumulation time	≈ 60 periods	1.73±0.08	13.8±0.7
Delay chains	≈ 43 periods	1.63	13.04

- Shorter accumulation times, smaller clock jitter measured
- Error analysis of the measurement

LABORATOIRE Hubert CURIEN UMR • CNRS • 5516 • ST-ETIENNE

Comparison with the S-o-A methods in FPGA



3

- [VABF08] : Counter (long accumulation time).
- [VFA09] : Coherent sampling.
- [YRG+17] : Delay Chain.
- [FL14] : Autocorrelation of distant samples.

3. Cyclone V, RO$\sim$112MHz (20 LCELL+NAND, manual P& R)

Hardware results in ASIC and comparison with the S-o-A

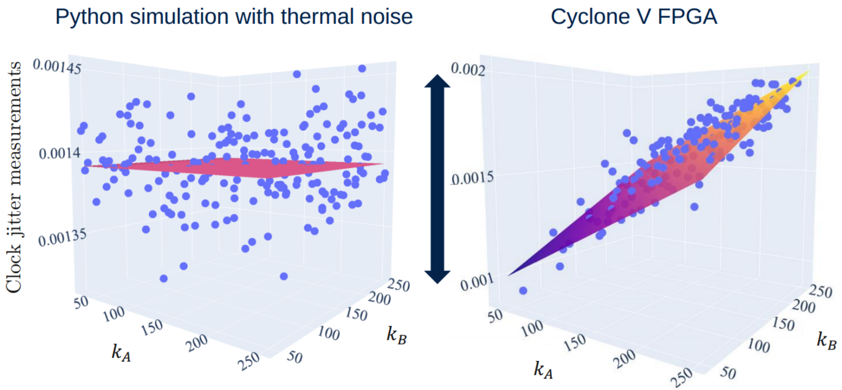
Ring oscillators at ≈39MHz

Measurement method	Accumulation time	Result	
		$\widetilde{a_{th}}/_T$ [‰]	$\widetilde{a_{th}}$ [ps]
Autocorrelation of distant samples	$\approx$ 300 periods	6.75	173.07
Coherent sampling method	$\approx$ 42 periods	0.84	21.5
Short accumulation time	$\approx$ 10 periods	0.41±0.05	10.5±1.3

- Shorter accumulation times, smaller clock jitter measured
- Error analysis of the measurement

Impact of the (even short) accumulation time on the measurement

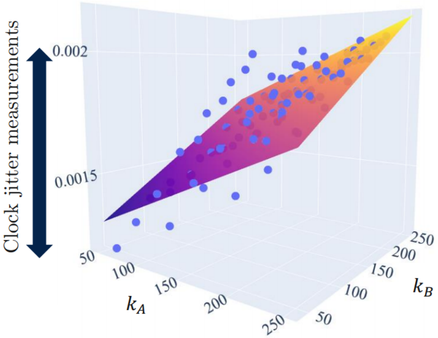
- Bad news. . .



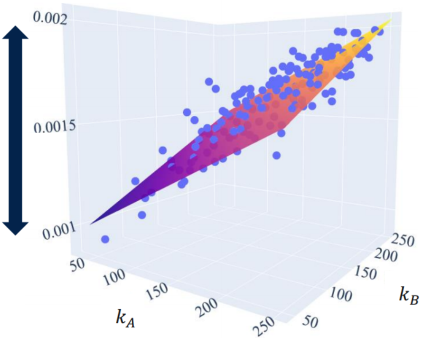
A new hope ?

- Injecting flicker noise in the simulation (allan tools) [4]

Python simulation with thermal and flicker noise

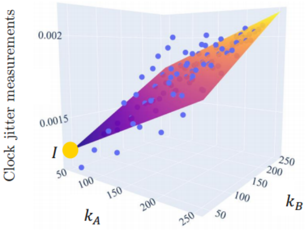


Cyclone V FPGA



4. Kasdin, N. J., & Walter, T. (1992). Discrete simulation of power law noise. In Proceedings of the Annual Frequency Control Symposium (pp. 274-283). Publ by IEEE.

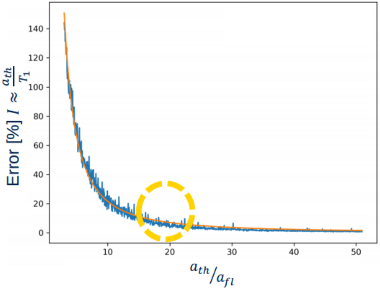
Future Work (1)



I is a good approximation of a_{th}.

if $a_{fl} \ll a_{th}$

But how much ?



$$20a_{fl} < a_{th}$$

!

a_{fl} and a_{th} are technology dependent coefficients

- To be investigated…

Future Work (2) : Application of the method to the PLL-TRNG

PLL-based TRNG (Work in Progress)

- Naturally filter the flicker noise
- The ratio $\frac{T_0}{T_1}$ is known ($\frac{K_M}{K_D}$) and very stable (reducing the error $\alpha_{0,1}$) and improving the precision of this measurement method.
- The ratio $\frac{K_M}{K_D}$ can be used (or better, chosen !) to have specific convergents in the continued fraction decomposition of $\frac{K_M}{K_D}$.
  - candidates (k_A, k_B) are very stable
  - candidates (k_A, k_B) can be predicted when the first case is identified (saving a lot of measurement time in comparison to the sweeping of k)

Future Work (2) : First results (to be confirmed/strengthened)

- Ornstein-Uhlenbeck process used to describe the bounded accumulated jitter inside a PLL (J. Mittmann (BSI), A. Christin/Q. Dallison (Thales)) :

$$\frac{\sigma_1}{T_1} \approx \frac{(k_A - k_B)\frac{T_0}{T_1} - (F_{k_A} - F_{k_B} - 1)}{\Phi^{-1}\left(\frac{M_{k_A}}{N}\right)\sqrt{F_{k_A}} - \Phi^{-1}\left(\frac{M_{k_B}}{N}\right)\sqrt{F_{k_B} + 1}}$$

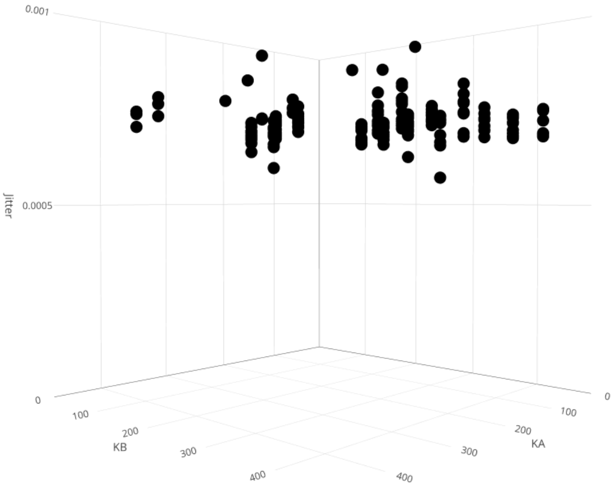
Future Work (2) : First results (to be confirmed/strengthened)

- Ornstein-Uhlenbeck process used to describe the bounded accumulated jitter inside a PLL (J. Mittmann (BSI), A. Christin/Q. Dallison (Thales)) :

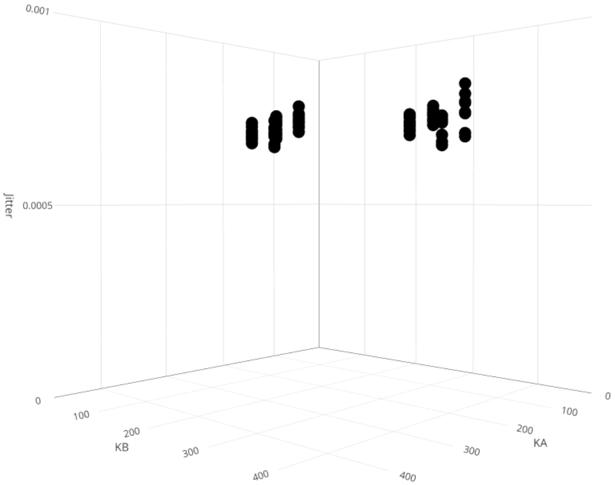
$$\frac{\sigma_1}{T_1} \approx \frac{(k_A - k_B)\frac{K_M}{K_D} - (F_{k_A} - F_{k_B} - 1)}{\Phi^{-1}\left(\frac{M_{k_A}}{N}\right)\sqrt{\frac{\beta}{2}\left(1 - e^{-\frac{2F_{k_A}}{\beta}}\right)} - \Phi^{-1}\left(\frac{M_{k_B}}{N}\right)\sqrt{\frac{\beta}{2}\left(1 - e^{-\frac{2(F_{k_B}+1)}{\beta}}\right)}}$$

- Non trivial convergents for $\frac{K_M}{K_D} = \frac{464}{475}$: $\frac{42}{43}, \frac{211}{216}$
  Candidates :
  $k \in \{42, 129, \underbrace{172}_{129+43}, \underbrace{215}_{172+43}, \underbrace{258}_{\substack{215+43\\=42+216}}, \underbrace{345}_{129+216}, \underbrace{388}_{345+43}, \underbrace{431}_{388+43}\}$

Future Work (2) Jitter estimation in the PLL (unfiltered)



Future Work (2) Jitter estimation in the PLL (filtered)



Conclusions

+ Proposition of a new measurement method working for short accumulation times (where the thermal noise is supposed to be predominant).
+ Only method with error bounds analysis allowing :
  - to set the methods parameters in order to minimize the error,
  - a conservative approach to feed stochastic models.
+ One of the most precise method for jitter measurement and easy to embed in hardware.
- The flicker noise seems to be influent even for such short accumulation times ($<$ 100 periods)... and must be taken into account in future works, **for all** jitter measurement methods in the state-of-the-art.
+ Seems very promising applied to the PLL-TRNG but need to be deeply studied (jitter transfer, β estimation).

Thank you !

Many thanks to :

- my PhD student (Arturo Garay, STM)
- my colleagues Nathalie Bochard and Viktor Fischer

Thank you !

Many thanks to :

- my PhD student (Arturo Garay, STM)
- my colleagues Nathalie Bochard and Viktor Fischer

Questions ?