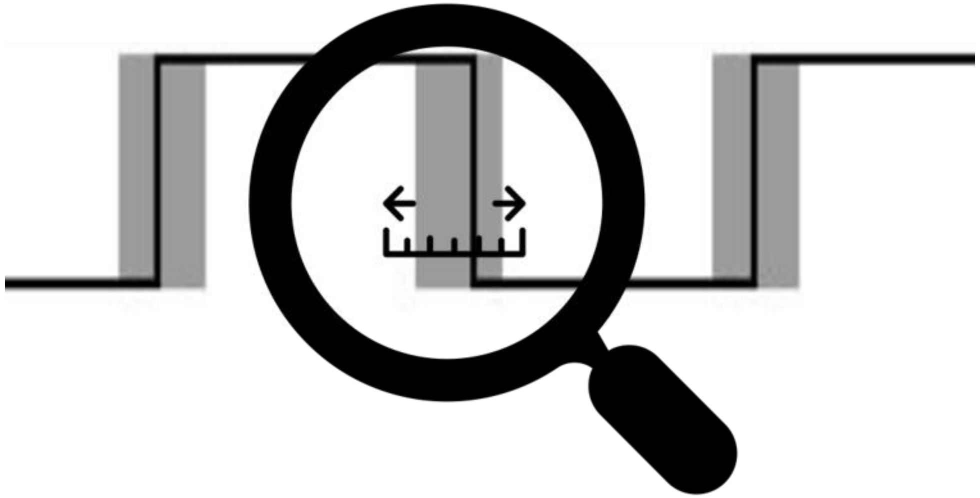
life.augmented

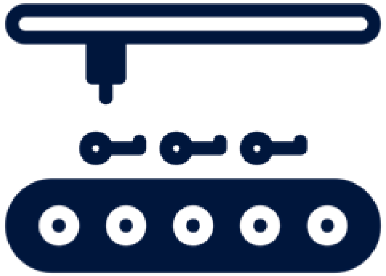


An evaluation procedure for comparing clock jitter measurement methods

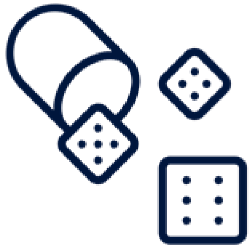
Arturo Mollinedo Garay
Florent Bernard
Viktor Fischer
Patrick Haddad
Ugo Mureddu

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE
UNIVERSITÉ DE LYON
UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

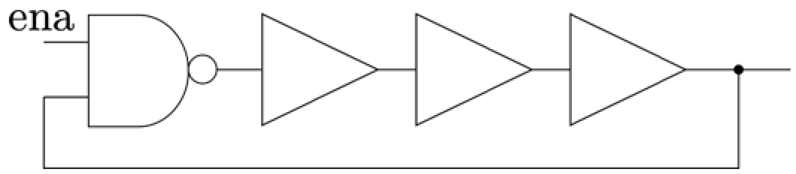
Brief reminder – clock jitter



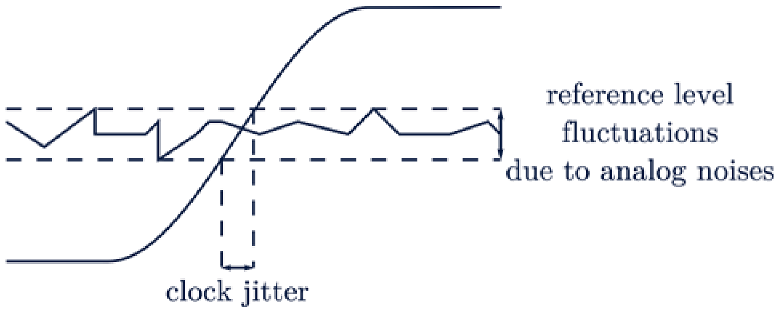
TRNGs are used to generate the inputs of cryptographic systems

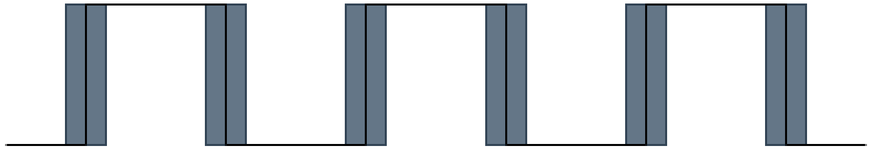


A randomness source is required



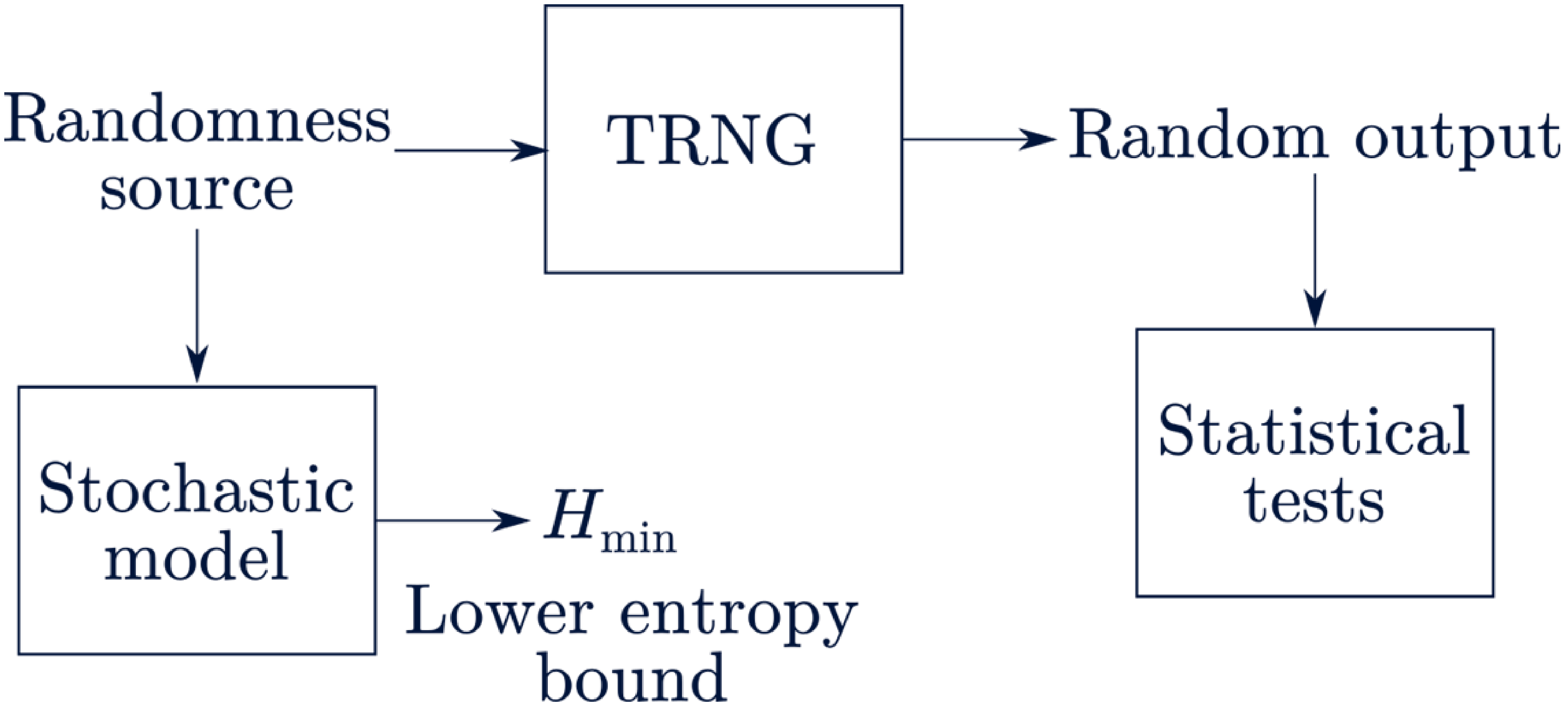
Ring oscillators are easily implementable in digital circuits



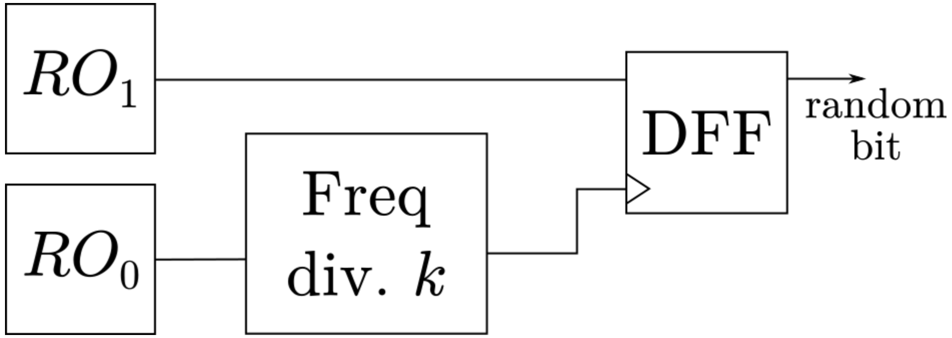


These fluctuations are an inevitable phenomena

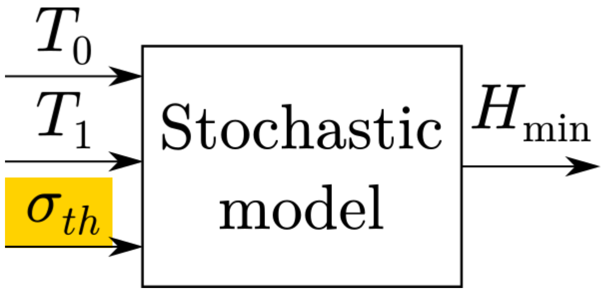
Evaluation of a TRNG



eRO-TRNG



eRO-TRNG



Lower bound entropy

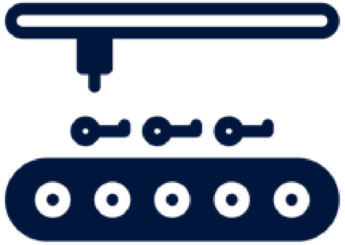
Online and embedded measurement of σ_{th}

Guarantee of the TRNG performance

[1] Baudet, M., D. Lubicz, J. Micolod, and A. Tassiaux. “On the Security of Oscillator-Based Random Number Generators,” 24(2):398–425. Journal of Cryptology, 2011.
.

The final goal

The need for
true random
numbers



eRO-TRNGs use jittery
digital signals

Embedded and continuous
measurements are required for the
entropy source characterization and
for its performance evaluation.

**Thoroughly evaluate
jitter measurement
methods**

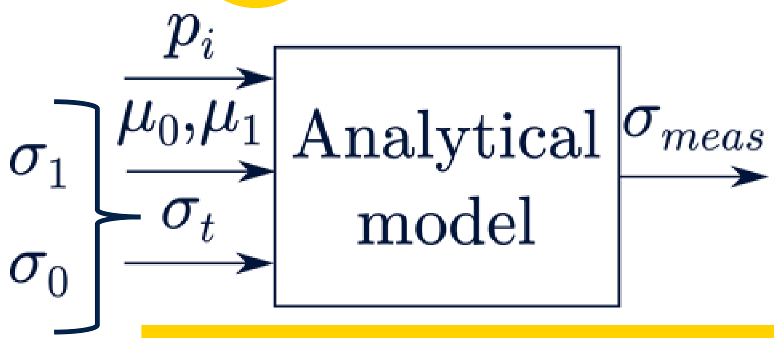
life.augmented

The evaluation procedure

life.augmented

The evaluation procedure

1 Modeling

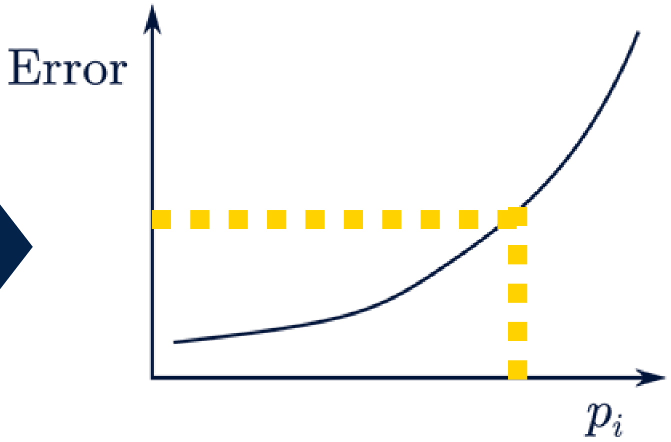


Neglect flicker noise

Clock jitter $\sigma = 1‰\mu$

$T \sim \mathcal{N}(\mu, \sigma^2)$

2 Simulation



$$err_{\%} = \frac{|\sigma_t - \sigma_{meas}|}{\sigma_t} . 100$$

3 Error analysis

Maximal error < 25%.

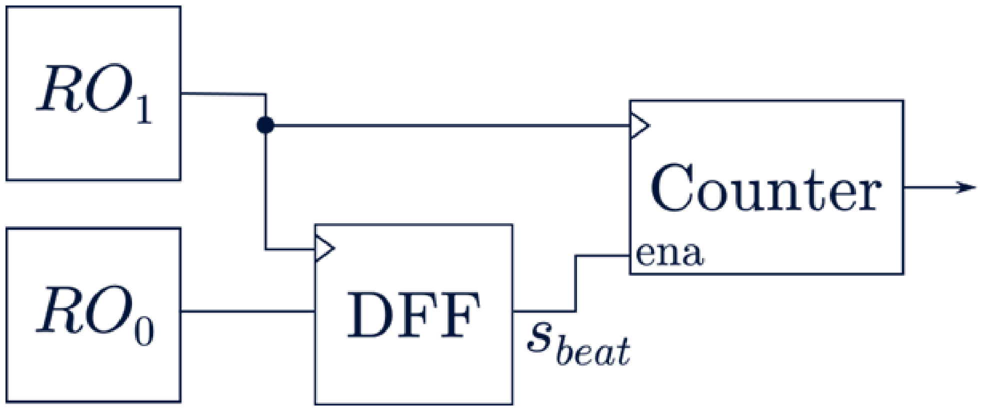
Average error < 10%.

Methods constraints on P_i

4 Hardware experiment

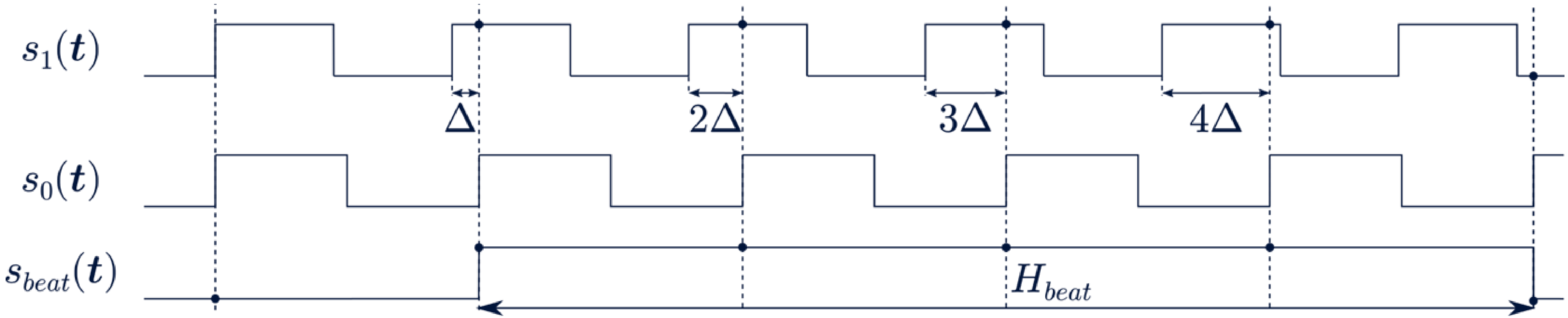
STEP 1 – Analytical model

The coherent sampling method



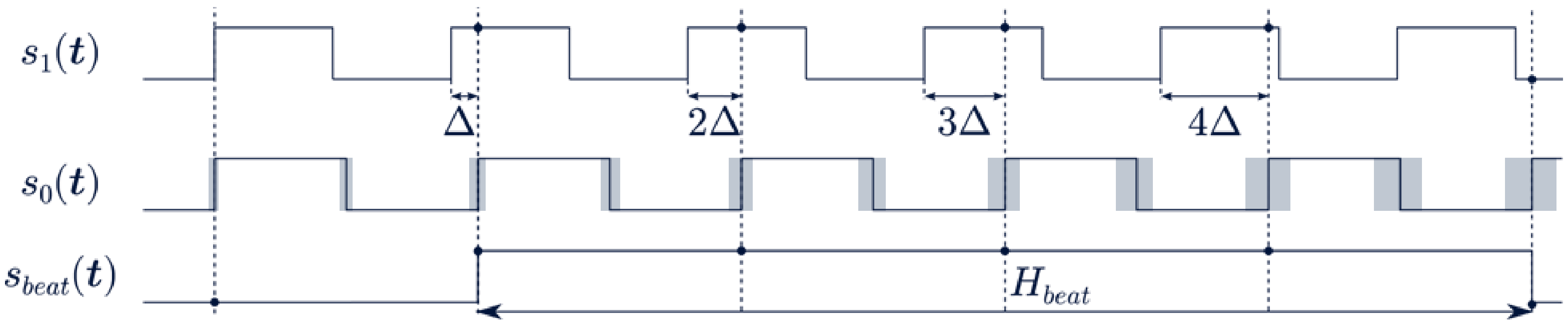
$$\boxed{\Delta := \mu_0 - \mu_1}$$

$$T_0 \sim \mathcal{N}(\mu_1 + \Delta, \sigma_t^2)$$
$$T_1 \sim \mathcal{N}(\mu_1, 0)$$



[2] Valtchanov, B., V. Fischer, and A. Aubert. “A Coherent Sampling Based Method for Estimating the Jitter Used as Entropy Source for True Random Number Generators.” In *International Conference on Sampling Theory and Applications - SAMPTA 2009*, 2009.

On the analytical model



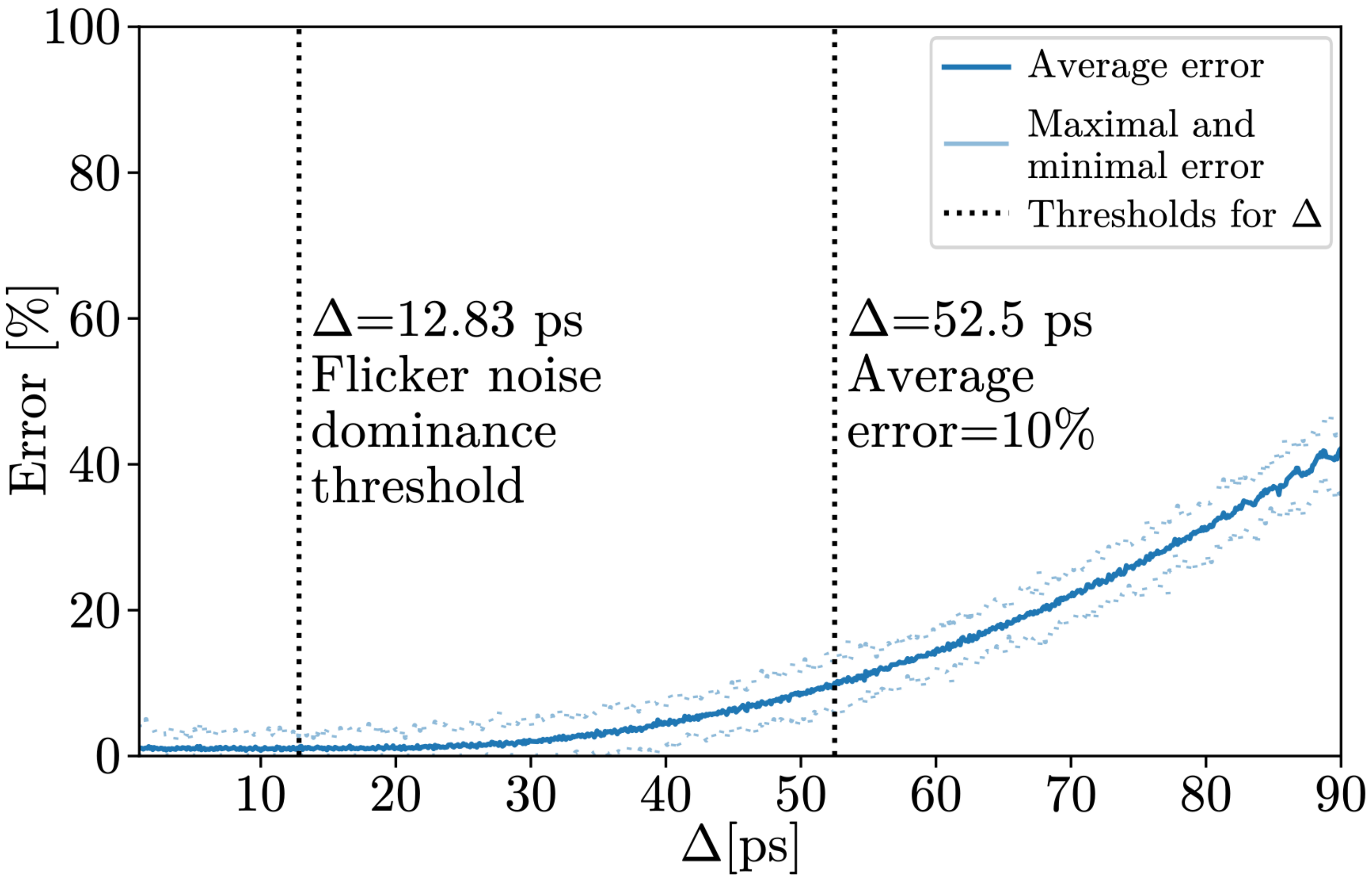
The precision of the method

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

STEP 2 – Simulations

life.augmented

The coherent sampling method



- Analyse $err_{\%} = f_{\sigma_{inp}}(\Delta)$
- Lower limit → flicker noise influence [3]
- Upper limit → acceptance limit on the error.

[3] Haddad, P., Y. Teglia, F. Bernard, and V. Fischer. “On the Assumption of Mutual Independence of Jitter Realizations in P-TRNG Stochastic Models.” In *Design, Automation & Test in Europe Conference & Exhibition - DATE 2014*, 1–6. IEEE, 2014.

life.augmented

STEP 3 – Study the results

The coherent sampling method

The interval can be found for any μ_1

- If Δ:

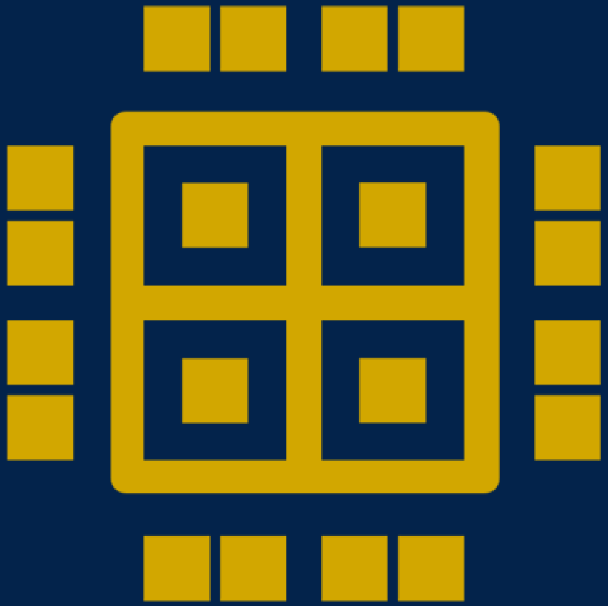
$$\Delta_{i,j} = \frac{|\mu_i - \mu_j|}{\mu_j} \, 100\% \, ; i \neq j$$

$\mu_j \rightarrow$ sampled clock ; $\mu_i \rightarrow$ sampling clock

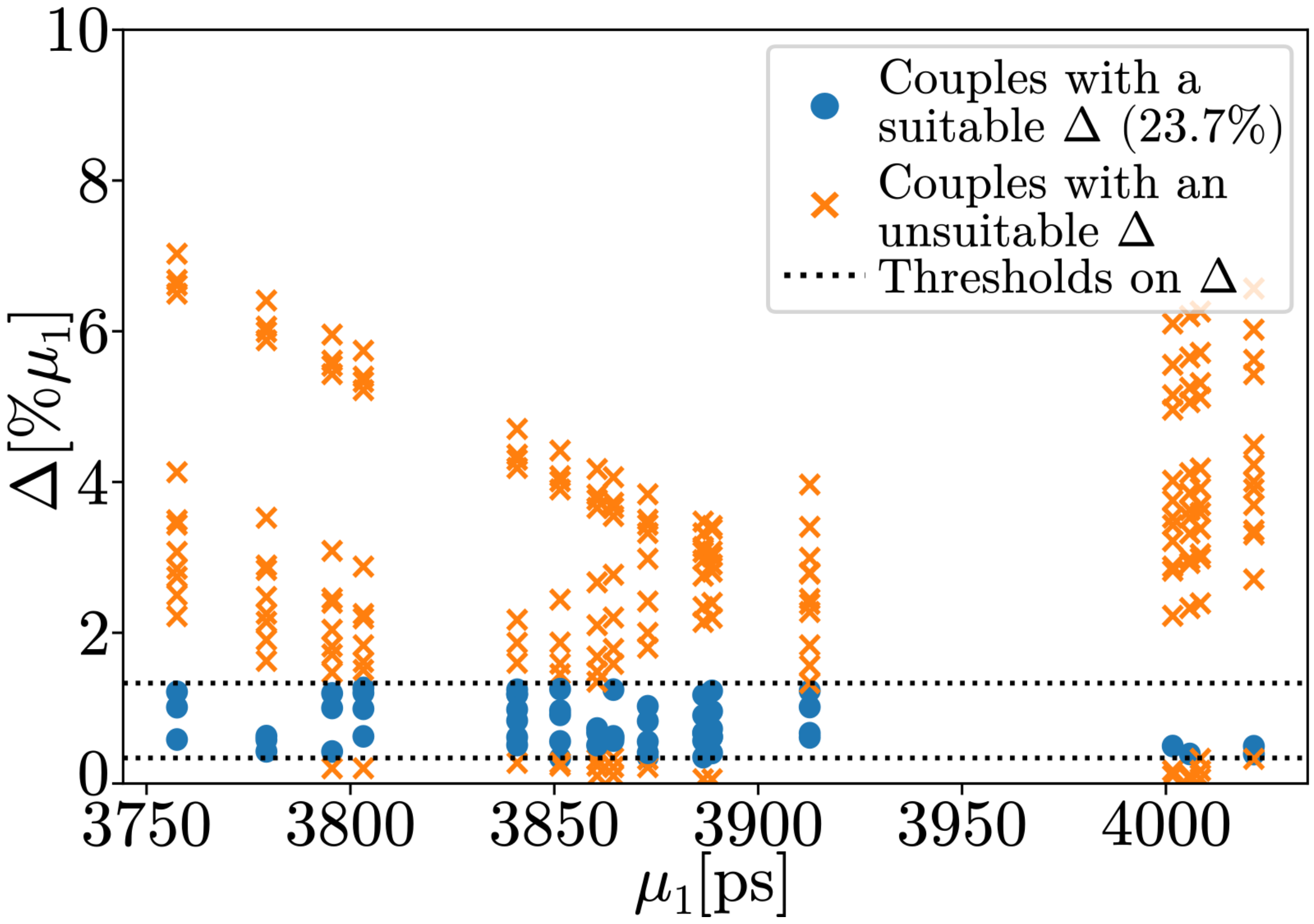
- Then:

$$\boxed{0.3\%\mu_1 < \Delta < 1.4\%\mu_1}$$

STEP 4 – Hardware experiment



The coherent sampling method

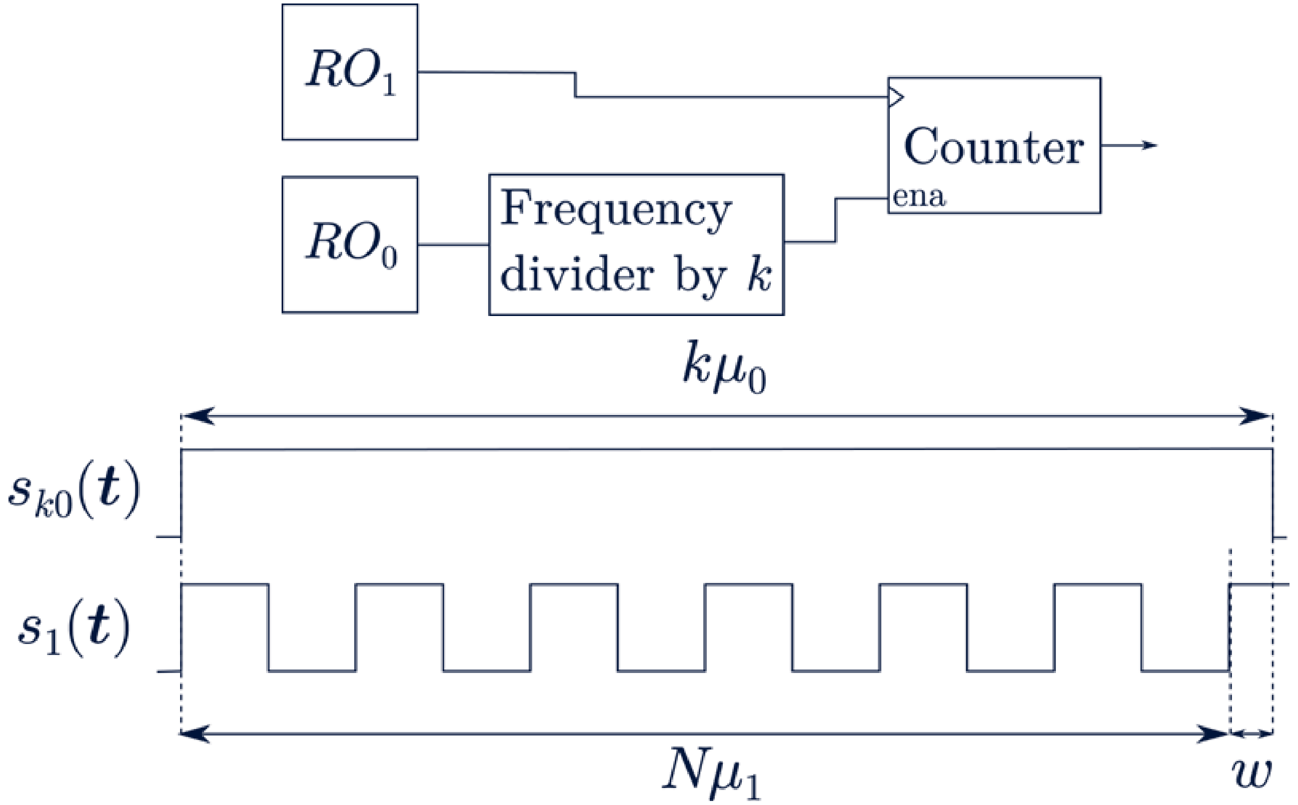


- 16 ROs → 240 pairs of ROs
- 23.7% had a suitable Δ.
- The critical dependence on Δ makes the method difficult to implement in hardware

Application of the procedure

The counter method

The variance of the counter values is used to calculate the jitter after the accumulation time $k\mu_0$ [4]

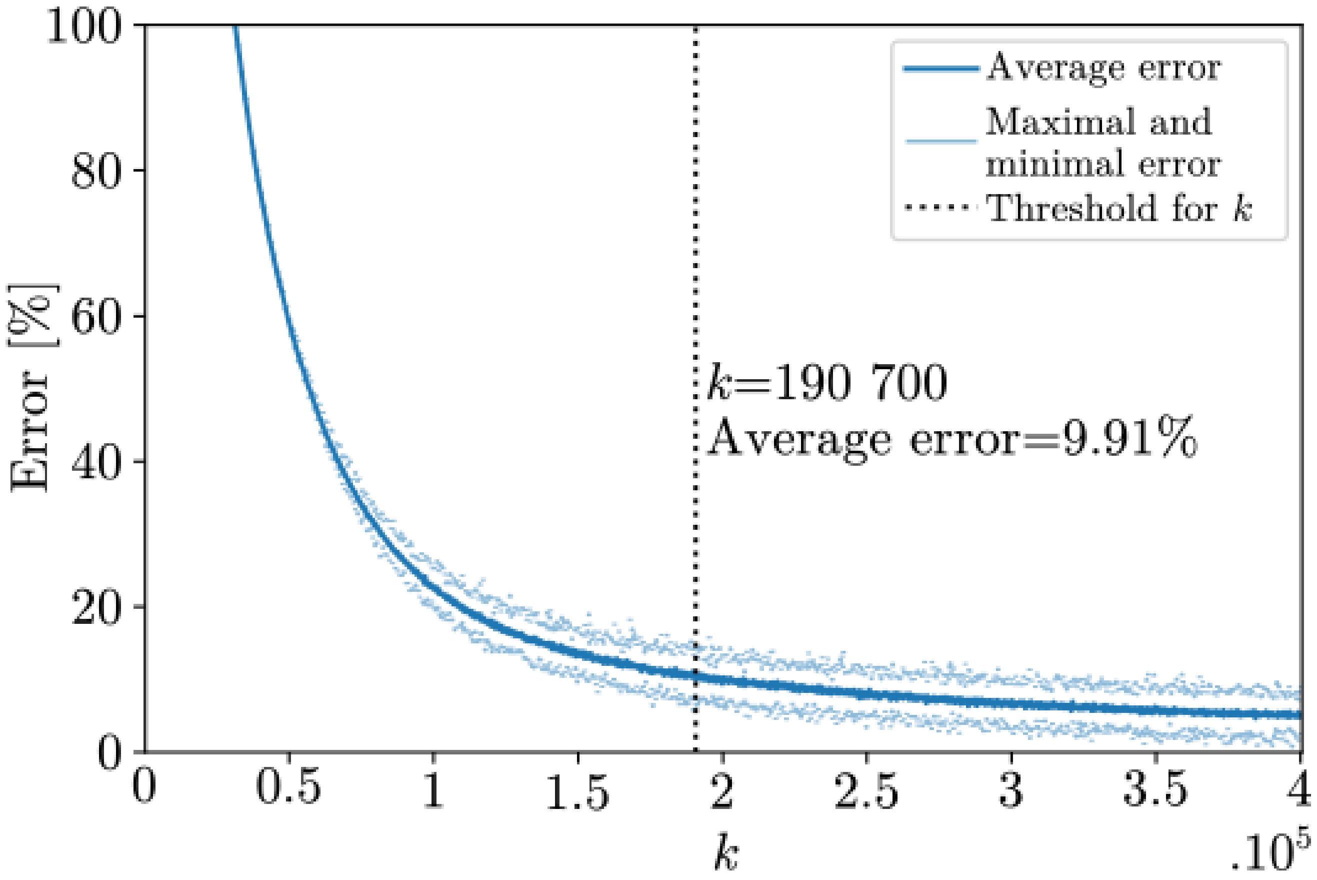


- The precision depends on k
- k chosen by the designer
- No hardware constraint

[4] Valtchanov, B., A. Aubert, F. Bernard, and V. Fischer. “Modeling and Observing the Jitter in Ring Oscillators Implemented in FPGAs.” In Proceedings of the 11th IEEE Workshop on Design & Diagnostics of Electronic Circuits & Systems - DDECS 2008, 158–63, 2008.

life.augmented

The counter method

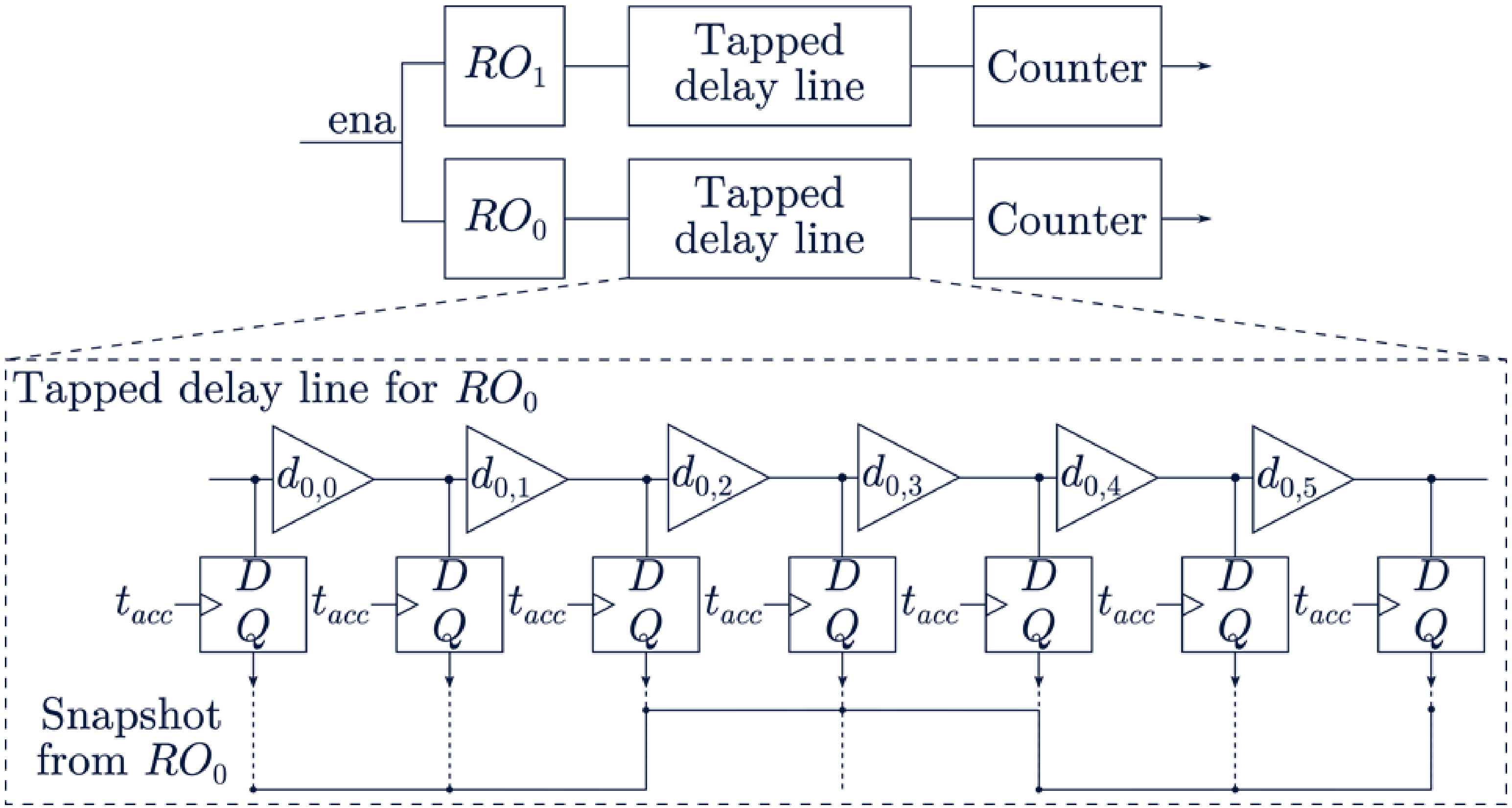


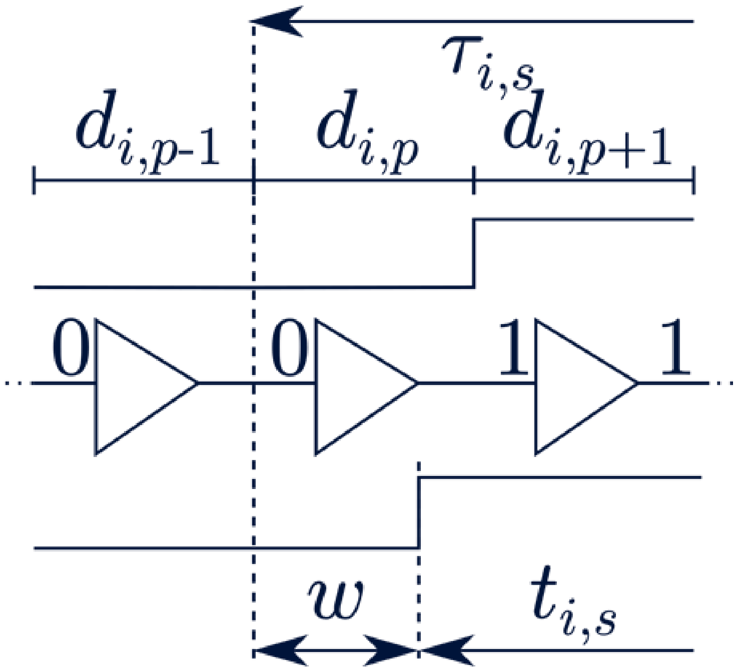
- Acceptable error for $k > 200{,}000$
- Flicker noise is not negligible for $k > 300$ [3]
- The method does not distinguish between the thermal noise and the flicker noise components
- The counter method is not applicable for thermal noise clock jitter measurement.

[3] Haddad, P., Y. Teglia, F. Bernard, and V. Fischer. “On the Assumption of Mutual Independence of Jitter Realizations in P-TRNG Stochastic Models.” In *Design, Automation & Test in Europe Conference & Exhibition - DATE 2014*, 1–6. IEEE, 2014.

The differential delay line method

The time of arrival of two edges coming from two ROs are measured with two delay lines [5]





[5] Yang, B., Rozic, V., M. Grujic, N. Mentens, and I. Verbauwhede. “On-Chip Jitter Measurement for True Random Number Generators.” In Asian Hardware Oriented Security and Trust Symposium - AsianHOST 2017, 91–96, 2017.

The differential delay line method

Simulations

- The delays of the buffers are given by the hardware.
- Variations in manufacturing → not identical delays.

$$d_{i,j} \sim \mathcal{N}(\mu_d, \sigma_d^2)$$

- Results

$$\mu_d < 18ps \; ; \; \sigma_d < 16.5ps$$

Hardware experiment

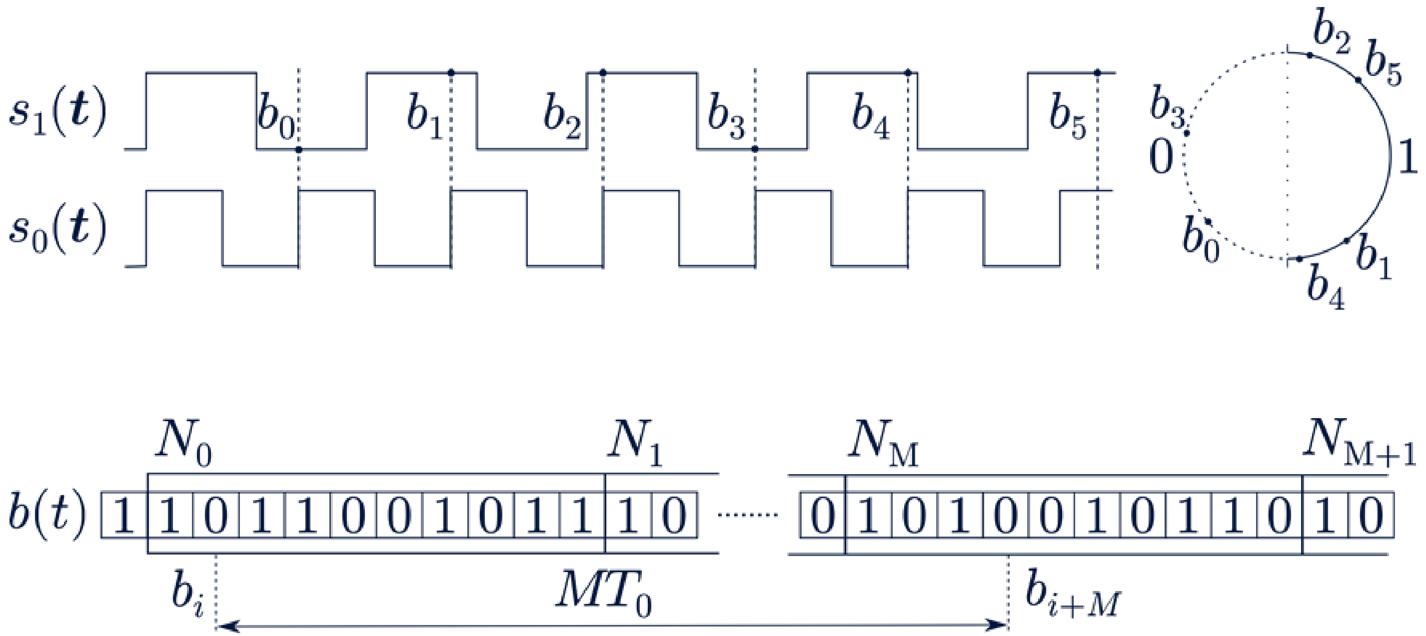
- Results

$$\mu_d = 4.84ps \; ; \; \sigma_d = 4.26ps$$

- At least 1.5 clock periods → 1,000 buffers ; f_0 of 400MHz.
- Delicate trade-off → cannot be met in the FPGA.

Method testing the autocorrelation of distant samples

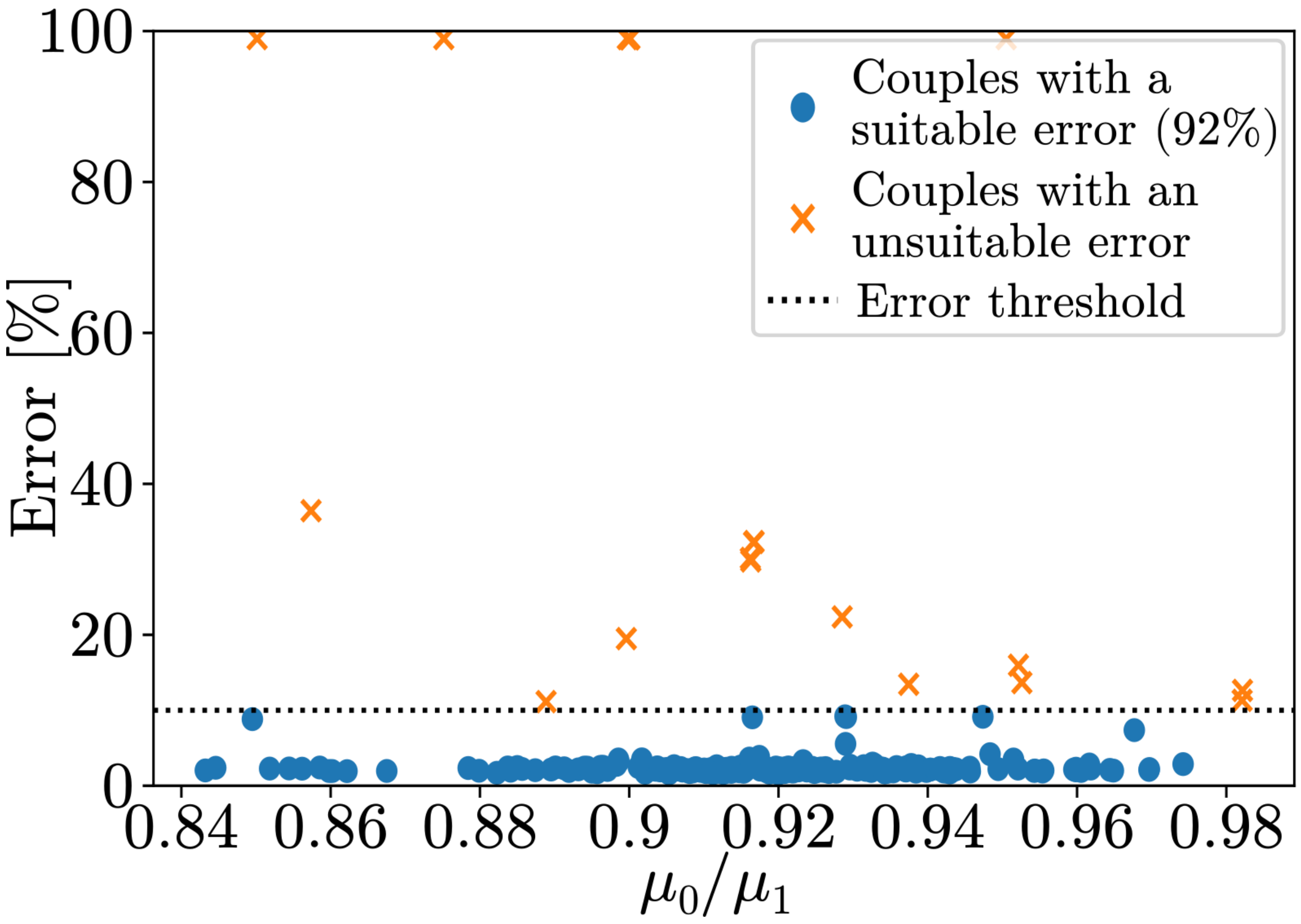
The method is based on the autocorrelation of coherent samples distant in time of a short accumulation time [6]



- Coherent sampling based
- No constraints on Δ.
- ${}^{\mu_0}/_{\mu_1} \not\approx {}^{p}/_{q}$; p, q small integers.
- Another pattern distant in time of $M\mu_0 \rightarrow$ accumulated jitter $M\mu_0$.

[6] Fischer, V., and D. Lubicz. “Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG.” In *Cryptographic Hardware and Embedded Systems - CHES 2014*, edited by Lejla Batina and Matthew Robshaw, 8731:527–43, 2014.

Method testing the autocorrelation of distant samples

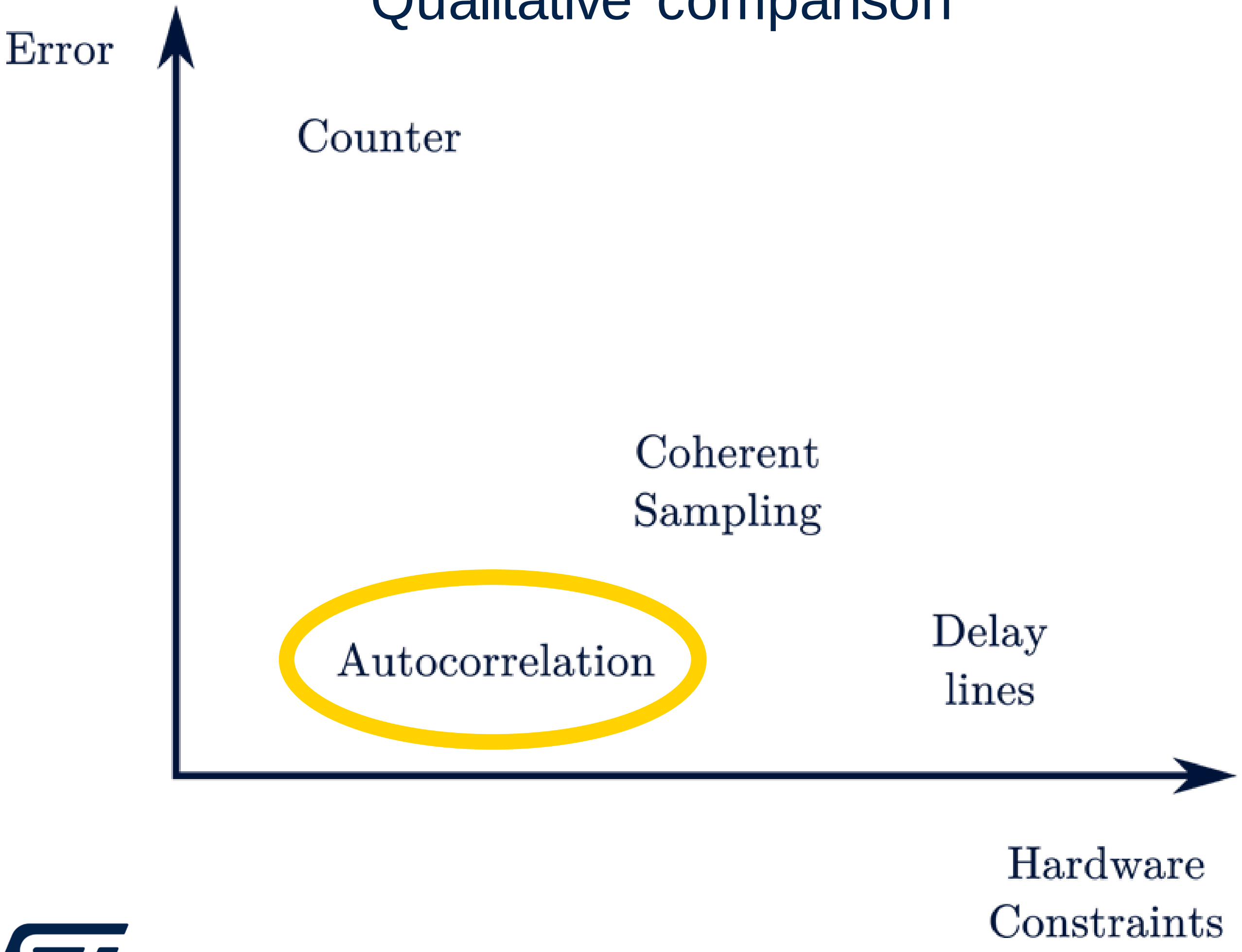


- Group A → 16 ROs, 9 buffers
- Group B → 16 ROs, 10 buffers
- 255 pairs of ROs → sampling from group A ; sampled group B
- 92% resulted in an acceptable error

Results and conclusion

Results summary

Qualitative comparison



- The method testing autocorrelation of distant samples is ahead of the others
- The rest of them should either:
  - Include the influence of flicker noise in their original model
  - Avoid the influence of flicker noise
  - Relax hardware constraints

Conclusion

Successfully identified the limits of each method

The models are simplistic compared to reality → inaccurate simulated measurements, inaccurate measurements in hardware

Accurate simulated measurements DO NOT mean accurate measurements in hardware

Our evaluation procedure is necessary but not sufficient

Our technology starts with You

Find out more at www.st.com

life.augmented

Bibliography

[1] Baudet, M., D. Lubicz, J. Micolod, and A. Tassiaux. “On the Security of Oscillator-Based Random Number Generators,” 24(2):398–425. Journal of Cryptology, 2011

[2] Valtchanov, B., V. Fischer, and A. Aubert. “A Coherent Sampling Based Method for Estimating the Jitter Used as Entropy Source for True Random Number Generators.” In *International Conference on Sampling Theory and Applications - SAMPTA 2009*, 2009.

[3] Haddad, P., Y. Teglia, F. Bernard, and V. Fischer. “On the Assumption of Mutual Independence of Jitter Realizations in P-TRNG Stochastic Models.” In *Design, Automation & Test in Europe Conference & Exhibition - DATE 2014*, 1–6. IEEE, 2014.

[4] Valtchanov, B., A. Aubert, F. Bernard, and V. Fischer. “Modeling and Observing the Jitter in Ring Oscillators Implemented in FPGAs.” In Proceedings of the 11th IEEE Workshop on Design & Diagnostics of Electronic Circuits & Systems - DDECS 2008, 158–63, 2008.

[5] Yang, B., Rozic, V., M. Grujic, N. Mentens, and I. Verbauwhede. “On-Chip Jitter Measurement for True Random Number Generators.” In Asian Hardware Oriented Security and Trust Symposium - AsianHOST 2017, 91–96, 2017.

[6] Fischer, V., and D. Lubicz. “Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG.” In *Cryptographic Hardware and Embedded Systems - CHES 2014*, edited by Lejla Batina and Matthew Robshaw, 8731:527–43, 2014.