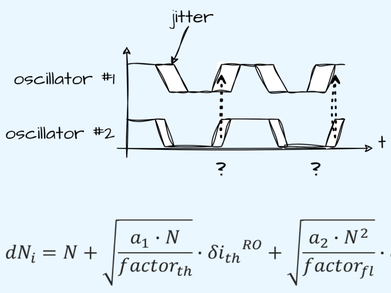
# OpenTRNG: an open-source initiative for ring-oscillator based TRNGs

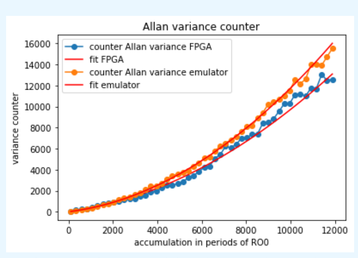
This project offers a comprehensive toolkit facilitating the development and evaluation of hardware TRNG. Key components include: emulators, hardware implementation and validation tools. [DTTIS24]

Follow us @CEA-Leti

## Phase noise emulator




$$dN_i = N + \sqrt{\frac{a_1 \cdot N}{factor_{th}}} \cdot \delta i_{th}{}^{RO} + \sqrt{\frac{a_2 \cdot N^2}{factor_{fl}}} \cdot \delta i_{fl}{}^{RO}$$

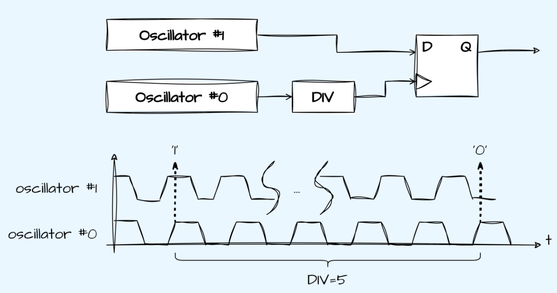



[CHES24] Impact of the Flicker Noise on the Ring Oscillator-based TRNGs, L. Benea, M. Carmona, V. Fischer, F. Pebay, R. Wacquez

- Emulates RO with thermal and flicker noises
- Generates RO time-series at a given RO frequency with thermal and flicker noise figure measured on real hardware

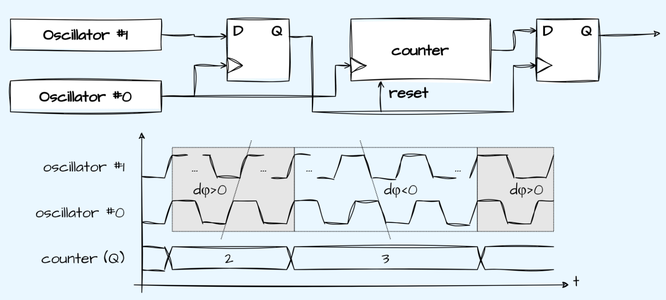
## Raw Random Number emulator

### ERO elementary RO based TRNG




- **Pros**
  - Simple design
  - Available model
  - Low risk of locking
- **Cons**
  - Lack of entropy
  - Need long integration time Low throughput

### COSO Coherent Sampling RO TRNG

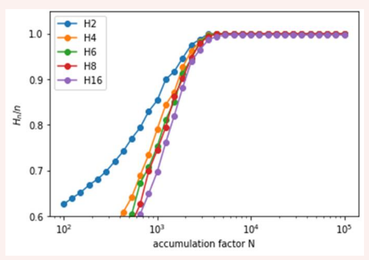



- **Pros**
  - Higher throughput
  - Internal metric for online tests
  - Total failure alarm (by design)
- **Cons**
  - Requires freq. adjustment on both RO
  - And that's it ☺

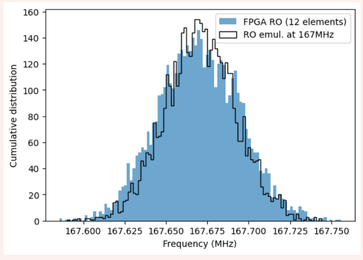
## Validation

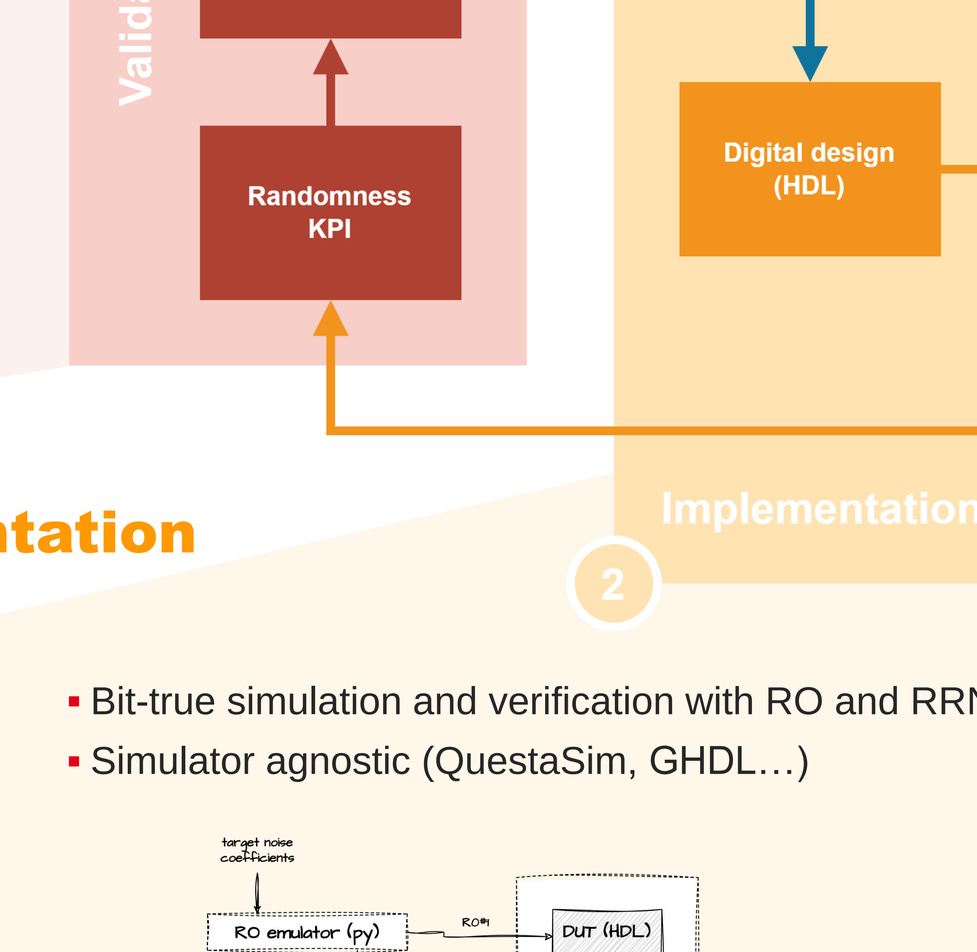
- Randomness KPI: entropy, variance and auto-correlation estimators
- Characterization of noise parameters on hardware target

Entropy estimations for ERO measured data into Xilinx A7 vs accumulation time

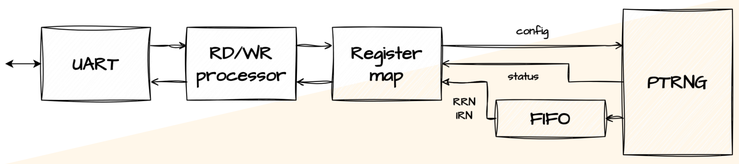



Emulated COSO vs. measured COSO on Xilinx Artix 7 FPGA

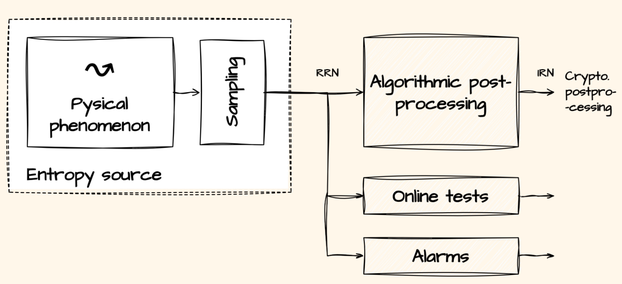


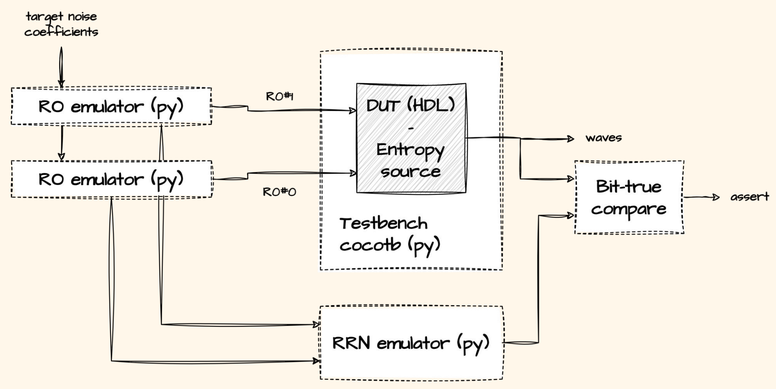

## Simulation and implementation




- Direct access to TRNG from PC
- Python script read/write in register map
- TRNG is pure PTG.2 as in AIS 20/31
- Entropy source (physical and sampling)
- Online test and total failure

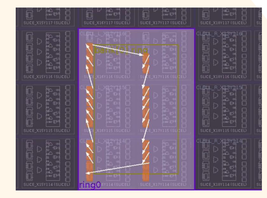


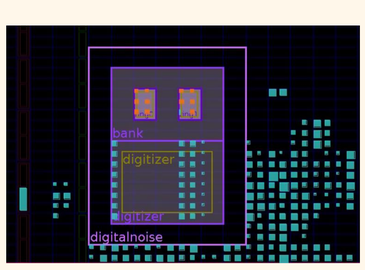

- Bit-true simulation and verification with RO and RRN emulators
- Simulator agnostic (QuestaSim, GHDL…)




- Architecture is portable to other FPGA and ASIC
- Auto-generate place and route constraints for RO
- Scriptable placement for bloc isolation

RO with 20 elements automated place and route in Xilinx A7




RO and sampling blocs physical isolation in Xilinx A7

github.com/opentrng

OpenTRNG


**F. PEBAY-PEYROULA[1], L. BENEA[1], M. CARMONA[1], R. WACQUEZ[2]**

1. Univ. Grenoble Alpes, CEA-Leti, F-38000 Grenoble, France
2. Mines de St-Etienne, CEA-Leti, F-13541 Gardanne, France



[DTTIS24] OpenTRNG: an open-source initiative for ring-oscillator based TRNGs, F. Pebay, L. Benea, M. Carmona, R. Wacquez
[CHES24] Impact of the Flicker Noise on the Ring Oscillator-based TRNGs, L. Benea, M. Carmona, V. Fischer, F. Pebay, R. Wacquez


Research for industrial innovation