TRNG research topic at CEA-leti

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

1.Univ. Grenoble Alpes, CEA, Leti, F-38000 Grenoble, France

Follow us @CEA-Leti

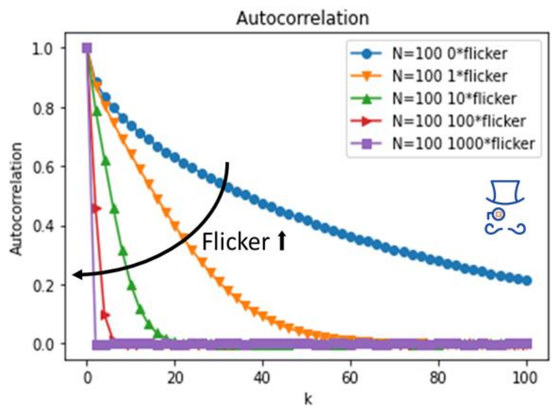
Introduction

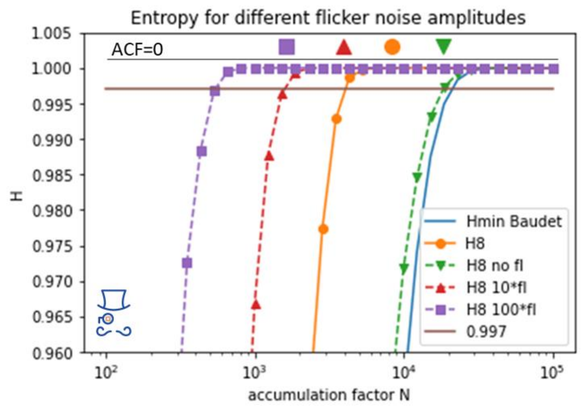
- True Random Number Generators (TRNG) are basic **building blocks** of most cryptographic system
- Issue : determining randomness (entropy) directly from generated numbers can generate **type I or type II errors** (false positives or negatives)
- Methodology : Identification of the physical phenomenon causing entropy → Use of noise models to **generate a stochastic model**
- Used structure : Ring Oscillators (RO) for their **predictable unpredictability** (well-established noise models)

1 1 1 1 1 1
1 0 1 0 1 0
1 1 0 0 1 0
1 0 0 1 0 1

Emulator : simulating sources of entropy

- Entropy in RO-based TRNGs stems from **thermal (random) and flicker (autocorrelated) noises**
- Real behavior of ROs can be emulated using the parameters extracted from Allan variance characteristics
- The effect of both noise sources on TRNG behavior can be determined using the **emulator**[1]
- Particularly, the **autocorrelation** of bits introduced by flicker noise was proven to be **limited**
- Flicker noise may have a positive **effect on entropy** (under certain conditions)
- **Generalizable approach** to other types of noises or structures



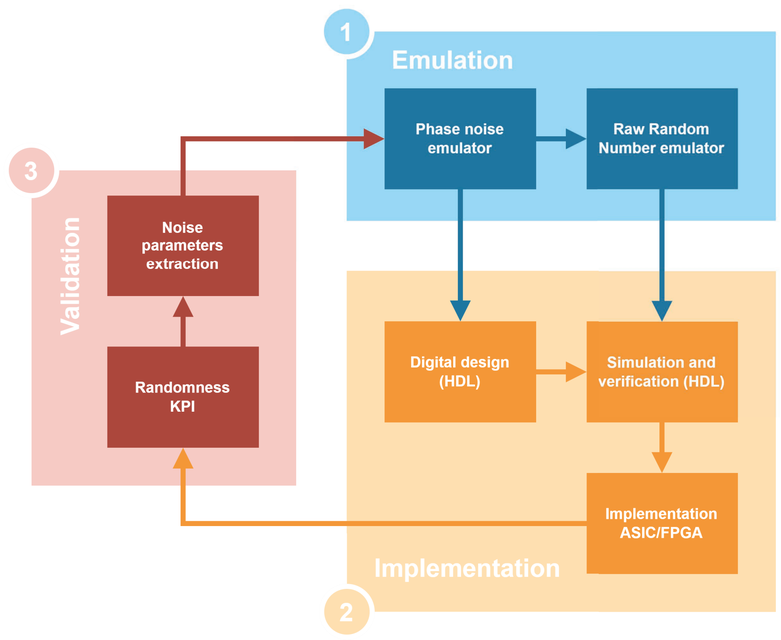


OpenTRNG

- OpenTRNG – a comprehensive **toolkit** facilitating the **development and evaluation** of hardware TRNG
- Key components include:
  - **Hardware implementation**
  - Phases noise and raw random number **emulators**
  - **Validation tools**

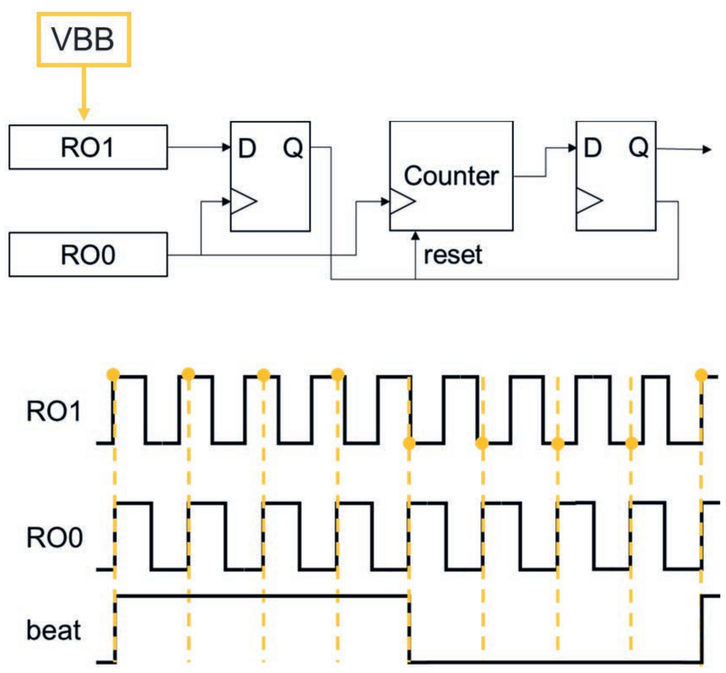
github.com/opentrng

OpenTRNG



COSOI-TRNG

- Coherent Sampling TRNG using **FD-SOI specificities** (back biasing) – in-house CEA-leti designed structure (4 patents)
- Its design offers an the **best throughput per area trade-off**, mutualizing the output and embedded statistical tests
- **Proof of concept** realized on VASCO#2 showed a throughput of 3.36 Mbits/s (result to be optimized in future iterations)



1.L. Benea, M. Carmona, V. Fischer, F. Pebay-Peyroula, and R. Wacquez, 'Impact of the Flicker Noise on the Ring Oscillator-based TRNGs', IACR TCHES, vol. 2024, no. 2, Art. no. 2, Mar. 2024, doi: 10.46586/tches.v2024.i2.870-889.

Research for industrial innovation