An illustration of a new certification approach for True Random Number Generators (TRNG)

Elie Noumon Allini • Florent Bernard • Viktor Fischer

Laboratoire Hubert Curien, UMR 5516 CNRS
Université Jean Monnet, Membre de l'Université de Lyon
Saint-Etienne, France

CryptArchi, Smolenice, June 2017

Importance of Random number generators

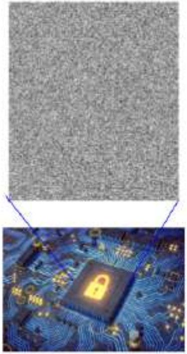
Crucial component of cryptographic systems

- Typical use
  - Key generation,
  - Initialization vector,
  - Counter measures against side channel attacks.
- Security relevance
  - Security of the whole system is based on the secret key
    - ↪ Key must be generated as often as needed,
    - ↪ Unpredictable and non reproducible way;
  - Need of *good* random numbers.

Certification

Can you prove it?

Our device produces very good randomness



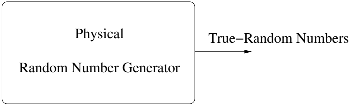
Bundesamt für Sicherheit in der Informationstechnik

Governmental organization

Is the TRNG embedded in your cryptographic device safe enough to ensure a high security level?

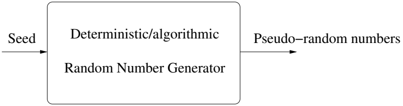
Types of Random Number Generation (RNG): 2 classes

Physical Random Number Generator (PRNG)



- Exploits noisy analog phenomenon: thermal noise, flicker noise, . . .
- May produce random numbers looking not really random.
- Design challenging.

Deterministic Random Number Generator (DRNG)

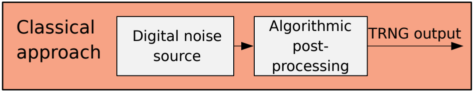


- Take a Seed as input.
- Algorithmic process is known.
- Security based on the Seed
- "Looks like" random numbers.

Question

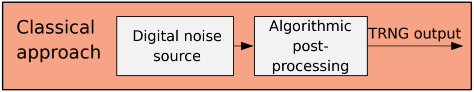
How to evaluate properly the quality of a Random Number Generator?

A first approach for TRNG evaluation:
Observation

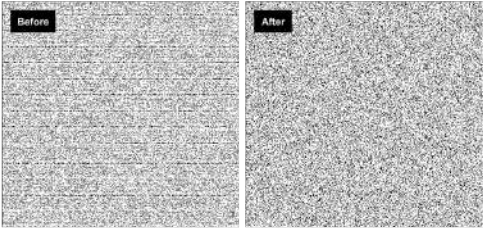


- Battery of statistical tests (FIPS, NIST, DieHard) at the TRNG output.
- Problem 1 : even a full deterministic sequence can pass these tests $\Rightarrow$ tests are necessary but not sufficient.

A first approach for TRNG evaluation:
Observation

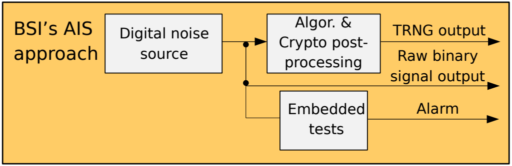


- Battery of statistical tests (FIPS, NIST, DieHard) at the TRNG output.
- Problem 2 :



- Need to perform tests **before** post-processing.

A second approach for TRNG evaluation: proof/certification



Same as the classical approach plus:

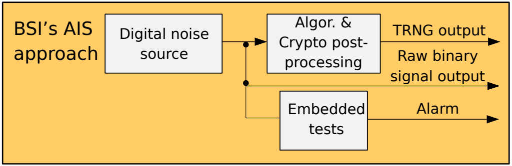
- Test the raw binary signal and estimate the entropy (min entropy) per generated bit
- Provide embedded tests to detect a total failure of the noise source.

Problem : Entropy is not a property of the generated sequence but of the underlying random variables.

Stochastic model

$\Rightarrow$ Need a stochastic model to compute a lower bound (H_{min}) of the entropy per bit as close as possible to the source of entropy.

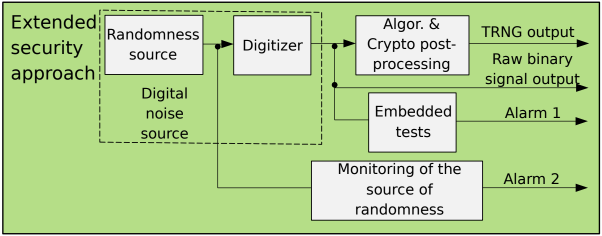
Stochastic Model



- Problems:
  - Model $\neq$ Reality
  - Need reasonable assumptions to work on random variables.
    - $\hookrightarrow$ Is the noise composed only of thermal noise[1] as it is almost always assumed in the TRNG state of the art?
  - There is no generic Model: each TRNG principle must be described with a dedicated stochastic model.

[1] Thermal noise is considered to be unavoidable and non manipulable

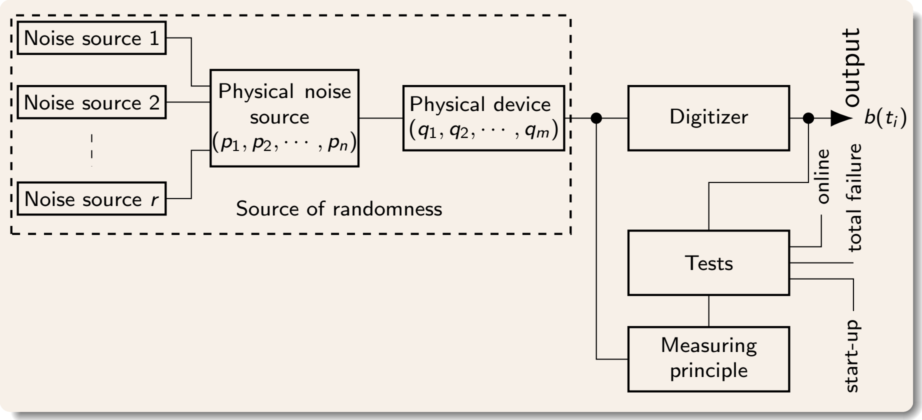
3rd approach: Even closer to the entropy source



- Identify and Model each noise source.
- Design digitization process (entropy extractor) to extract maximum entropy.
- Provide a mathematical proof to compute a lower bound of entropy rate.
- Develop **specific** tests of the source of randomness to avoid a total failure of the entropy source and to monitor it "online".
- Work in progress: Workgroup "alea" with DGA-MI, ANSSI, Institut Fourier, LaHC-SESAM

1. Evaluation process
2. Conclusion

General overview of a hardware-based TRNG



Random number generator

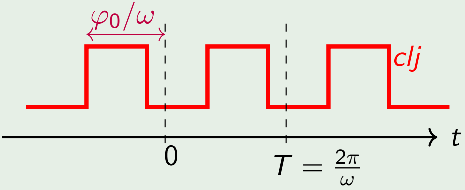
Internal state in the diagram

Formal definition

- Physical device
  - internal state $E : \begin{array}{ccc} \mathbb{R}_+ & \longrightarrow & V \\ t & \longmapsto & E(t) \end{array}$
  - produces a sequence of bits $(b_{t_i})_{1 \leqslant i \leqslant n}$ in some given time.
- Value of b_{t_i} knowing E is determined.

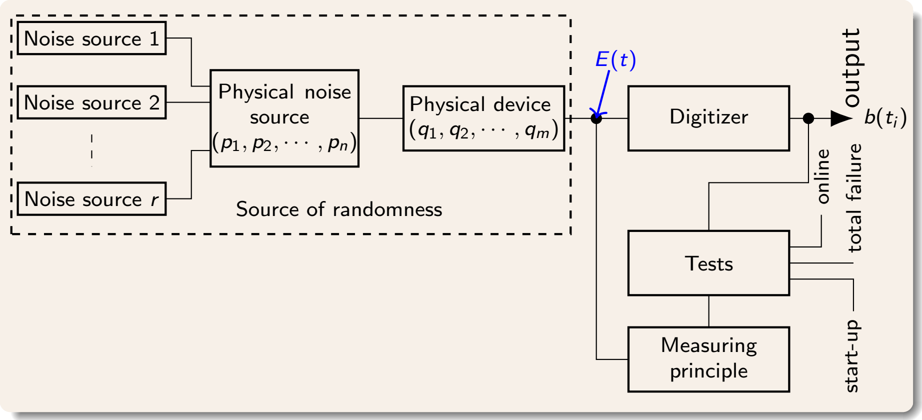
Example

- $clj : t \longmapsto P(\omega t + \varphi_0)$
  - P is 2π-periodic
- $V = [0, 2\pi[$
- $E : t \longmapsto \omega t + \varphi_0 \mod 2\pi$

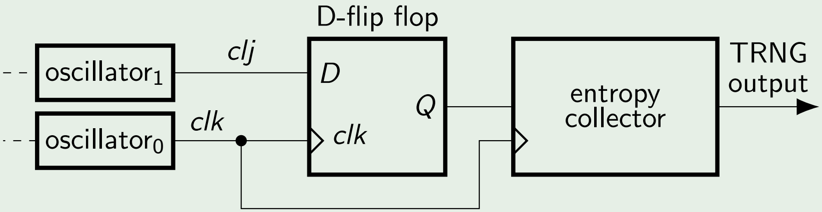


Random number generator

Internal state in the diagram



General principle of an oscillator based TRNG



♣ *clk*

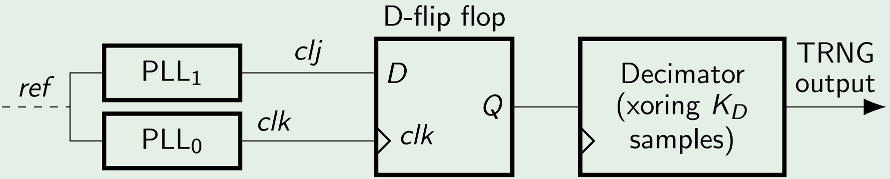
- reference signal,
- *constant period* T_{clk}.

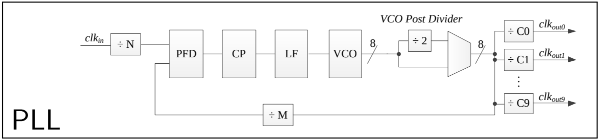
♣ *clj*

- jittery signal;
- random variable
  ↪ mean value T_{clj}.

General principle of an oscillator based TRNG

PLL-based TRNG

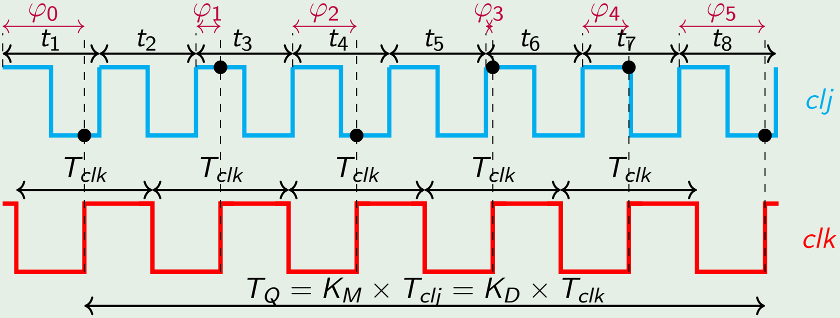




$$
\begin{cases}
K_M = M \\
K_D = N \times C_0 \\
\dfrac{F_{clk_{in}}}{F_{clk_{out0}}} = \dfrac{K_M}{K_D}
\end{cases}
$$

- Control of the phase difference between input and output signal of the PLL $\Rightarrow$ Control of the drift that remains bounded.

Sampling example

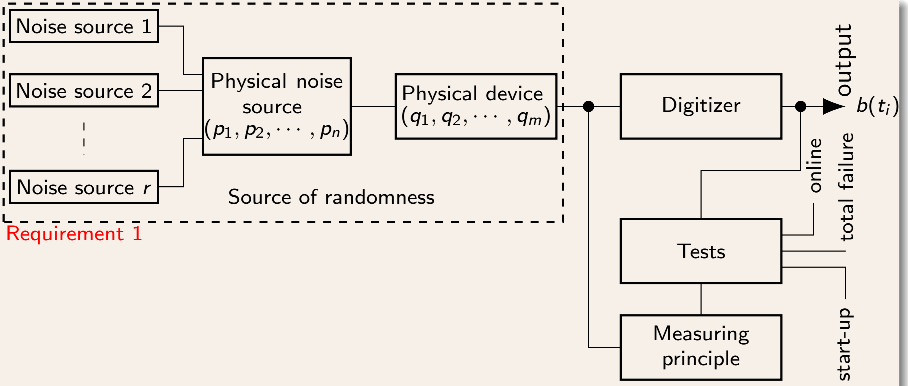


- t_i : realizations of T_j;
- φ_i : phase of clj at time iT_{clk},
  - ↪ $E(iT_{clk})$
  - ↪ $iT_{clk} + \varphi_0 \mod T_{clj}$
- K_M : number of cycles of clj;
- K_D : number of samples,
  - ↪ number of cycles of clk.

Identification of the noise source

Requirement 1

The physical phenomenon at the origin of the unpredictable character of the generator operation must be well identified.



Identification of the noise source

Requirement 1

The physical phenomenon at the origin of the unpredictable character of the generator operation must be well identified.

Sources of entropy in PLL-TRNG

- Differential jitter (dynamic difference in phases)
  - between clock signals generated in two PLLs connected in parallel.
- Three sources can be recognized:
  - input clock jitter,
  - intrinsic noise of the PLL,
  - supply noise contributing to the PLL output clock jitter.

Input clock jitter

- Input jitter with frequency lower than the PLL bandwidth :
  - passed by the PLL without being modified (not filtered out).
- When frequency corresponds to the PLL bandwidth :
  - the closed loop transfer function of the PLL features a peak,
  - input jitter amplified by the relative size of the peak,
    - ↪ depending on the loop damping factor.
- When frequency is higher than the PLL bandwidth
  - input jitter is attenuated at 20db/decade.

Conclusions

- Jitter of the input clock should be as small as possible
  - limit the PLL output jitter to the PLL intrinsic jitter,
  - use of quartz.
- Input clock frequency should be as high as possible
  - much higher then the PLL bandwidth.

Intrinsic noise of the PLL

- VCO contributes the most to PLL intrinsic noise.
- Main components of the PLL intrinsic noise :
  - Thermal noise
  - Flicker noise
- Flicker noise may be significantly reduced :
  - appropriate selection of multiplication and division factors.

Conclusions

- Output clock frequency should be as high as possible
  - reduce the contribution of the flicker noise.
- PLL bandwidth should be as large as possible
  - reduce the long term jitter at PLL output.

Supply noise contribution

- Analog and digital supply noises contribute to the jitter :
  - any fast (step) variation on the analog supply of the PLL
    - ↪ instantaneous change in VCO frequency,
    - ↪ reflected as jitter at the PLL output clock.
  - any step variations on the digital supply of the PLL
    - ↪ a variation in the delay of the digital circuits,
    - ↪ result in variation of the clock time period,
    - ↪ reflected as time period jitter at the PLL output.
- Time period deviation is independent of the PLL output time period
  - unlike the deviation due to intrinsic device noises.

Conclusions

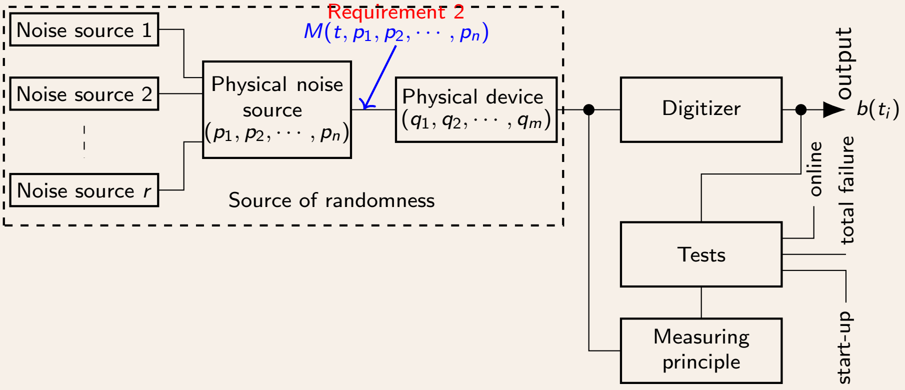
- Analog and digital power supplies should use
  - linear regulators and a high quality filters;
- Digital power supplies powering the PLL
  - must not power also the FPGA core.

Characterization of the noise

Stochastic model

Requirement 2

The physical noise must have a stochastic model $M(t, p_1, p_2, \cdots, p_n)$.



Characterization of the noise

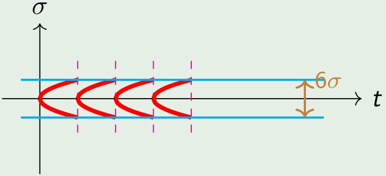
Stochastic model

Requirement 2

The physical noise must have a stochastic model $M(t, p_1, p_2, \cdots, p_n)$.

In the case of a PLL-based TRNG

- ♣ $M(t, \sigma) \equiv \mathcal{N}(0, \sigma)$
  - $\sigma = \sqrt{K_M} \times \sigma_{VCO}$.



Requirement 2bis

The physical noise stochastic model $M(t, p_1, p_2, \cdots, p_n)$ should be used to get a probability distribution of TRNG the internal state $(\varphi(t))$.

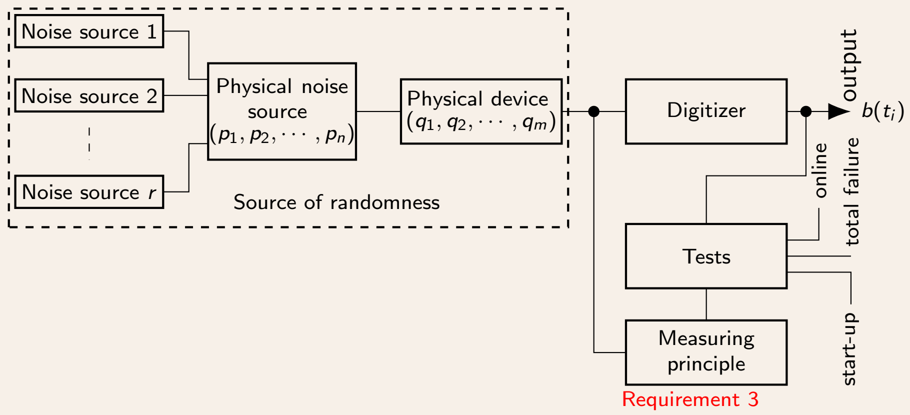
$$\mathbb{P}\big(\varphi(t) | p_1, p_2, \cdots, p_n, \varphi(t_0)\big).$$

Parameters evaluation

Requirement 3

- It should be possible to evaluate the initial state φ_0.
- It should be possible to experimentally evaluate $p_1, p_2, \cdots, p_n$.
- It should be possible to evaluate measurement errors.

Parameters evaluation



Parameters evaluation

Requirement 3

- It should be possible to evaluate the initial state φ_0.
- It should be possible to experimentally evaluate $p_1, p_2, \cdots, p_n$.
- It should be possible to evaluate measurement errors.

Measurement techniques

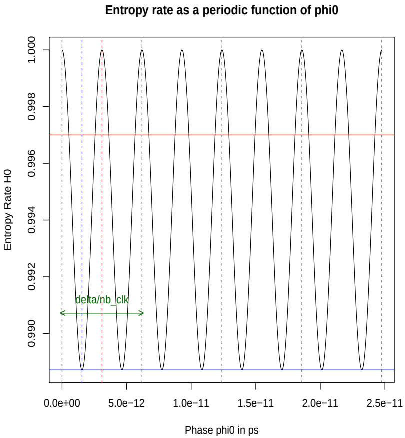
- φ_0 can be quite difficult to evaluate.
- The number of unstable samples is directly related to parameter $p_1 = \sigma$.
- The duty cycle can be approximated by $\frac{\#\{X_i=1\}}{K_D}$.

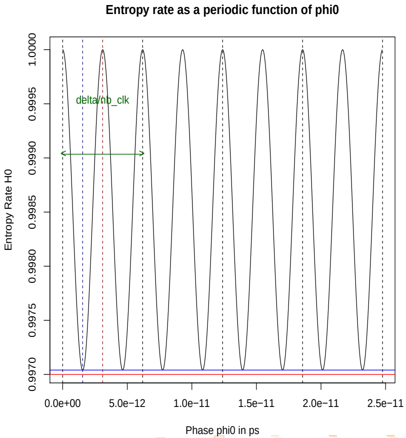
A way to circumvent evaluation of φ_0

A conservative approach

Worst case

Set a higher σ_{min} such that for **any** φ_0 we have $H_{min} \geqslant 0.997$.





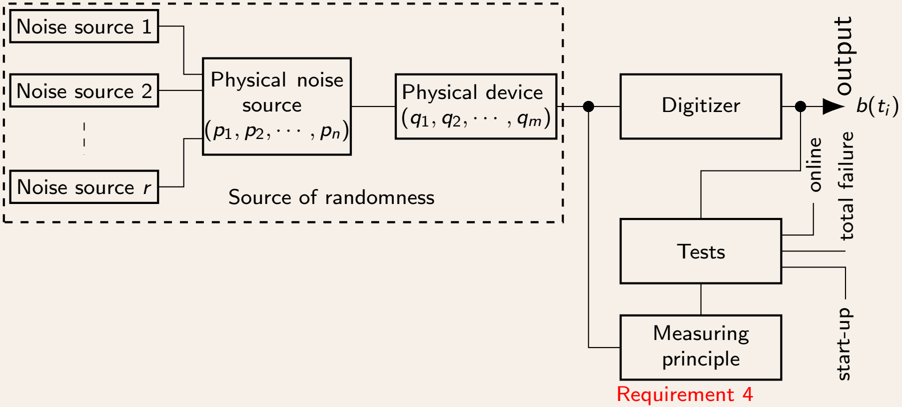
Stability of parameters

Requirement 4

Stability of parameters $p_1, \cdots, p_n$ should be evaluated with regard to :

- physical environmental conditions (temperature, voltage, etc),
- technological environmental conditions,
- aging tests.

Stability of parameters



Stability of parameters

Requirement 4

Stability of parameters $p_1, \cdots, p_n$ should be evaluated with regard to :

- physical environmental conditions (temperature, voltage, etc),
- technological environmental conditions,
- aging tests.

Case of the PLL-based generator

- Jitter (σ) is bounded and duty cycle (α) close to 0.5 at the output,
  - model should tolerate slight unbalances.
- Tests still on progress.

1. Evaluation process
   - Physical noise
   - Analog to digital converter
2. Conclusion

Statistical model of a TRNG

Definition

- Statistical model of the TRNG
  - stochastic model $N(t, p_1, p_2, \cdots, p_n, q_1, q_2, \cdots, q_m)$
    - ↪ $p_1, p_2, \cdots, p_n$ parameters of the physical noise model,
    - ↪ $q_1, q_2, \cdots, q_m$ parameters of the TRNG;
  - values in the set of sequences of bits of arbitrary length.
- About parameters $q_1, q_2, \cdots, q_m$
  - some should be adjustable,
  - none should be manipulable (by an attacker).

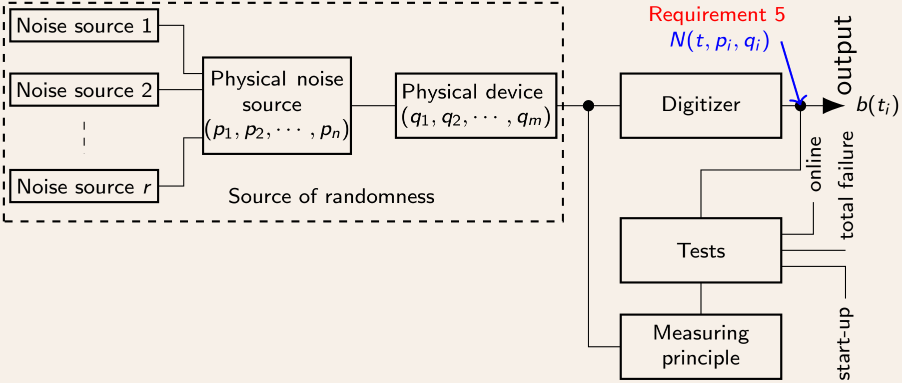
Parameters in the case of a PLL-based TRNG

- Initial internal state : φ_0.
- σ, α.
- K_M, K_D.

Statistical model of a TRNG

Requirement 5

A statistical model of the TRNG should be available and should use the probability distribution $\mathbb{P}\big(\varphi(t)|p_1, p_2, \cdots, p_n, \varphi(t_0)\big)$.



Statistical model of a TRNG

Requirement 5

A statistical model of the TRNG should be available and should use the probability distribution $\mathbb{P}\big(\varphi(t)|p_1, p_2, \cdots, p_n, \varphi(t_0)\big)$.

In the case of a PLL-based TRNG

- X_i random variable with values in $\{0, 1\}$
  - logical level of the sampled bit at time iT_{clk}.
- Probability to sample bit 1 at $i \times T_{clk}$[a]

$$\mathbb{P}(X_i = 1) \;=\; \mathbb{P}(\varphi_i < \alpha T_{clj}) - \mathbb{P}(\varphi_i < 0) + 1 - \mathbb{P}(\varphi_i < T_{clj}).$$

[a] F. Bernard, V. Fischer, B. Valtchanov. Mathematical Model of Physical RNGs Based On Coherent Sampling. Tatra Mountains - Mathematical Publications, 2010.

Use of the statistical model of a TRNG

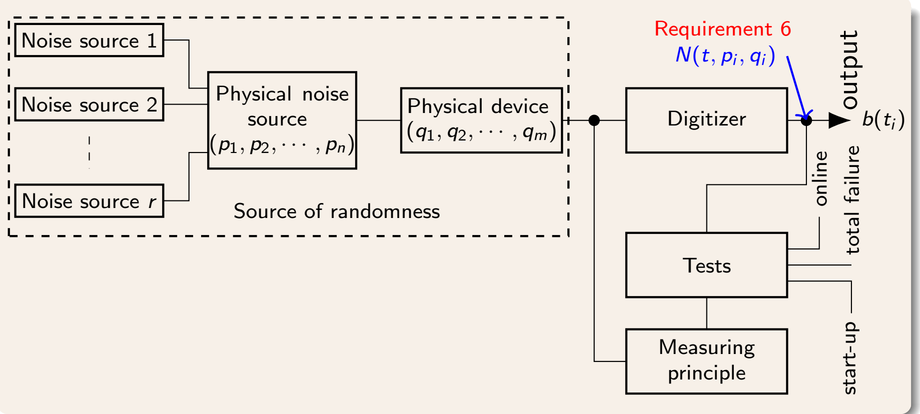
Obtaining the best configuration

Requirement 6

From the statistical model of the TRNG, it should be possible to adjust parameters $q_1, q_2, \cdots, q_m$ in order to bound the value defined by the bias on the bits that output from the generator.

Use of the statistical model of a TRNG

Obtaining the best configuration



Use of the statistical model of a TRNG

Obtaining the best configuration

Requirement 6

From the statistical model of the TRNG, it should be possible to adjust parameters $q_1, q_2, \cdots, q_m$ in order to bound the value defined by the bias on the bits that output from the generator.

In the case of a PLL-based TRNG

- Combinatorial optimization
  - heuristic and metaheuristic methods.
- Work still in progress.

Use of the statistical model of a TRNG

Monitoring the source of entropy

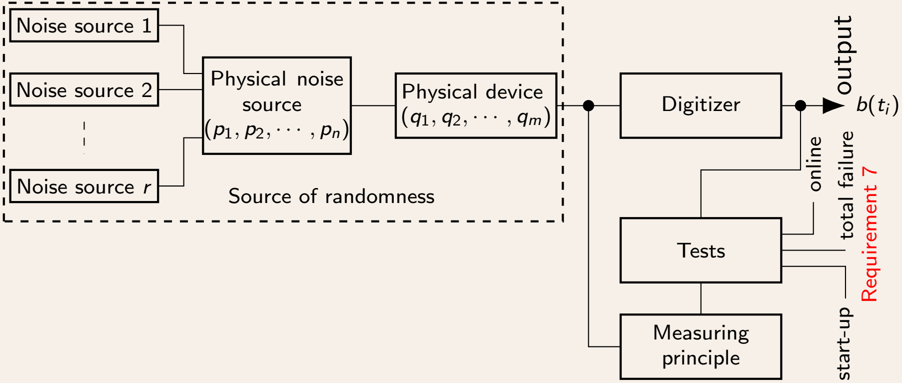
Requirement 7

Some parametric tests should be available

- at start-up,
- online,
- total failure test.

Use of the statistical model of a TRNG

Monitoring the source of entropy



Use of the statistical model of a TRNG

Monitoring the source of entropy

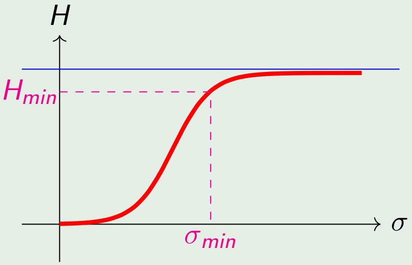
Requirement 7

Some parametric tests should be available

- at start-up,
- online,
- total failure test.

A parametric test

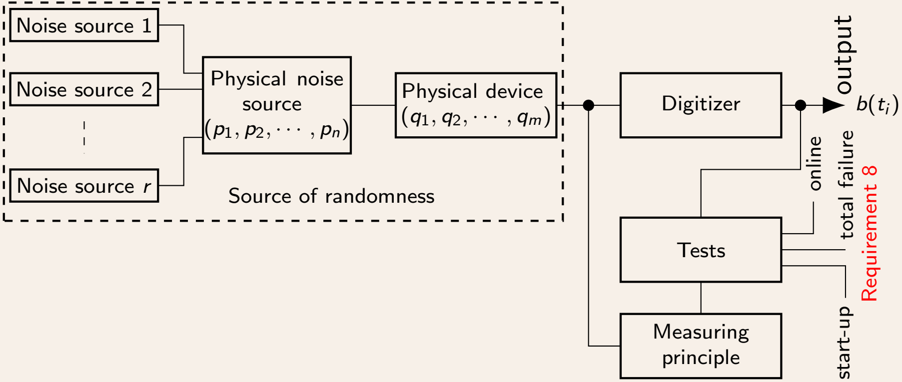
- $H = f(\sigma | K_M, K_D, \varphi_0, \alpha)$
- Entropy threshold H_{min}
  - minimum entropy tolerated
    - $\hookrightarrow$ alarm (under H_{min});
  - related to σ_{min}.
- Online test.



Deterministic tests

Requirement 8

There must be tests of deterministic functions that verify proper operation of the functional elements of the TRNG.



1. Evaluation process
2. Conclusion

Feasibility and pertinence of the approach

Higher security level

- Take into account the source of randomness
  - not only the output or digitized noise.

Illustration of the approach

- Evaluated on the PLL-based TRNG
  - approach valid.
- Evaluated on the RO-based TRNG
  - by D. Lubicz (DGA),
  - approach valid.

General process?

- Other hardware generators
  - TERO,
  - STR,
  - ...


Last Slide
Thank You