Problématiques modernes de la génération d'aléa véritable: étude approfondie d'un TRNG basé sur les PLLs.

Nathalie Bochard, Florent Bernard[1]

Laboratoire Hubert Curien, UMR 5516 CNRS
Université Jean Monnet, Saint-Etienne, France

Journées nationales du GDR Sécurité, 28 juin 2023

[1]joint work with: V. Fischer, Q. Dallison, M. Skorski

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;
    - ↪ From a physical randomness source (thermal noise,. . .)
  - Need to generate *good* **True** random numbers;

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;
    - ↪ From a physical randomness source (thermal noise,. . .)
  - Need to generate *good* **True** random numbers;

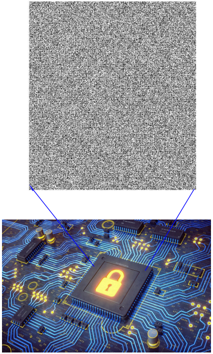
Certification

Our devices produce very good randomness !

THALES

life.augmented

SECURE-iC
THE SECURITY SCIENCE COMPANY



Yes it seems, can you prove it?

MINISTÈRE DE LA DÉFENSE

DGA

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

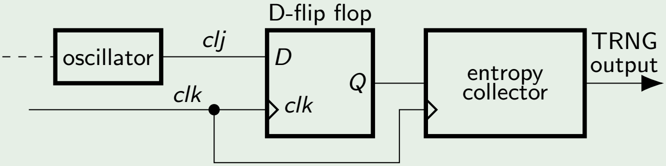
Bundesamt
für Sicherheit in der
Informationstechnik

Governmental organization

Is the Random Number Generator good enough to be embedded in cryptographic devices?

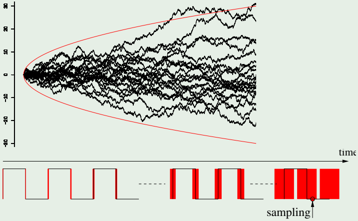
General principle of many hardware TRNG

General principle



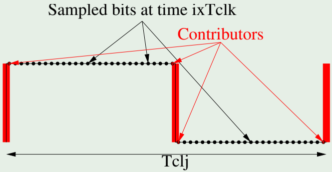
Two different ways of harvesting entropy

- Jitter accumulation



  - Ex: RO-based TRNG

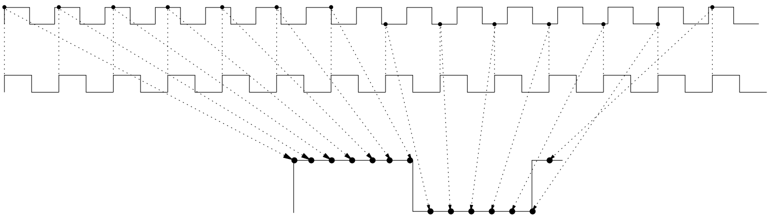
- Time resolution



  - Ex: Coherent sampling

Coherent sampling based TRNG

- General Principle (sampling signal: clk, sampled signal: clj)



  - The set of samples (eventually rearranged) gives the form of the original signal (reconstructed period)
  - $|T_{clj} - T_{clk}| = \Delta$ distance between two successive samples.
  - if Δ is small enough, some samples are expected to be influenced by the phase jitter.
  - Used in COSARO-TRNG[2] and enhanced by Valtchanov[3]

[2] P. Kohlbrenner, K. Gaj: An Embedded True Random Number Generator for FPGAs, ACM/SIGDA FPGA 2004

[3] B. Valtchanov: True Random Number Generators: Modeling and Implementation in FPGAs, Phd Thesis, 2010

Coherent sampling: implementation issues

- Δ must be smaller than the jitter σ_{jitt} to guarantee that samples are influenced by the jitter.

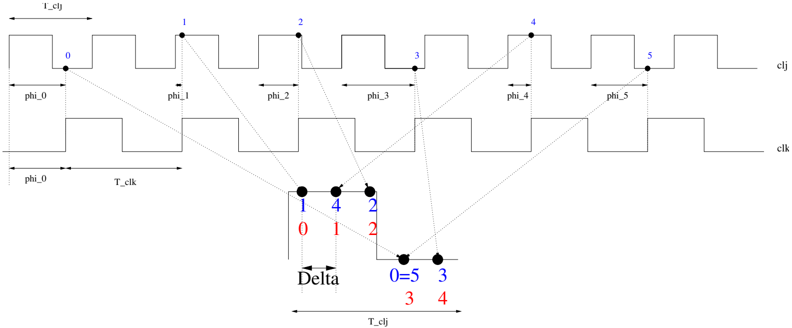
Critical point: precise delay control

- oscillators must have frequencies very close to each others $\Rightarrow$ need a carefull/manual place and routing for each device individually.
- Consequence: oscillators can lock. . .

- The initial phase between two successive reconstructed periods is not necessarily the same...

Coherent sampling: when frequencies are rationaly related

- Exemple: $\frac{T_{clk}}{T_{clj}} = \frac{7}{5} = \frac{p}{q} \quad (5 \times T_{clk} = 7 \times T_{clj})$



- For $i \in \{0, \ldots, q-1\}$, $\varphi_i = \varphi_0 + i \times T_{clk} \mod T_{clj}$
- $\Delta := \frac{T_{clj}}{q}$
- Samples have to be reordered (using the rational relation): $N_{\varphi_0} + i \times p \mod q = j \quad (3 + i \times 7 \mod 5 = j)$

Coherent sampling: solution to previous issues

Δ must be smaller than the jitter σ_{jitt}

- ♣ $\Delta = \frac{T_{clj}}{q}$ distance between two successive samples on the reconstructed period (can be as small as q is big)

The initial phase φ_0 between two reconstructed periods is not constant

- ♣ Due to the relation $\frac{T_{clk}}{T_{clj}} = \frac{p}{q}$, φ_0 is constant for each reconstructed period.

$$(\varphi_q = \varphi_0 + \underbrace{q \times T_{clk}}_{=p \times T_{clj}} \mod T_{clj} = \varphi_0 + \underbrace{p \times T_{clj}}_{\mod T_{clj} = 0} \mod T_{clj} = \varphi_0)$$

Ensuring a rational frequency between T_{clj} and T_{clk}

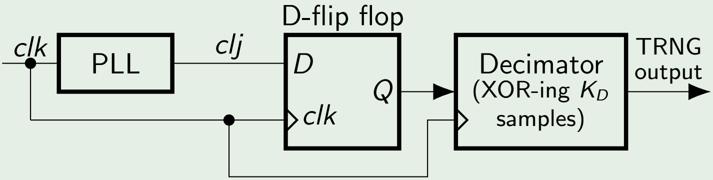
PLL (Phase Locked Loop): designed to guarantee a rational frequency between its input and output signals

$\Rightarrow$ PLLs are interesting to design TRNG based on coherent sampling.

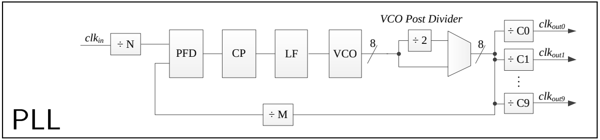
1. PLL-based TRNG
2. Stochastic model of the PLL-based TRNG
3. Use of the model: tests of the entropy source
4. Conclusion and future work

General principle of a PLL-based TRNG

PLL-based TRNG



V.Fischer, M. Drutarovsky: True Random Number Generator Embedded in Reconfigurable Hardware, CHES 2002



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

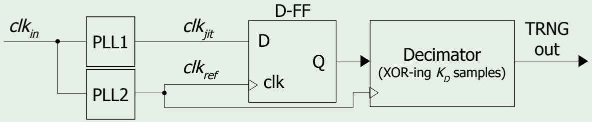
- Control the phase difference between input and output signal of the PLL ⇒ Control the drift that remains bounded.

Differential principle: from one to two PLL

- In order to reduce global influences a differential principle is recommended[4]
- Increasing the resolution of coherent sampling (i.e. increasing K_D), can be limited by the range of values for N and C ($K_D = N \times C$).

Solution: proposal of a two PLL design

$$K_M = K_{M1} \cdot K_{D2}$$
$$K_D = K_{D1} \cdot K_{M2}$$



$$\frac{F_{clk_{jit}}}{F_{clk_{ref}}} = \frac{\frac{K_{M_1}}{K_{D_1}} F_{clk_{in}}}{\frac{K_{M_2}}{K_{D_2}} F_{clk_{in}}} = \frac{K_{M_1} \cdot K_{D_2}}{K_{M_2} \cdot K_{D_1}} = \frac{K_M}{K_D}$$

[4] Valtchanov B. et al, Modeling and observing the jitter in ring oscillators implemented in FPGAs, DDECS 2008

Bit rate vs sensitivity (resolution)

- Sensitivity to jitter: $S = \frac{K_D}{T_{clj}}$
- Bit rate: $R = \frac{1}{K_D \times T_{clk}}$

Tradeoff

- Priority 1: K_D should be high enough to ensure a *sufficient* sensitivity to the jitter;
- Priority 2: K_D should be as small *as possible* to ensure the highest bit rate.

Question

How to determine the PLL's parameters in order to achieve these two goals (and find the best tradeoff)?

Optimization of the PLL configuration for TRNG

PLL SPECIFICATIONS OF SELECTED FPGA FAMILIES

Parameter	Cyclone V		Spartan-6		SmartFusion®2	
	Min	Max	Min	Max	Min	Max
f_{ref}(MHz)	5	500	19	540	1	200
P_{VCO_i}	1	2	1	1	1	32
N_i	1	512	1	52	1	16384
M_i	1	512	1	64	1	4194304
C_i	1	512	1	128	1	255
f_{PFD_i}(MHz)	5	325	19	500	1	200
f_{VCO_i}(MHz)	600	1300	400	1080	500	1000
f_{out_i}(MHz)	0	460	3.125	400	20	400

$\Rightarrow$ Billions of possible configurations
How to find the suitable ones ($<1\%$)?

Available Tool

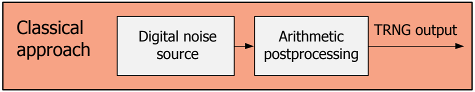
Set (security, throughput, ...) constraints to get suitable configurations among possible configurations.[a]

[a] E.N. Allini, O. Petura, V. Fischer, F. Bernard, Optimization of the PLL Configuration in a PLL-based TRNG Design, DATE 2018, Dresden, Germany

Assessment of the PLL-TRNG quality

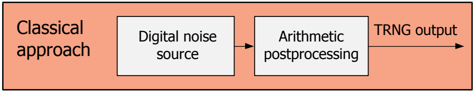
How to assess the quality of the proposed generator?
How this assessment can be used to set security constraints?

A first approach for TRNG evaluation: Observation

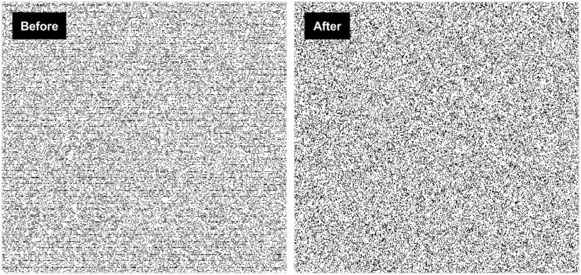


- Battery of statistical tests (FIPS, NIST, DieHard) at the TRNG output.
- Problem1: even a full deterministic sequence can pass these tests
  $\Rightarrow$ tests are necessary **but not sufficient**
- Need to perform tests **before** post-processing.

A first approach for TRNG evaluation: Observation

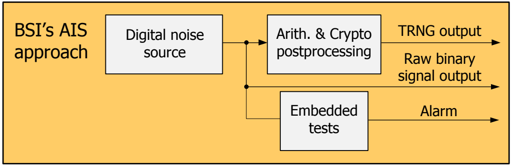


- Battery of statistical tests (FIPS, NIST, DieHard) at the TRNG output.
- Problem2:



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

A second approach for TRNG evaluation: proof/certification



Same as the classical approach plus:

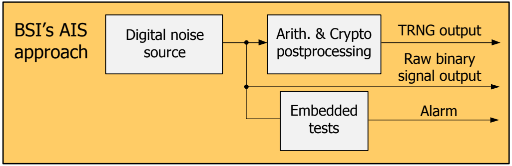
+ Test the raw binary signal and estimate the entropy (min entropy) per generated bit
+ Provide embedded tests to detect a total failure of the noise source.

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

Stochastic model

⇒ 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:
  - There is no generic Model: each TRNG principle must be described with a dedicated and parameterized stochastic model.
  - Model $\neq$ Reality
  - Need reasonable assumptions to work on random variables.
    - ↪ Is the extracted noise composed only of thermal noise[5] as it is almost always assumed in the TRNG state of the art?
    - ↪ What about correlations between sampled random bits?

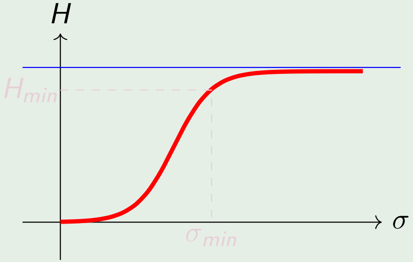
[5] Thermal noise is considered to be unavoidable and non manipulable

1. PLL-based TRNG
2. Stochastic model of the PLL-based TRNG
3. Use of the model: tests of the entropy source
4. Conclusion and future work

Goals of the stochastic model

Entropy rate (H) and thresholds

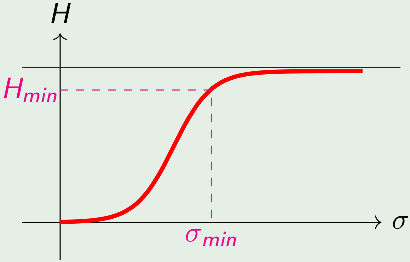
- Stochastic model should give
  $$H = f\big(\underbrace{\text{noise param.}}_{\sigma} \,\big|\, \underbrace{\text{TRNG param.}}_{K_M, K_D, \alpha, \varphi_0}\big)$$
- Entropy threshold H_{min}
  - minimum entropy tolerated
  - related to σ_{min} (thanks to the model).
  - Sufficient entropy is achieved when $\sigma \geqslant \sigma_{min}$
- Online test(s) based on the model must be related to σ_{min}
  $$OT(\sigma) < \underbrace{OT(\sigma_{min})}_{\text{threshold}} \Rightarrow \text{alarm}$$



Goals of the stochastic model

Entropy rate (H) and thresholds

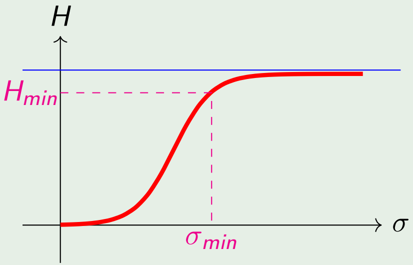
- Stochastic model should give
  $H = f(\underbrace{\text{noise param.}}_{\sigma} \mid \underbrace{\text{TRNG param.}}_{K_M, K_D, \alpha, \varphi_0})$
- Entropy threshold H_{min}
  - minimum entropy tolerated
  - related to σ_{min} (thanks to the model).
  - Sufficient entropy is achieved when $\sigma \geqslant \sigma_{min}$
- Online test(s) based on the model must be related to σ_{min}
  $OT(\sigma) < \underbrace{OT(\sigma_{min})}_{\text{threshold}} \Rightarrow$ alarm



Goals of the stochastic model

Entropy rate (H) and thresholds

- Stochastic model should give
  $H = f(\underbrace{\text{noise param.}}_{\sigma} \mid \underbrace{\text{TRNG param.}}_{K_M, K_D, \alpha, \varphi_0})$
- Entropy threshold H_{min}
  - minimum entropy tolerated
  - related to σ_{min} (thanks to the model).
  - Sufficient entropy is achieved when $\sigma \geqslant \sigma_{min}$
- Online test(s) based on the model must be related to σ_{min}
  $OT(\sigma) < \underbrace{OT(\sigma_{min})}_{\text{threshold}} \Rightarrow$ alarm

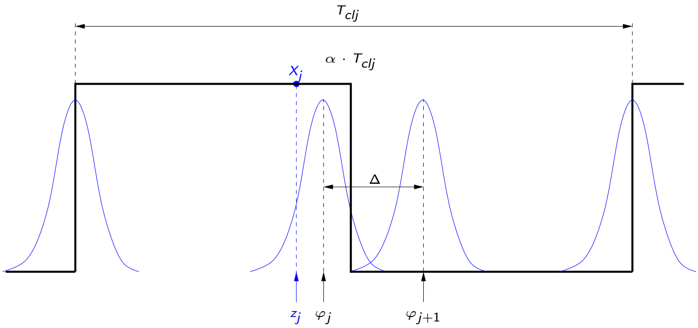


Reconstructed period from experimental data

Steps

- Describe the probability distribution of the space of phases (depending on the jitter)
- Compute the probability $\Pr(X_j = 1)$ that the bit X_j sampled at time $i \times T_{clk} = (j \cdot K_M^{-1} \mod K_D) \cdot T_{clk}$ is equal to 1.
- Compute the probability of XOR-ing bits X_j, $B_{out} := \bigoplus_{j=0}^{K_D-1} X_j$
- Compute a lower bound for the entropy of B_{out} in the worst case.
- Use this lower bound to define experimental online tests and their thresholds based on the expected H_{min} from standards.

Reconstructed period and space of phase



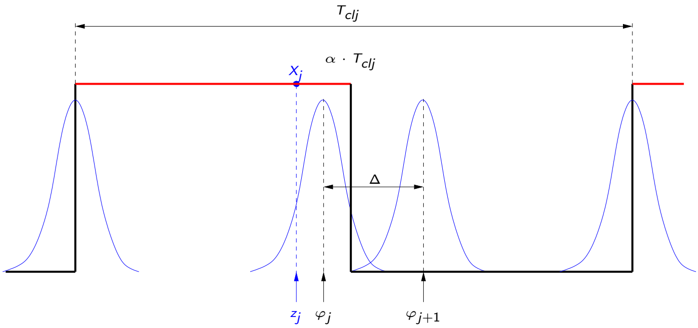
Space of phase

Random phases z_j as realizations of the random variable $\mathcal{Z}_j \sim \mathcal{N}\left(\varphi_j, \sigma^2\right)$ where $\varphi_j = \varphi_0 + j \cdot \Delta \mod T_{clj}$

Sampling: $\Pr(X_j = 1)$ (assuming $\sigma << T_{clj}$)

$\Pr(X_j = 1) = \Pr(0 < \mathcal{Z}_j < \alpha \cdot T_{clj}) + \Pr(T_{clj} < \mathcal{Z}_j < T_{clj} + \alpha \cdot T_{clj})$

Reconstructed period and space of phase



Space of phase

Random phases z_j as realizations of the random variable $\mathcal{Z}_j \sim \mathcal{N}\left(\varphi_j, \sigma^2\right)$ where $\varphi_j = \varphi_0 + j \cdot \Delta \mod T_{clj}$

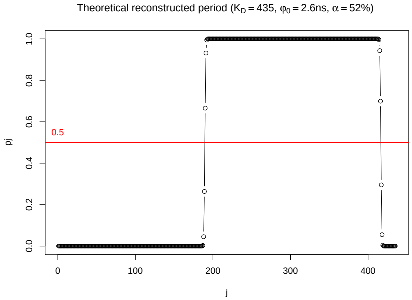
Sampling: $\Pr(X_j = 1)$ (assuming $\sigma << T_{clj}$)

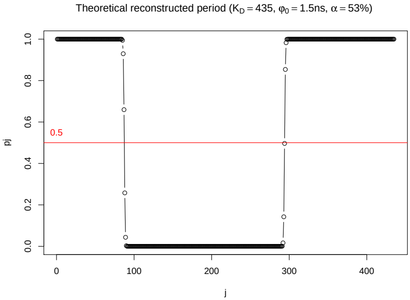
$$\Pr(X_j = 1) = \Pr(0 < \mathcal{Z}_j < \alpha \cdot T_{clj}) + \Pr(T_{clj} < \mathcal{Z}_j < T_{clj} + \alpha \cdot T_{clj})$$

Theoretical reconstructed period

Set of probabilities $p_j := \Pr(X_j = 1)$

For j in $\{0, \ldots, K_D - 1\}$, $p_j = \Phi\left(\frac{\alpha \cdot T_{clj} - \varphi_j}{\sigma}\right) - \Phi\left(-\frac{\varphi_j}{\sigma}\right) + 1 - \Phi\left(\frac{T_{clj} - \varphi_j}{\sigma}\right)$





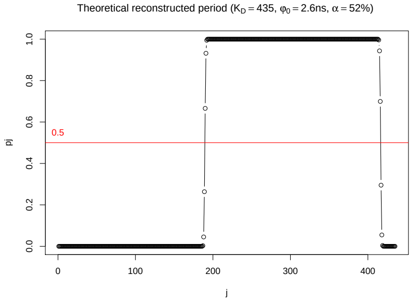
TRNG output B_{out}

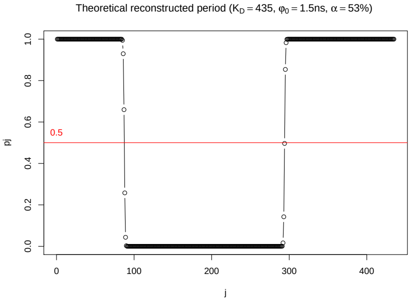
$$B_{out} = \bigoplus_{j=0}^{K_D-1} X_j, \qquad \Pr(B_{out} = 1) = ??$$

Theoretical reconstructed period

Set of probabilities $p_j := \Pr(X_j = 1)$

For j in $\{0, \ldots, K_D - 1\}$, $p_j = \Phi\left(\frac{\alpha \cdot T_{clj} - \varphi_j}{\sigma}\right) - \Phi\left(-\frac{\varphi_j}{\sigma}\right) + 1 - \Phi\left(\frac{T_{clj} - \varphi_j}{\sigma}\right)$





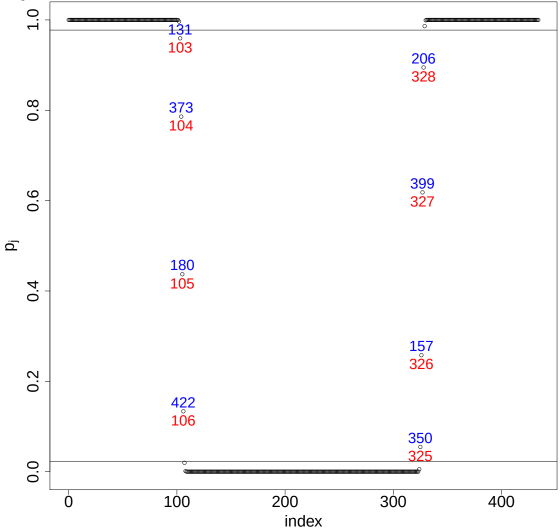
TRNG output B_{out} (Assuming independance of bits ??)

$$B_{out} = \bigoplus_{j=0}^{K_D-1} X_j, \qquad \Pr(B_{out} = 1) = \frac{1}{2} + (-2)^{K_D-1} \prod_{j=0}^{K_D-1} \left(p_j - \frac{1}{2}\right) \quad \text{(Davies Formula)}$$

A closer look at the reconstructed period

Adjacent bits (index j) in the reconstructed period are **not adjacent in time** (index i):

$j = i \times K_M \mod K_D$



- Minimum distance in time between contributors: 23 clock periods
- Idea: for a sufficiently large distance between contributors, they can be supposed uncorrelated
- Specific K_M, K_D should be found to maximize this distance.

Distance between contributors

Contributors and set of distances (More formally!)

- A contributor is a sample X_j such that $0 < \Pr(X_j = 1) < 1$
  $(0.02275 \leqslant \Pr(X_j = 1) \leqslant 0.97725 \Leftrightarrow \varphi_j - 2\sigma \leqslant \mathcal{Z}_j \leqslant \varphi_j + 2\sigma)$
  Remark: For a given σ_{min} and PLL configuration, the theoretical minimum number of contributors can be computed (usually $\sim 6 - 8$).
- Offsets to be considered in the reconstructed period can be either:
  - between adjacent contributors in the same edge: $\tau_1 = 2$ or 3
  - between contributors in the rising or falling edge.
    Depends on the duty cycle α and τ_1.
    Minimum offset: $\tau_2^{min} = \lceil \max(\alpha \cdot K_D, (1-\alpha) \cdot K_D) \rceil - \tau_1$
    Maximum offset: $\tau_2^{max} = \lceil \max(\alpha \cdot K_D, (1-\alpha) \cdot K_D) \rceil + \tau_1$

  $\mathcal{T} = [\![1, \tau_1]\!] \bigcup [\![\tau_2^{min}, \tau_2^{max}]\!]$
- For $\tau \in \mathcal{T}$, $d_{min}(\tau) := \min((\tau \times K_M^{-1}) \mod K_D, K_D - (\tau \times K_M^{-1} \mod K_D))$

Example: $K_M = 728$, $K_D = 435$, $\alpha = 0.49 \rightarrow \mathcal{T} = [\![1, 3]\!] \bigcup [\![219, 225]\!]$

- $\{d_{min}(\tau)\}_{\tau \in \mathcal{T}} = \{193, 49, 144, 72, 170, 23, 216, 26, 167, 75\}$
- S_c is the set of index j corresponding to contributors such that $d_{min}(\tau)$ is sufficiently high (23?, 26?, 49?, 72?, 75?) to ensure uncorrelated contributors.

Distance between contributors

Contributors and set of distances (More formally!)

- A contributor is a sample X_j such that $0 < \Pr(X_j = 1) < 1$
  $(0.02275 \leqslant \Pr(X_j = 1) \leqslant 0.97725 \Leftrightarrow \varphi_j - 2\sigma \leqslant \mathcal{Z}_j \leqslant \varphi_j + 2\sigma)$
  Remark: For a given σ_{min} and PLL configuration, the theoretical minimum number of contributors can be computed (usually $\sim 6 - 8$).
- Offsets to be considered in the reconstructed period can be either:
  - between adjacent contributors in the same edge: $\tau_1 = 2$ or 3
  - between contributors in the rising or falling edge.
    Depends on the duty cycle α and τ_1.
    Minimum offset: $\tau_2^{min} = \lceil \max(\alpha \cdot K_D, (1-\alpha) \cdot K_D) \rceil - \tau_1$
    Maximum offset: $\tau_2^{max} = \lceil \max(\alpha \cdot K_D, (1-\alpha) \cdot K_D) \rceil + \tau_1$

  $\mathcal{T} = [\![1, \tau_1]\!] \bigcup [\![\tau_2^{min}, \tau_2^{max}]\!]$
- For $\tau \in \mathcal{T}$, $d_{min}(\tau) := \min((\tau \times K_M^{-1}) \mod K_D, K_D - (\tau \times K_M^{-1} \mod K_D))$

Example: $K_M = 728$, $K_D = 435$, $\alpha = 0.49 \rightarrow \mathcal{T} = [\![1, 3]\!] \bigcup [\![219, 225]\!]$

- $\{d_{min}(\tau)\}_{\tau \in \mathcal{T}} = \{193, 49, 144, 72, 170, 23, 216, 26, 167, 75\}$
- S_c is the set of index j corresponding to contributors such that $d_{min}(\tau)$ is sufficiently high (23?, 26?, 49?, 72?, 75?) to ensure uncorrelated contributors.

Distance between contributors

Contributors and set of distances (More formally!)

- A contributor is a sample X_j such that $0 < \Pr(X_j = 1) < 1$
  $(0.02275 \leqslant \Pr(X_j = 1) \leqslant 0.97725 \Leftrightarrow \varphi_j - 2\sigma \leqslant \mathcal{Z}_j \leqslant \varphi_j + 2\sigma)$
  Remark: For a given σ_{min} and PLL configuration, the theoretical minimum number of contributors can be computed (usually $\sim 6 - 8$).
- Offsets to be considered in the reconstructed period can be either:
  - between adjacent contributors in the same edge: $\tau_1 = 2$ or 3
  - between contributors in the rising or falling edge.
    Depends on the duty cycle α and τ_1.
    Minimum offset: $\tau_2^{min} = \lceil \max(\alpha \cdot K_D, (1-\alpha) \cdot K_D) \rceil - \tau_1$
    Maximum offset: $\tau_2^{max} = \lceil \max(\alpha \cdot K_D, (1-\alpha) \cdot K_D) \rceil + \tau_1$

  $\mathcal{T} = [\![1, \tau_1]\!] \bigcup [\![\tau_2^{min}, \tau_2^{max}]\!]$
- For $\tau \in \mathcal{T}$, $d_{min}(\tau) := \min((\tau \times K_M^{-1}) \mod K_D, K_D - (\tau \times K_M^{-1} \mod K_D))$

Example: $K_M = 728$, $K_D = 435$, $\alpha = 0.49 \rightarrow \mathcal{T} = [\![1, 3]\!] \bigcup [\![219, 225]\!]$

- $\{d_{min}(\tau)\}_{\tau \in \mathcal{T}} = \{193, 49, 144, 72, 170, 23, 216, 26, 167, 75\}$
- S_c is the set of index j corresponding to contributors such that $d_{min}(\tau)$ is sufficiently high (**23**?, **26**?, **49**?, **72**?, **75**?) to ensure uncorrelated contributors.

Exam time!! (This is not a statistical test: do not answer randomly ;-))

For these two similar configurations on Xilinx Spartan 6, which one is the best?

- Config. 1: $K_M = 476$, $K_D = 495$, $f_{clj} = 145$MHz, $f_{clk} = 148.44$MHz
  Bit rate: $R = 0.3$ Mbit/s, Sensitivity to jitter: $S = 0.07$
- Config. 2: $K_M = 464$, $K_D = 475$, $f_{clj} = 141.67$MHz, $f_{clk} = 147.32$MHz
  Bit rate: $R = 0.31$ Mbit/s, Sensitivity to jitter: $S = 0.069$

Exam time!! (This is not a statistical test: do not answer randomly ;-))

For these two similar configurations on Xilinx Spartan 6, which one is the best?

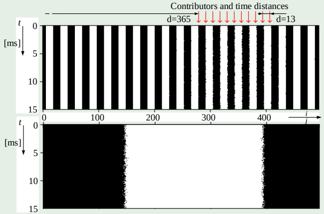
- Config. 1: $K_M = 476$, $K_D = 495$, $f_{clj} = 145\text{MHz}$, $f_{clk} = 148.44\text{MHz}$
  Bit rate: $R = 0.3$ Mbit/s, Sensitivity to jitter: $S = 0.07$
- Config. 2: $K_M = 464$, $K_D = 475$, $f_{clj} = 141.67\text{MHz}$, $f_{clk} = 147.32\text{MHz}$
  Bit rate: $R = 0.31$ Mbit/s, Sensitivity to jitter: $S = 0.069$

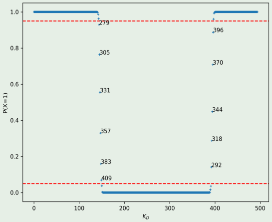
Exam time!! (This is not a statistical test: do not answer randomly ;-))

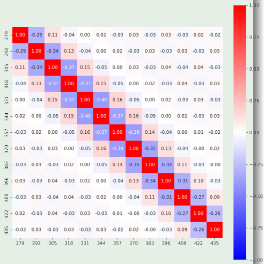
For these two similar configurations on Xilinx Spartan 6, which one is the best?

- Config. 1: $K_M = 476$, $K_D = 495$, $f_{clj} = 145\text{MHz}$, $f_{clk} = 148.44\text{MHz}$
  Bit rate: $R = 0.3$ Mbit/s, Sensitivity to jitter: $S = 0.07$
- Config. 2: $K_M = 464$, $K_D = 475$, $f_{clj} = 141.67\text{MHz}$, $f_{clk} = 147.32\text{MHz}$
  Bit rate: $R = 0.31$ Mbit/s, Sensitivity to jitter: $S = 0.069$

Explanation: Config. 1, from experimental data ($d_{min} = 13$)





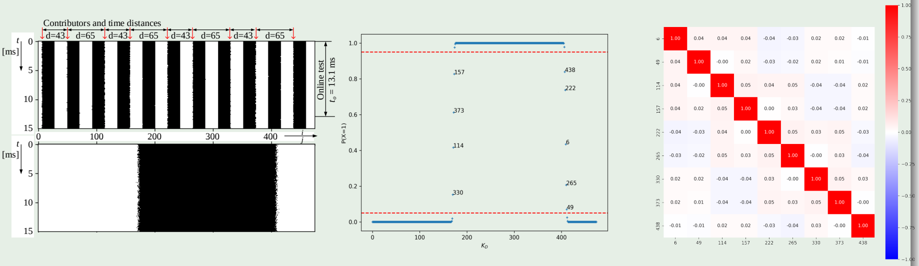


Exam time!! (This is not a statistical test: do not answer randomly ;-))

For these two similar configurations on Xilinx Spartan 6, which one is the best?

- Config. 1: $K_M = 476$, $K_D = 495$, $f_{clj} = 145\text{MHz}$, $f_{clk} = 148.44\text{MHz}$
  Bit rate: $R = 0.3$ Mbit/s, Sensitivity to jitter: $S = 0.07$
- Config. 2: $K_M = 464$, $K_D = 475$, $f_{clj} = 141.67\text{MHz}$, $f_{clk} = 147.32\text{MHz}$
  Bit rate: $R = 0.31$ Mbit/s, Sensitivity to jitter: $S = 0.069$

Explanation: Config. 2, from experimental data ($d_{min} = 43$)



A closer look at Davies formula in case of correlation between bits

Davies formula

- Eq.(1) is used to compute $Pr(X_1 \oplus X_2 = 1)$ in the case where X_1 and X_2 are not independent, where $\mu := Pr(X_1 = 1)$, $\nu := Pr(X_2 = 1)$ and $\rho := Corr(X_1, X_2)$

$$Pr(X_1 \oplus X_2 = 1) = \frac{1}{2} - 2\left(\mu - \frac{1}{2}\right)\left(\nu - \frac{1}{2}\right) - \rho\sqrt{\mu(1-\mu)\nu(1-\nu)} \qquad (1)$$

- $\Rightarrow$ 2 conditions to consider the extra term $\rho\sqrt{\mu(1-\mu)\nu(1-\nu)}$ negligible:
  1. The correlation factor ρ between contributors is very small;
  2. The probability that a bit X_j is equal to a one is very close to 0 or very close to 1. ($\Leftrightarrow X_j$ is NOT a contributor)
- The set of distances helps to ensure the first condition by removing correlated samples from the set of contributors.

Summary and consequences: toward a lower bound for Entropy

- $H(B_{out}) = H\left(\bigoplus_{j=0}^{K_D-1} X_j\right) \geq H\left(\bigoplus_{j \in S_c} X_j\right) = f(\underbrace{\sigma}_{\text{noise}} \mid \underbrace{K_M, K_D,}_{\text{tunable}} \underbrace{\alpha, \varphi_0}_{\text{unknown}})$

A closer look at Davies formula in case of correlation between bits

Davies formula

- Eq.(1) is used to compute $Pr(X_1 \oplus X_2 = 1)$ in the case where X_1 and X_2 are not independent, where $\mu := Pr(X_1 = 1)$, $\nu := Pr(X_2 = 1)$ and $\rho := Corr(X_1, X_2)$

$$Pr(X_1 \oplus X_2 = 1) = \frac{1}{2} - 2\left(\mu - \frac{1}{2}\right)\left(\nu - \frac{1}{2}\right) - \rho\sqrt{\mu(1-\mu)\nu(1-\nu)} \qquad (1)$$

- $\Rightarrow$ 2 conditions to consider the extra term $\rho\sqrt{\mu(1-\mu)\nu(1-\nu)}$ negligible:
  1. The correlation factor ρ between contributors is very small;
  2. The probability that a bit X_j is equal to a one is very close to 0 or very close to 1. ($\Leftrightarrow X_j$ is NOT a contributor)
- The set of distances helps to ensure the first condition by removing correlated samples from the set of contributors.

Summary and consequences: toward a lower bound for Entropy

- $$H(B_{out}) = H\left(\bigoplus_{j=0}^{K_D-1} X_j\right) \geqslant H\left(\bigoplus_{j \in S_c} X_j\right) = f(\underbrace{\sigma}_{\text{noise}} \mid \underbrace{K_M, K_D,}_{\text{tunable}} \underbrace{\alpha, \varphi_0}_{\text{unknown}})$$

Determining the lower bound for the Entropy as a function of σ

Unknown parameters φ_0 and α

2 strategies:

- Measure them precisely.
- Determine the worst case for both of them

Determining the lower bound for the Entropy as a function of σ

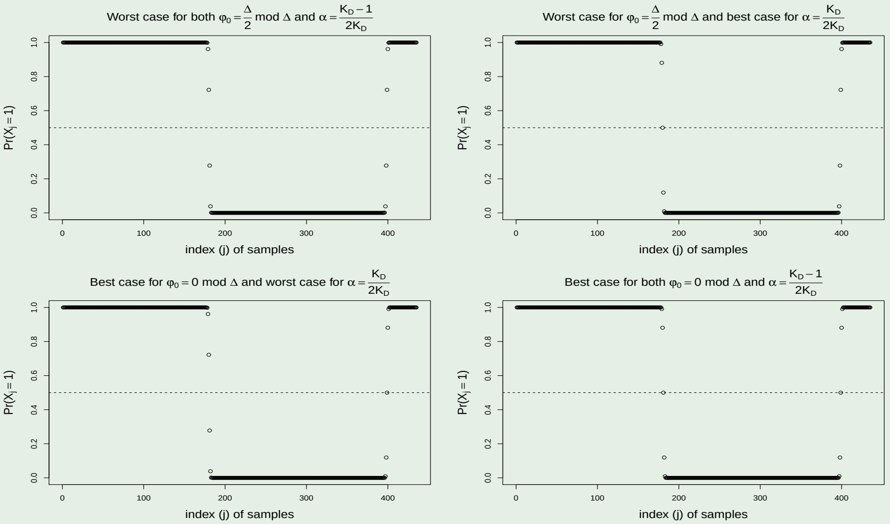
Unknown parameters φ_0 and α

2 strategies:

- Measure them precisely. Hard... embeddability, precision
- Determine the worst case for both of them

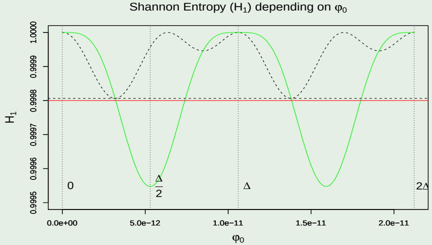
Determining the lower bound for the Entropy as a function of σ

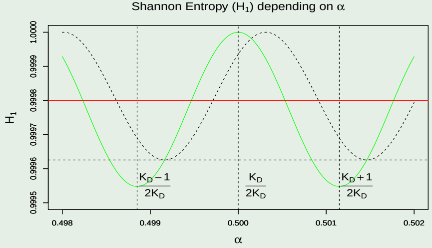
Plotting $f(\sigma \mid K_M, K_D, \alpha, \varphi_0)$ using the model



Determining the lower bound for the Entropy as a function of σ

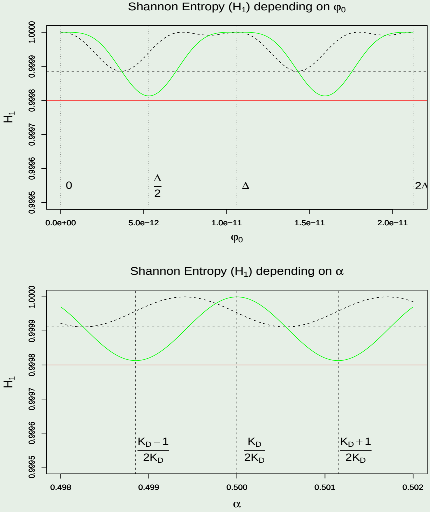
Plotting $f(\sigma \mid K_M, K_D, \alpha, \varphi_0)$ using the model $(\sigma < \sigma_{min})$





Determining the lower bound for the Entropy as a function of σ

Plotting $f(\sigma \mid K_M, K_D, \alpha, \varphi_0)$ using the model ($\sigma \geqslant \sigma_{min}$)

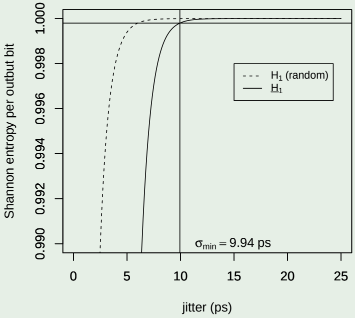


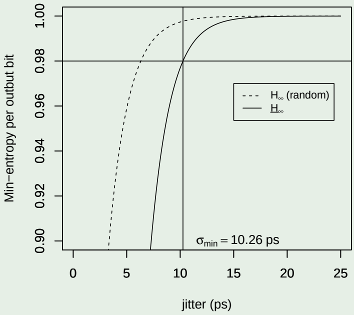
Determining the lower bound for the Entropy as a function of σ

Lower bound for $H(B_{out})$

$$H(B_{out}) \geqslant H\left(\bigoplus_{j\in S_c} X_j\right) = f(\sigma \mid K_M, K_D, \alpha, \varphi_0) \geqslant f(\sigma \mid K_M, K_D, \underbrace{\frac{K_D-1}{2K_D}, \frac{\Delta}{2}}_{\text{worst cases}})$$

Plot of Entropies in the worst case as a function of σ - Determination of σ_{min}





1 PLL-based TRNG

2 Stochastic model of the PLL-based TRNG

3 Use of the model: tests of the entropy source

4 Conclusion and future work

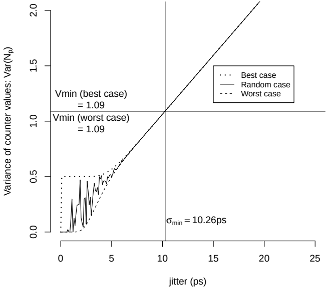
Metric and online test

Metric used

- N_p random variable representing the number of samples X_j equal to 1 in one pattern period of K_D samples
  Motivation: Counters are easy to implement and conveys more information than the single bit B_{out}.
- N_p follows a Poisson Binomial distribution over the set $(p_j)_{j \in [\![0;K_D-1]\!]}$
- $Var(N_p)$ is used as it is easy to implement in hardware and gives information on σ

Online test: $Var(N_p)$ and $\sigma_{min} \rightarrow V_{min}$

- $$Var(N_p) = \sum_{j=0}^{K_D-1} p_j(1-p_j) \geqslant \underbrace{\sum_{j \in S_c} p_j(1-p_j)}_{V_{min}}$$
- V_{min} is a threshold for this test. It can be computed from p_j according to the model for the σ_{min} previously found.
- Latency: $\sim 2 \cdot 10^6$ periods of clk.



Total Failure test

Principle

- Also use N_p (already available in hardware from the online test)
- Count how many consecutive N_p values are identical.
- Must react quickly (faster than the Online test) in case of total loss of entropy.

Thresholds

- Compute the probability that l values N_p are identical using the model:
- $\Pr(N_1 = \cdots = N_l) \approx$

$$\sum_{k=1}^{K_D} \left(\Phi\left(\frac{k + 0.5 - \mathbb{E}(N_p)}{\sqrt{\mathrm{Var}(N_p)}} \right) - \Phi\left(\frac{k - 0.5 - \mathbb{E}(N_p)}{\sqrt{\mathrm{Var}(N_p)}} \right) \right)^l \leqslant \beta$$

False alarm parameters	Once per day	Once per week	Once per month
β	$2^{-34.58}$	$2^{-37.38}$	$2^{-39.49}$
Threshold $l_{min}(\beta)$	24	26	28
Latency (as the number of periods T_{clj}) (150-200 times faster than the Online test)	10 440	11 310	12 180
Latency (in μs)	80.643	87.363	94.083

Use of the Statistical model of a TRNG

- Obtain the "best" configuration:
- Constraints:
  - Throughput: $R = \frac{1}{T_{clk} \cdot K_D}$
  - Sensitivity to jitter: $S = \frac{1}{\Delta} = \frac{K_D}{T_{clj}}$
  - Constrained ranges for M_i, N_i, C_i depending on the manufacturer
  - **Distances between contributors** (new)

An algorithm has been proposed to help the designer to define these tunable parameters (M_i, N_i, C_i) to find the best tradeoff between security requirements, throughput among feasible configurations.[6]

[6] B. Colombier et al, Backtracking Search for Optimal Parameters of a PLL-based True Random Number Generator, DATE 2020

1 PLL-based TRNG

2 Stochastic model of the PLL-based TRNG

3 Use of the model: tests of the entropy source

4 Conclusion and future work

Conclusion and future work

Conclusions

- Improvement of the stochastic model (assumptions, correlations) and better confidence in its use.
- Introduction of distance between contributors ⇒ possibility to predict configurations that will strongly reduce correlations
- Design of new embedded and specific tests (online, tot) based on the model and counter values
- Cited as an illustrative example of the AIS31 evaluation scheme *A proposal for: Functionality classes for random number generators - Version 2.35 - Draft*
- More details on the presented results: CHES 2023, sept. 2023 in Prague.

Open problems and current/future work

- Characterize more precisely the contribution of thermal noise at the output of the PLL[a]
- Potential well: Ornstein-Uhlenbeck process.

[a] Work initiated by E. Noumon Allini (PhD) and continued by Quentin Dallison (PhD student, Thales, UJM)


Last Slide
Thank You