Design of Secure TRNGs for Cryptography – Past, Present, and Future

Viktor FISCHER

Univ Lyon, UJM-Saint-Etienne, CNRS
Laboratoire Hubert Curien UMR 5516
F-42023, SAINT-ETIENNE, France

fischer@univ-st-etienne.fr

Workshop Wr0ng2017, Paris, April 2017

HEC10R

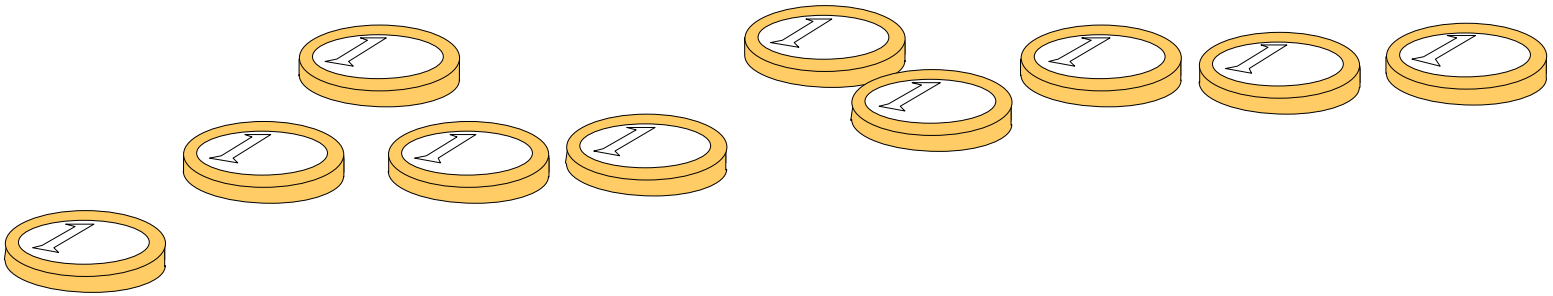
LABORATOIRE HUBERT CURIEN

Random Numbers in Cryptography

- **(True) Random Number Generator (RNG or TRNG)**
  Physical function generating a sequence of random bits or symbols (e.g. groups of bits = numbers)
- **RNG (or RBG, i.e. Random Bit Generator)**
  Essential part of cryptographic systems
- Today's cryptographic systems mostly implemented in **logic devices** (e.g. smart cards)
- Challenge: find and exploit **analog sources of randomness in digital devices** using a standard technology (avoid a full custom design)

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Fair Tossing of Fair Coins

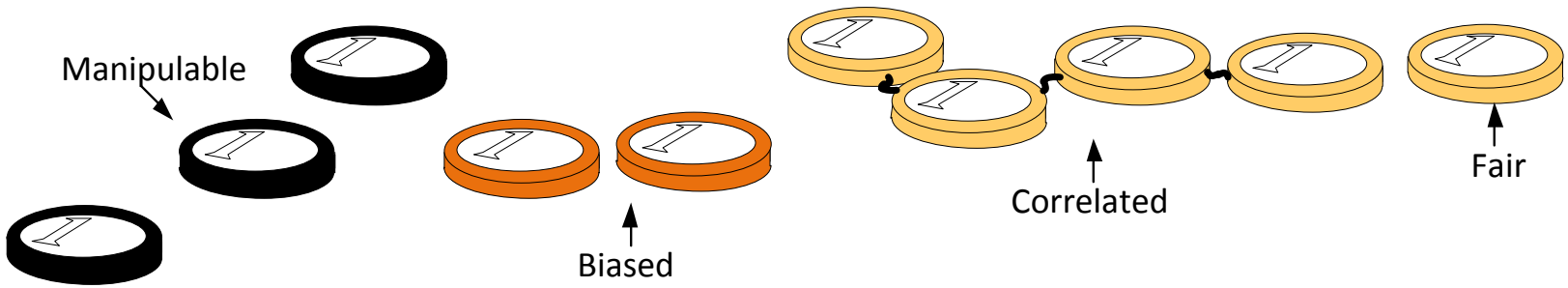


- Mathematical approach:
  - Considered as an **ideal TRNG**
  - Ten fair coins give **entropy rate of ten bits per trial**
- Physical approach:
  - What (physically) means **'fair tossing'**[1] and **'fair coins'**?
  - What can be the **frequency of trials**?

[1] In fact, mechanical systems are perfectly predictable. Only initial conditions determine the entropy.

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Tossing (Partially) Unfair Coins – Realistic TRNG

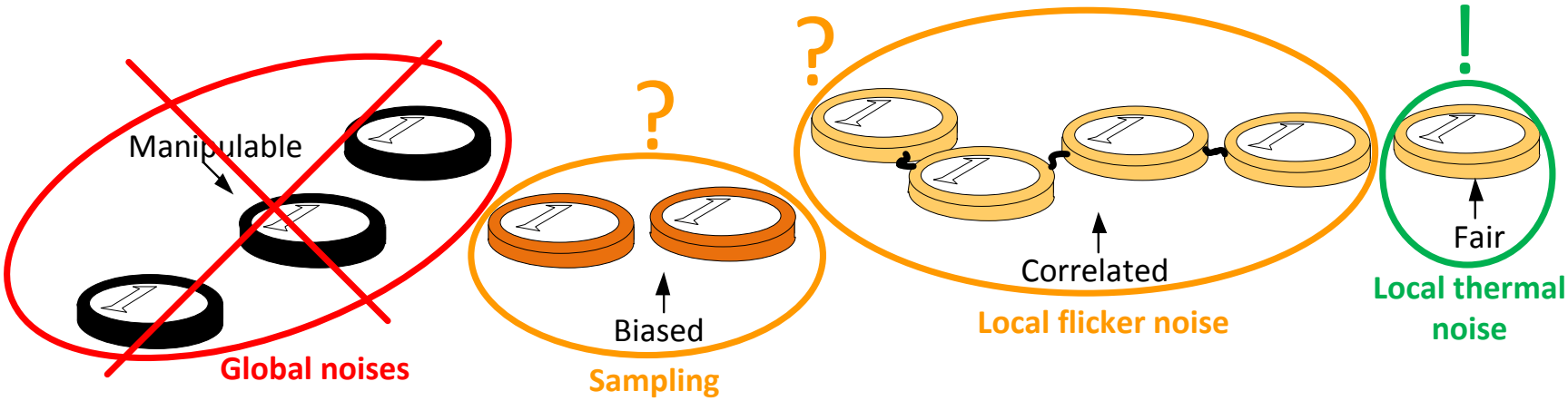


- How much entropy per trial, if:
  - One (independent) fair coin
  - Four correlated coins
  - Two biased coins
  - Three manipulable coins
- Can the output be manipulable, if the ten coins' values are bit-wise XORed to get **just one output bit?**

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Tossing (Partially) Unfair Coins – Realistic TRNG

In the context of oscillator based TRNG:



- How much entropy per trial, if:
  - One (independent) fair coin
  - Four correlated coins
  - Two biased coins
  - Three manipulable coins
- Can the output be manipulable, if the ten coins' values are bit-wise XORed to get **just one output bit?**

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Conclusions Regarding Our Study Case

- Design of a TRNG is rather a physical than a mathematical project
- Physical parameters of the sources of randomness must be thoroughly evaluated:
  - Characteristics of each exploited source of randomness
  - Relationship between individual sources of randomness
  - Distribution of output random values (bias)
  - Correlation or even dependence between output values
  - Manipulability
  - Agility (spectrum)

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Random Number Generation and Security

- Two main security requirements on RNGs:
  - R1: Good statistical properties of the output bitstream
  - R2: Output unpredictability
- Statistical properties can be easily evaluated using general purpose (black box) statistical tests
- Unpredictability is more difficult to assess
  - In PRNGs guaranteed by the underlying algorithm – it must be computationally difficult to guess future and past random numbers
    - Approved cryptographic algorithm should be used
  - In TRNGs guaranteed by a sufficient entropy rate per generated random number
    - Approved design approach should be used

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Classical versus Modern TRNG Design Approach

- Recall – two main security requirements on TRNGs:
  - R1: Good statistical properties of the output bitstream
  - R2: Output unpredictability

- Security evaluation – classical approach:
  - Assess both requirements using statistical tests – insufficient

- Modern (more stringent) ways of assessing security:
  - Evaluate statistical parameters using statistical tests
  - Evaluate entropy using an entropy estimator (stochastic model)
  - Test online the source of entropy using dedicated statistical tests

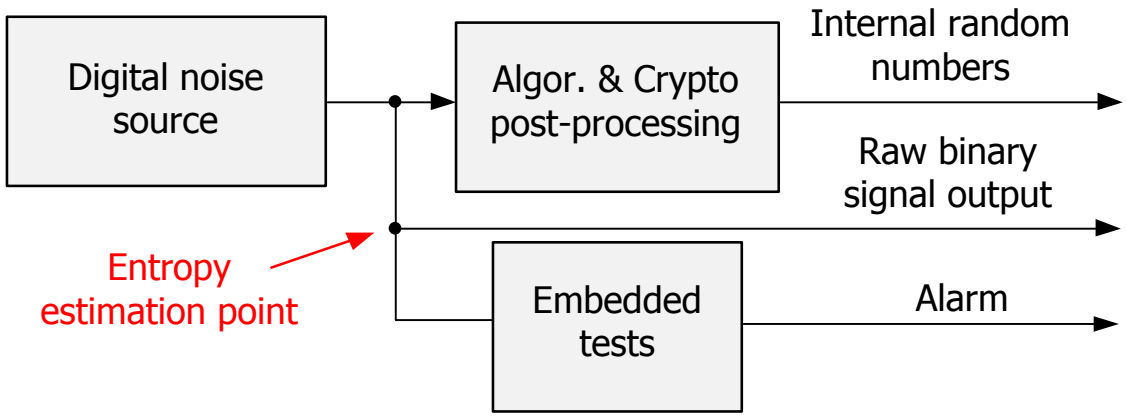
Objectives of the talk

- To discuss modern approaches in the TRNG design
- To illustrate the new methodology on a comprehensive example

Outline

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Contemporary TRNG Design – Recommendations AIS 31



- Digital noise source
  - Should have as high entropy rate per bit as possible
  - Should enable sufficient bit-rate
  - Shouldn't be manipulable (robustness)
- Post-processing (optional)
  - Algorithmic – enhances statistics without reducing the entropy
  - Cryptographic – for unpredictability when source of entropy fails
- Dedicated embedded tests
  - Fast total failure test with low probability of false alarms
  - Online tests detecting quickly and reliably intolerable weaknesses

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

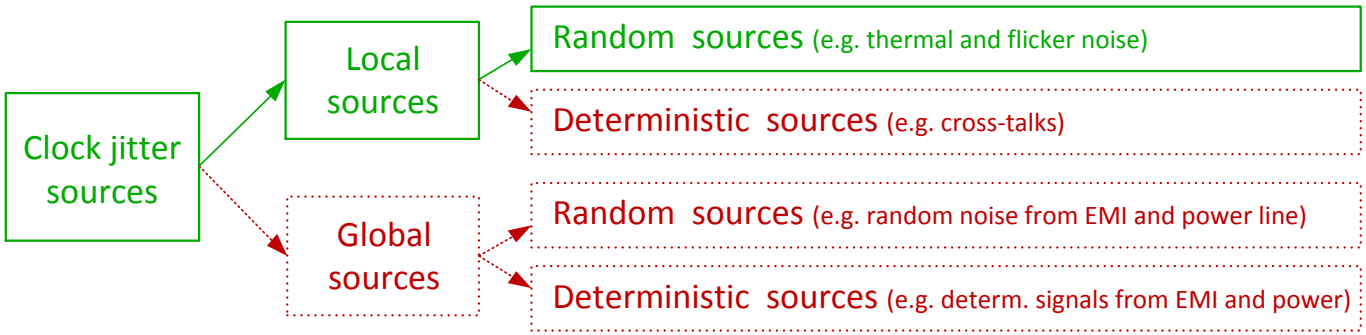
Sources of Randomness in Logic Devices

- Commonly used sources related to some physical process, **basically coming from electric noises**
  - **Clock jitter**: short-term variation of an event from its ideal position
  - **Metastability**: ability of an unstable equilibrium electronic state to persist for an indefinite period in a digital system (rare)
  - **Oscillatory metastability**: ability of a bi-stable circuit (e.g. an RS flip-flop) to oscillate for an indefinite period
  - **Initialization of flip-flops**: initialization of a flip-flop (or a memory element) to a random state (after power-up or periodically)
  - **Chaos**: stochastic behavior of a deterministic system which exhibits sensitive dependence on initial conditions

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Sources of Randomness: Jittery Clock Signals

- Clock jitter – the most frequently used in logic devices
- The jitter in clock generators is caused by [1]
  - Local noise sources
  - Global noise sources



- **Sources in red are manipulable!**
- **The entropy must be estimated depending on the local non-manipulable sources (in green)**

[1] B. Valtchanov, A. Aubert, F. Bernard, and V. Fischer, Modeling and observing the jitter in ring oscillators implemented in FPGAs, DDECS 2008

Choice of the Source of Randomness

- The source of randomness must be **clearly defined, well characterized and quantified**
- With respect to the entropy harvesting method, it should serve as an **input parameter of the stochastic model**
- Problem #1: False entropy source
  E.g. while claiming to use metastability, the designer uses some other, uncharacterized source of entropy (electric noises)
- Problem #2: **Entropy overestimation**
  The effect of manipulable sources is not excluded from entropy estimation – the general purpose statistical tests are not able to exclude them!

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Digitization of the Noise Signal

- **Explicite**
  - Sampling of a noisy signal
  - Counting of random events
  - Time-to-digital conversion
- **Hidden** (or implicite)
  - Conversion of analog electric noises to the timing jitter of the clock signal
- Sometimes it is difficult or even **impossible to separate** digitization from the post-processing
- If the digitization is hidden or if it is mixed with the post-processing, the **raw random signal – difficult to determine**

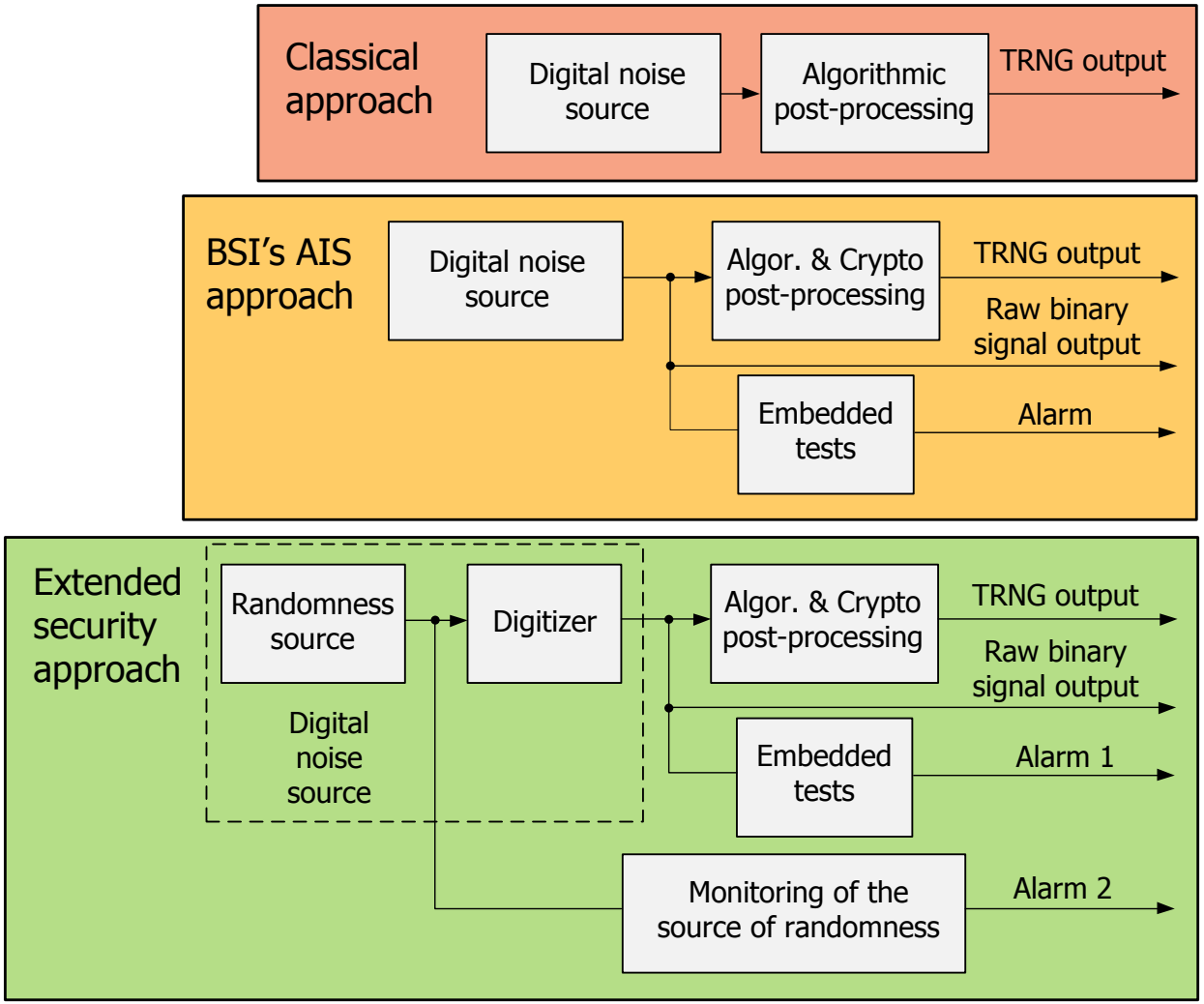
LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Outline

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Secure TRNG Design – Evolution

- TRNG designs should continue to evolve towards security:

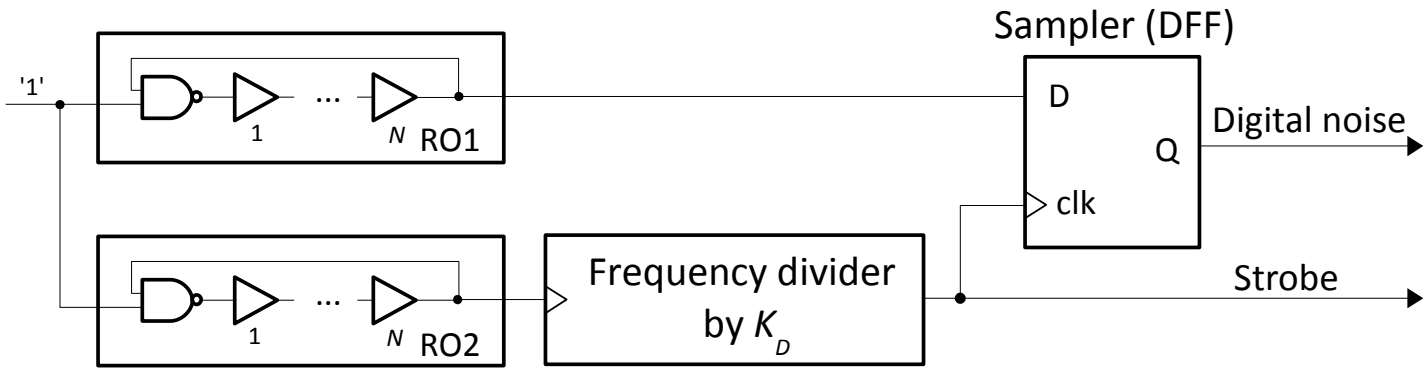


Characterization and Quantification of Noise Sources

- All the sources (and only the sources) that determine the entropy rate at generator's output need to be characterized and quantified
- Consequently, the noise sources should be characterized and quantified with respect to the stochastic model, which determines the entropy rate
- Next, we will illustrate this approach on a comprehensive example using an elementary oscillator-based TRNG ...

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Elementary Oscillator-Based TRNG (ELO TRNG)



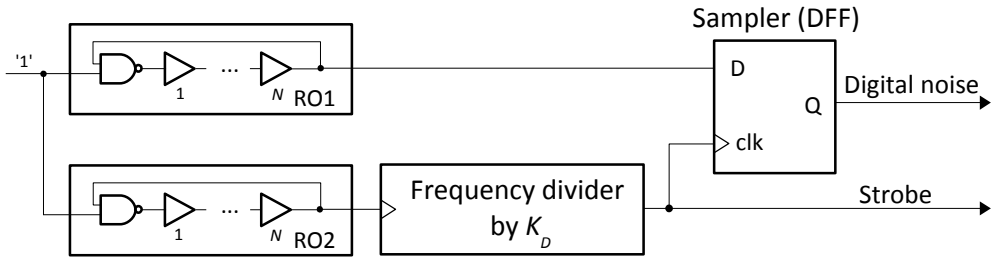
- First proposed by Fairfield *et al.* [1]
- Modeled by Baudet *et al.* [2] – the entropy depends on the clock jitter coming from the **thermal noise** and the frequencies of the two clock signals
- The frequency divider determines the sampling period
- Depending on the jitter size, the K_D value can be very big (greater than 300 000)

[1] R.C. Fairfield, R.L. Mortenson, and K.B. Coulthart. An LSI random number generator (RNG). Advances in Cryptology, 1985

[2] M. Baudet, D. Lubicz, J. Micolod, and A. Tassiaux. On the security of oscillator-based random number generators. Journal of Cryptology, 2011

LABORATOIRE HUBERT CURIEN

ELO TRNG – Security Analysis



- The effect of the global jitter sources (often neglected!) is significantly reduced by the principle – two identical oscillators are impacted in the same way by the global perturbation signals
- According to the model, the *lower bound of the Shanon entropy rate* per bit at the generator output is given as:

$$H_{min} \approx 1 - \frac{4}{\pi^2 \ln(2)} e^{-4\pi^2 Q} = 1 - \frac{4}{\pi^2 \ln(2)} e^{\frac{-4\pi^2 \sigma_{jit}^2 T_2}{T_1^3}} \quad (1)$$

The lower entropy bound is determined by measurable parameters!

- Mean frequencies of the two ring oscillators – T_1, T_2
- Variance of the jitter coming from the **thermal noise** – σ_{jit}^2

Measurement of the Non-Manipulable Clock Jitter 1/2

Algorithm for computing variance V of the jitter[1]

- **Input**: The output sequence $[b_1, \ldots, b_n]$ of an elementary TRNG with $K_D = 1$, K, M and N integers [2],
- **Output**: $V_0 = 4V/T_1^2$ where V is the variance of the jitter accumulated during MT_2.

Algorithm 1

for $i = 0, \ldots, K$ **do**

$S_i \leftarrow [Ni + 1, \ldots, Ni + N]$;

$c[i] = \mathbb{P}_{S_i}(b_j \neq b_{j+M})$;

end for;

$V_0 \leftarrow \frac{1}{K}\sum_{i=0}^{K} c[i]^2 - \left(\frac{1}{K}\sum_{i=0}^{K} c[i]\right)^2$;

return: V_0;

[1] V. Fischer and D. Lubicz. Embedded evaluation of randomness in oscillator based elementary TRNG. CHES 2014

[2] In practice, $K \sim 10000$, $N \sim 100$ and $M > N$, we let $M \sim 200 \div 1600$

LABORATOIRE HUBERT CURIEN

Measurement of the Non-Manipulable Clock Jitter 2/2

Algorithm 1 – Recall

for $i = 0, \ldots, K$ **do**

$S_i \leftarrow [Ni+1, \ldots, Ni+N]$;

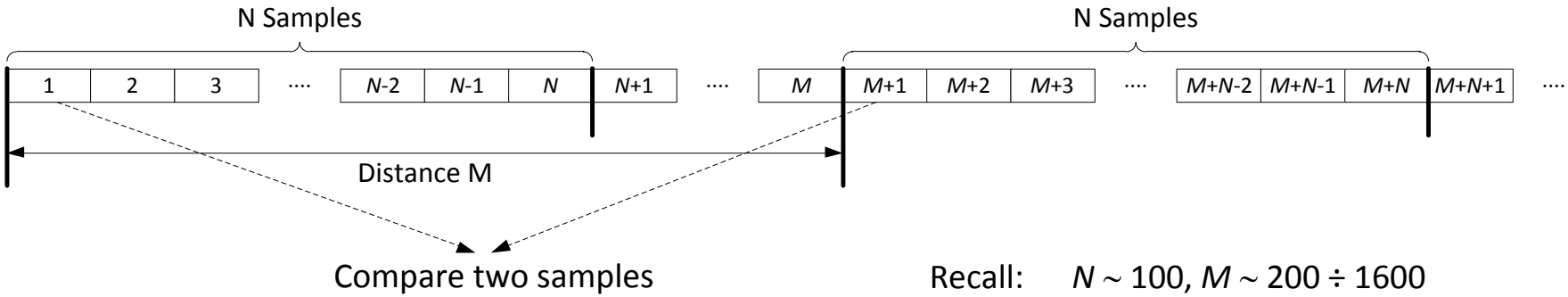
$c[i] = \mathbb{P}_{S_i}(b_j \neq b_{j+M})$;

end for;

$V_0 \leftarrow \frac{1}{K}\sum_{i=0}^{K} c[i]^2 - \left(\frac{1}{K}\sum_{i=0}^{K} c[i]\right)^2$;

return: V_0;

- For all elements from the set S_i compute $c[i] = \frac{\#\{j \in S_{i_0} \,|\, b_j \neq b_{j+M}\}}{N}$

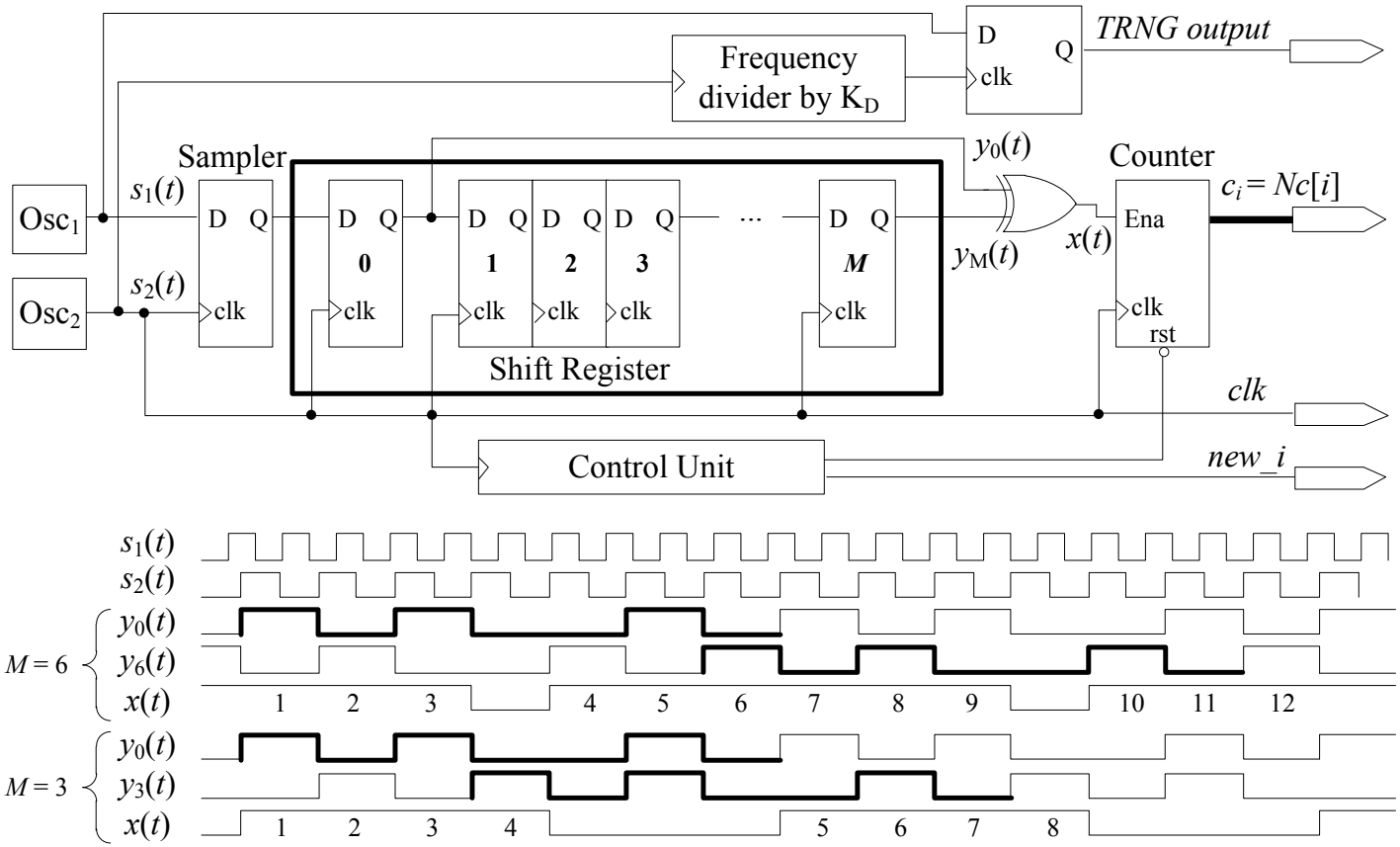


Recall: $N \sim 100$, $M \sim 200 \div 1600$

LABORATOIRE HUBERT CURIEN

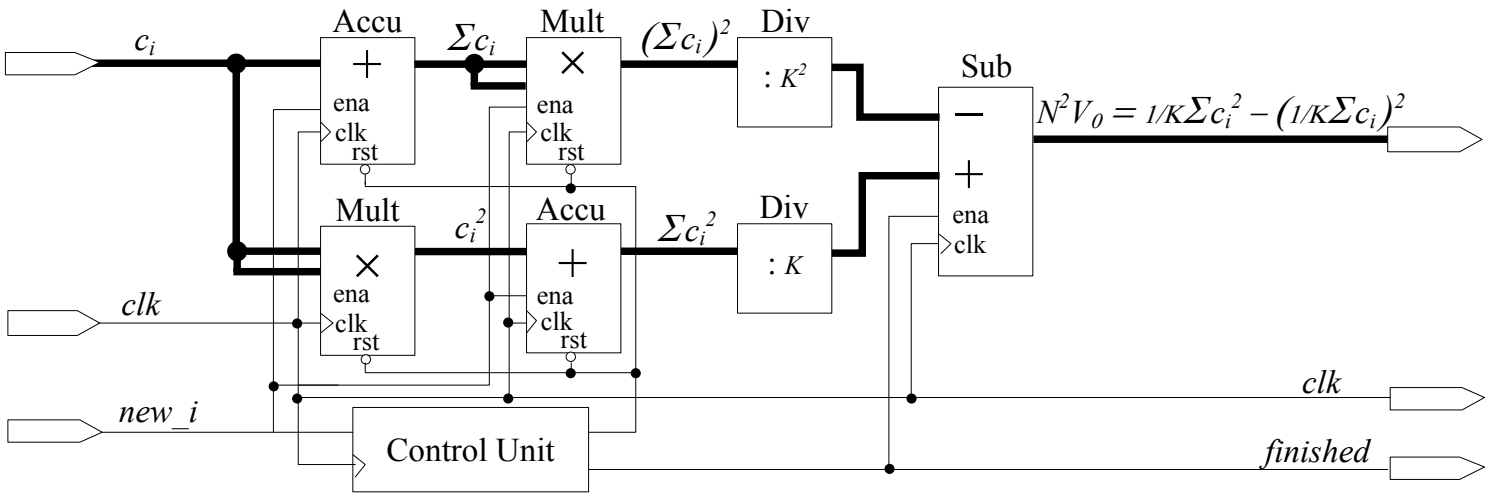
Hardware Implementation of the Jitter Measurement 1/2

- Jitter measurement circuitry implemented in two blocks
- The first block computes K successive values $c_i = Nc[i]$



Hardware Implementation of the Jitter Measurement 2/2

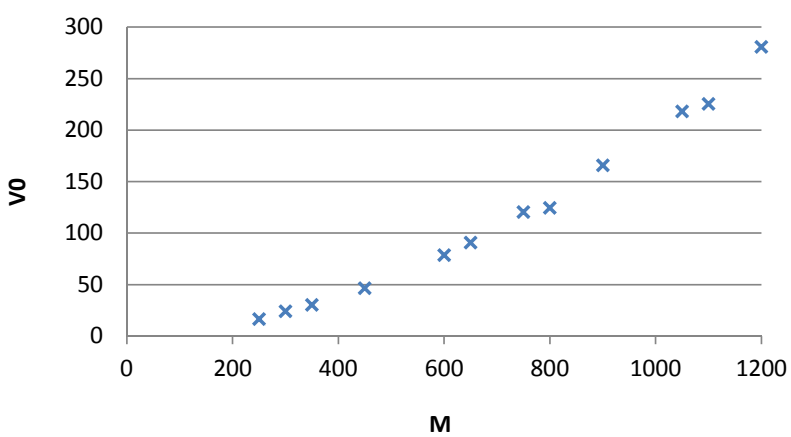
- Recall: Jitter measurement circuitry implemented in two blocks
- The second block computes the relative variance $4V/T_1^2$ from K values $c[i]$ according to Algorithm 1

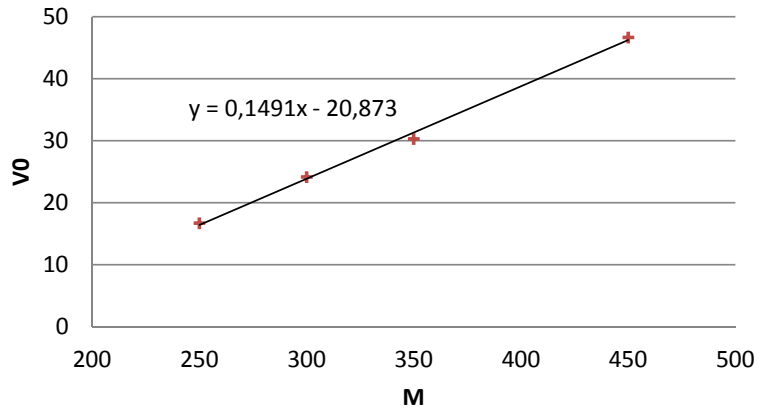


- Summary: Two accumulators, two multipliers, one subtractor, two divisions by shifting right

Evaluation of the Jitter Measurement in Hardware

- Implementation results in Altera Cyclone III FPGA module
  - The ELO TRNG including jitter measurement circuitry with 32-bit data path occupied:
    - 301 logic cells (LEs),
    - up to 450 memory bits,
    - one DSP block 9x9,
    - four DSP blocks 18x18
- Jitter measurement results ($250 < M < 1200$, $N \sim 120$ and $K = 8192$)





  - From the slope of the measured V_0 for $250 < M < 450$: **Jitter size**: $\sigma = 5.01$ ps per period $T_1 = 8.9$ ns.

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Outline

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Monitoring of the Source of Randomness

- Monitoring = continuous quantification (embedded measurement) of the noise source
- The measurement should be performed as close to the source as possible (reduced latency)
- The impact of the manipulable sources on the measurement results should be avoided
- The quantified source of randomness should be used
  - As an input for the **stochastic model** for entropy estimation
  - As a basis for the **dedicated stochastic tests** – fast and efficient

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Model-Based Entropy Management 1/2

For the previous example:

- Knowing the size of the jitter, we can now manage the entropy rate at the TRNG output:
  - From Eq. (1), we compute the value of the frequency divider K_D, to ensure that the entropy per bit will always be higher than $H_{min} = 0.997$:

$$K_D > \frac{-\ln\left(\frac{\pi}{2}\sqrt{(1-H_{min})\ln(2)}\right)}{2\pi^2 \frac{T_2}{T_1}\frac{\sigma^2}{T_1^2}}$$

- For $T_1 = 8.9$ ns, $T_2 = 8.7$ ns, $\sigma = 5.01$ ps and $H_{min} = 0.997$, we get $K_D \approx 430\,000$

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

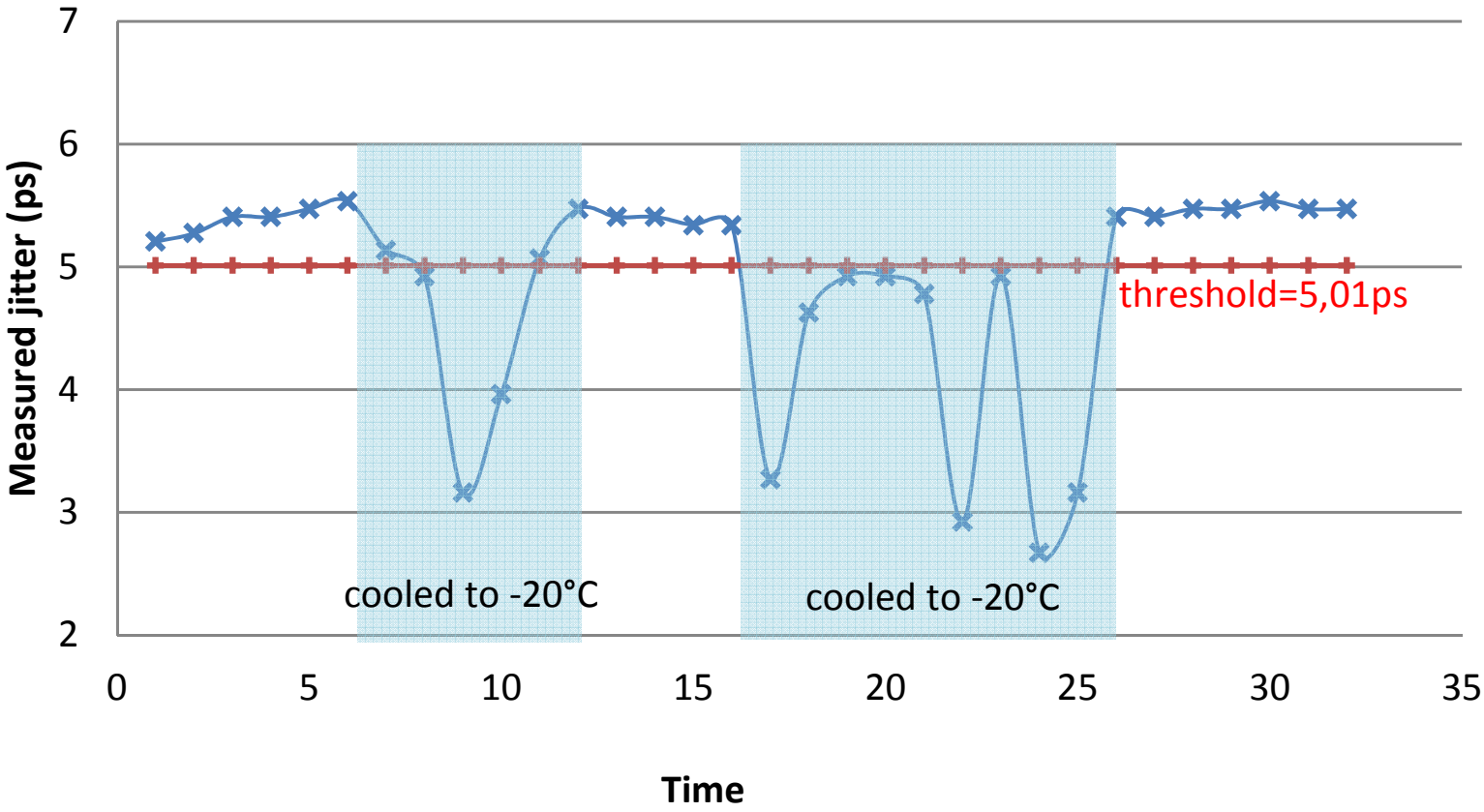
Model-Based Entropy Management 2/2

- **The jitter measurement circuitry can serve for online testing**: for the given K_D, the jitter size σ_c should not drop below 5.01 ps, in order to **guarantee sufficient entropy rate at TRNG output**
- The proposed dedicated test needs $N \cdot K = 128 \cdot 8192 \approx 1 \cdot 10^6$ periods T_2 to be finished = **less than 3 TRNG output bits!**
- We observed that the proposed embedded test is **much more conservative** than the tests FIPS 140-1 – the TRNG output passed these tests (and even the tests NIST SP 800-22) for $K_D > 100\,000$
- **It is sufficient to put a 3-element shift register at the TRNG output, in order to get each output bit continuously tested**

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Evaluation of the Method by Attacks

- Studied attack – jitter reduction by decreasing the temperature
  - The temperature was rapidly changed to $-20\,^{\circ}\mathrm{C}$ and left to rise back to $21\,^{\circ}\mathrm{C}$ for several times.



Outline

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Conclusion – TRNGs Suitable for Source Monitoring

- To comply with the proposed principle of randomness monitoring, the TRNGs must fulfill the following conditions:
  - Their stochastic model must be feasible
  - The model must depend on measurable inputs
- Not all TRNGs comply with this principle, but many of them do, e.g.:
  - Generators with uniformly distributed clock phases [1]
  - TRNGs with periodically occurring clock phases (coherent sampling)[2] [3]
  - Generators with a transitional oscillatory state [4]

[1] A. Cherkaoui,V. Fischer, L. Fesquet, A. Aubert: A Very High Speed True Random Number Generator with Entropy Assessment, CHES 2013

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

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

[4] M. Varchola, M. Drutarovsky: New High Entropy Element for FPGA Based True Random Number Generators, CHES 2010

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Conclusions

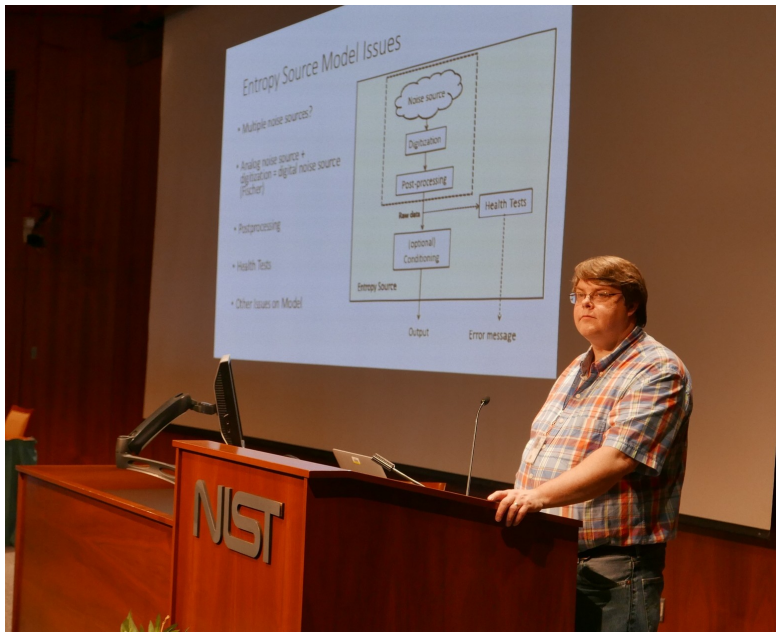
- We demonstrated that in conjunction with a suitable statistical model, the quantified noise source can be **used to estimate entropy** at the output of the generator
- We also showed that this entropy estimator can be used to build a **rapid dedicated on-line statistical test** that is perfectly adapted to the generator's principle
- This approach ensures **high level of security** by rapidly detecting all deviations from the expected behavior

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

During the NIST RBG workshop in Washington in May 2016

Position of NIST:

- No set of general-purpose statistical tests can measure the entropy per sample in an arbitrary sequence of values
- Right way to build a noise source is:
  - Design your noise source
  - Understand it
  - Model it
  - Use your model to estimate entropy
  - Run G-P tests as sanity check
- We require design documentation and an entropy estimate from designer to support this...
- ...but we're limited in what resources we can demand for validation testing, and what expertize we can require from labs.



John Kelsey
NIST SP 800-90 Manager
NIST, USA

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE

Acknowledgments

This work was performed in the framework of the project

HECTOR

Hardware Enabled Crypto and Randomness

The HECTOR project has received funding from the
European Union's Horizon 2020 research and innovation programme
under grant agreement number 644052 starting from March 2015

www.hector-project.eu

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT-ETIENNE