Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG

Viktor FISCHER
Jean Monnet University Saint-Etienne, France

David LUBICZ
DGA-Maitrise de l'information, France
Université de Rennes 1, Rennes, France

CHES 2014 – Busan, Korea

July 2014

Random Numbers in Cryptography

- Random number generators constitute an essential part of (hardware) cryptographic modules
- They generate random numbers that are used as:
  - Cryptographic keys
  - Masks in countermeasures against side channel attacks
  - Initialization vectors, nonces, padding values, ...

Classical versus Modern TRNG Design Approach

- Two main security requirements on RNGs:
  - R1: Good statistical properties of the output bitstream
  - R2: Output unpredictability
- Classical approach:
  - Assess both requirements using statistical tests – often impossible
- Modern ways of assessing security:
  - Evaluate statistical parameters using statistical tests
  - Evaluate entropy using entropy estimator (stochastic model)
  - Test online the source of entropy using dedicated statistical tests

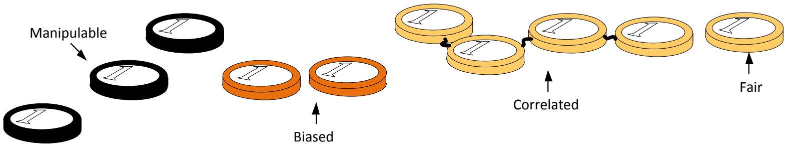
Our objectives

Propose jitter measurement method that can be

- Easily embedded in logic devices
- Used for entropy assessment based on existing stochastic model [a]

[a] M. Baudet *et al.*, On the Security of Oscillator-Based Random Number Generators, Journal of Cryptology, 2011

Tossing (Partially) Unfair Coins – Realistic TRNG



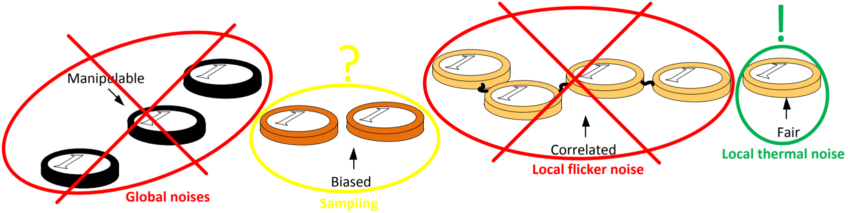
- How much entropy per trial, if:
  - One (independent) fair coin
  - Four correlated coins
  - Two biased coins
  - Three manipulable coins
- Can the output be manipulable, if the ten coins values are bit-wise XORed in order to get one output bit?

DGA

LABORATOIRE Hubert CURIEN UMR • CNRS • 5516 • ST-ETIENNE

Tossing (Partially) Unfair Coins – Realistic TRNG

In the context of oscillator based TRNG:



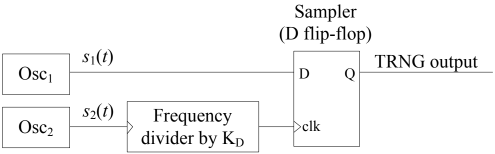
- How much entropy per trial, if:
  - One (independent) fair coin
  - Four correlated coins
  - Two biased coins
  - Three manipulable coins
- Can the output be manipulable, if the ten coins values are bit-wise XORed in order to get one output bit?

Outline

Outline

Elementary oscillator based TRNG

- Principle

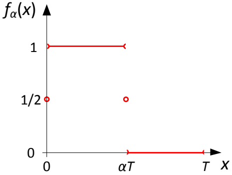


where

- $s_i(t) = f(\omega_i(t + \xi_i(t))), i = 1, 2$ are two jittery clock signals,
- ω_1 and ω_2 are their mean frequencies,
- $\xi_1(t)$ and $\xi_2(t)$ represent their absolute phase drifts,
- $\zeta = \omega_1 / \omega_2$ is the relative mean frequency.

Function f_α – specific T-periodic function

- $f_\alpha(x) = 1$ for all $0 < x < \alpha T$
- $f_\alpha(x) = 0$ for all $\alpha T < x < T$
- $f_\alpha(0) = f_\alpha(\alpha T) = 1/2$



Assumed properties of the clock signals 1/2

- Osc_1 is a perfectly stable oscillator ($\xi_1 = 0$)
- All the phase drift comes from Osc_2, we want to characterize the phase jitter $\xi_2 = \xi$
- According to Baudet *et al.* [1], the random walk component of the phase evolution can be modeled by an ergodic stationary Markov process
  - If the Markov process is Gaussian, it is completely determined by the variance $V(\Delta t)$, where $\Delta t = t - t_0$
  - The random walk component is produced by noise sources which affect each transition *independently*, therefore $V(\Delta t) = \sigma_0^2 \Delta t$

[1] M. Baudet *et al.*, On the Security of Oscillator-Based Random Number Generators, Journal of Cryptology, 2011

Assumed properties of the clock signals 2/2

- We consider existence of $1/f^{\beta}$ noises, where $0 < \beta < 2$, as they also contribute to phase jitter

$1/f^{\beta}$ noises are autocorrelated:

- They are not taken into account in the stochastic model used for entropy estimation
- They must not contribute to the size of the measured jitter – we wish to measure only the random walk component of the phase evolution

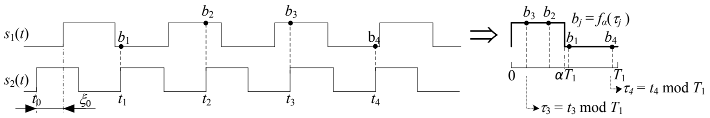
Global noises are manipulable:

- We do not consider the impact of the global noise sources on the jitter measurement – this impact is significantly reduced because of the differential EO TRNG principle

Outline

Principle of the embedded jitter measurement 1/5

- We wish to measure the variance $V(\Delta t)$ from knowledge of an output bit sequence of an elementary oscillator-based TRNG with $K_D = 1$
- Relation between the sampling process and function $f_\alpha(\cdot)$:



where $x_j \mod T_i$ is the modulo operation on real numbers

Principle of the embedded jitter measurement 2/5

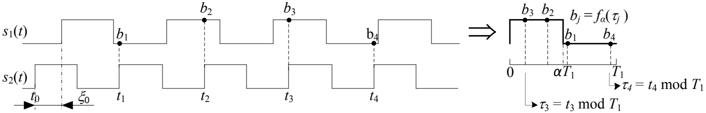
- **Definition of ε-uniformity**:

Distribution of samples $\{(jT_2 - \xi(t_j)) \mod T_1\}_{j \in J}$ is ε-uniform, if for all $[a, b]$:

$$\left| \frac{\#\{j \in J | (jT_2 - \xi(t_j)) \mod T_1 \in [a,b]\}}{\#J} - \frac{b-a}{T_1} \right| < \varepsilon.$$

  - Number of samples in interval $[a, b]$ inside the translated period T_1, over the number of samples in subset J is ε-close to the size of interval $[a, b]$ over period T_1.

- Recall the right side of the previous figure:



Principle of the embedded jitter measurement 3/5

Fact 1 (proof given in the paper)

- For an ε-uniform set of samples, we define

$$\mathbb{P}_{S_{i_0}}\{b_j \neq b_{j+M}\} = \frac{\#\{j \in S_{i_0} | b_j \neq b_{j+M}\}}{\#S_{i_0}}.$$

- If $(MT_2 + \xi(t_{i_0}) - \xi(t_{i_0+M})) \mod T_1 \leq \min(\alpha T_1, (1-\alpha)T_1)$ then

$$\left| \mathbb{P}_{S_{i_0}}\{b_j \neq b_{j+M}\} - \left(\frac{2(MT_2 + \xi(t_{i_0}) - \xi(t_{i_0+M}))}{T_1} \mod 1 \right) \right| < \varepsilon,$$

- If $(MT_2 + \xi(t_{i_0}) - \xi(t_{i_0+M})) \mod T_1 \geq \max(\alpha T_1, (1-\alpha)T_1)$ then

$$\left| \mathbb{P}_{S_{i_0}}\{b_j \neq b_{j+M}\} + \left(\frac{2(MT_2 + \xi(t_{i_0}) - \xi(t_{i_0+M}))}{T_1} \mod 1 \right) \right| < \varepsilon,$$

- otherwise

$$\left| \mathbb{P}_{S_{i_0}}\{b_j \neq b_{j+M}\} - 2\min(\alpha, 1-\alpha) \right| < \varepsilon.$$

Principle of the embedded jitter measurement 4/5

Algorithm for computing variance V of the jitter

- **Input**: The output sequence $[b_1, \ldots, b_n]$ of an elementary TRNG with $K_D = 1$, K, M and N integers [1],
- **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] In practice, $K \sim 10000$, $N \sim 100$ and $M > N$, we let $M \sim 200 \div 1600$

Principle of the embedded jitter measurement 5/5

Algorithm 1 – Recall

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

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

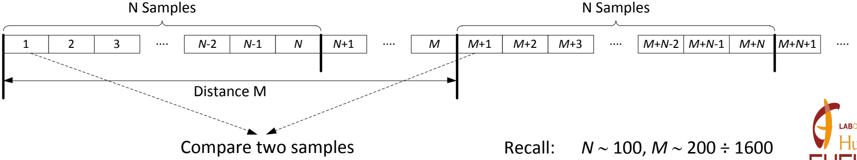
  $c[i] = \mathbb{P}_{S_i}(b_j \neq b_{j+M})$;

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 $c[i] = \frac{\#\{j \in S_{i_0} | b_j \neq b_{j+M}\}}{N}$

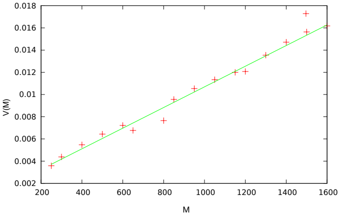


Recall: $N \sim 100$, $M \sim 200 \div 1600$

Evaluation of the method by simulations

- **Objective** – recover the jitter size that was indeed introduced to generated clocks, independently from the frequency ratio

- Two clock signals generated: $T_1 = 8\,923$ ps and $T_2 = 8\,803$ ps
- Using the rng.pkg package, Gaussian jitter sequences with σ_c = 10 ps, 15 ps, and 20 ps were generated and injected to two clocks
- EO TRNG output bit sequences were used for computing the jitter variance
- Error smaller than 5 % was observed



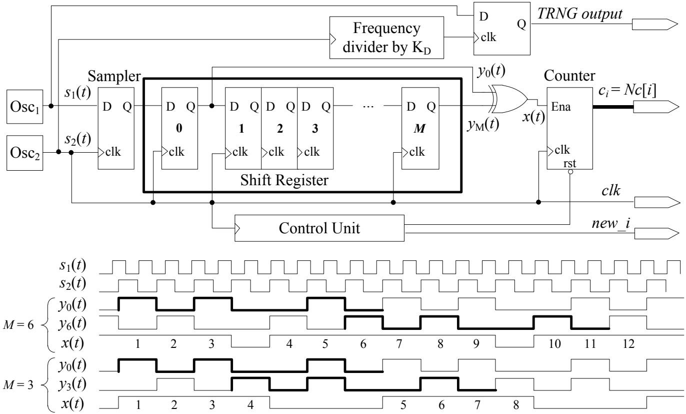
Injected jitter σ_c	Calculated slope a	σ_c/T_1	$\sqrt{a}/2$	Error percentage
10 ps	9.299909 10^{-6}	0.00156	0.00152	2 %
15 ps	2.03211 10^{-5}	0.00234	0.00225	3 %
20 ps	2.03211 10^{-5}	0.00312	0.00297	5 %

DGA

LABORATOIRE Hubert CURIEN UMR • CNRS • 5516 • ST-ETIENNE

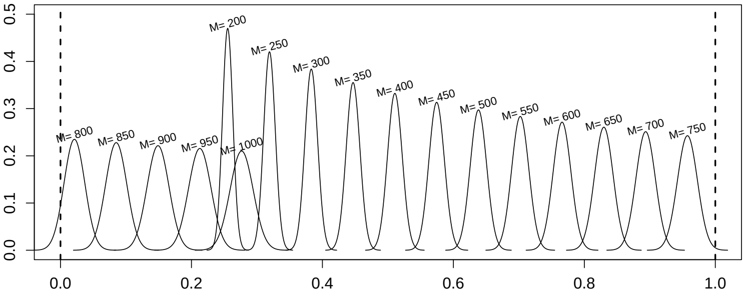
Hardware implementation of the jitter measurement 1/3

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



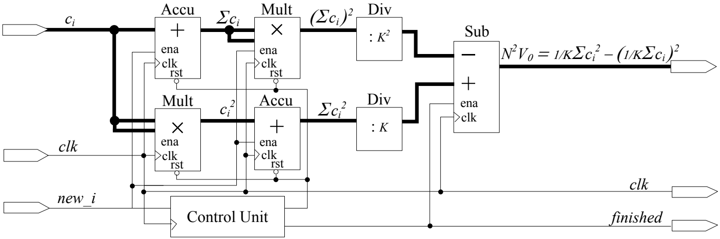
Hardware implementation of the jitter measurement 2/3

- **Important remark**:
  - For some values of M, measured values $c_i = Nc[i]$ are incorrect (e. g. for $M = 750$ and $M = 800$ in the figure below)
  - These values are easy to detect – they must not be taken into account in variance computations



Hardware implementation of the jitter measurement 3/3

- 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

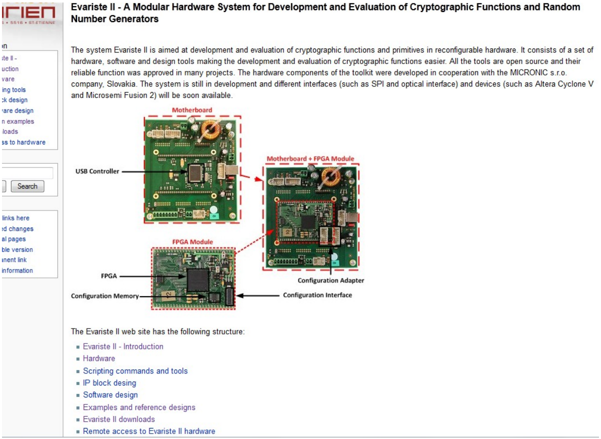


- Summary: Two accumulators, two multipliers, one subtractor, two divisions by shift right

Evaluation of the jitter measurement in hardware 1/2

Evariste II system – A Modular Hardware System for Design and Evaluation of Cryptographic Functions and TRNG (Open-source!)

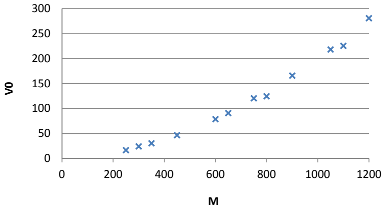
http://labh-curien.univ-st-etienne.fr/wiki-evariste-ii/index.php/Main_Page

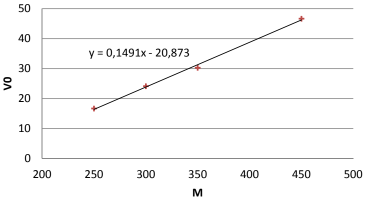


Evaluation of the jitter measurement in hardware 2/2

- Implementation results in Altera Cyclone III FPGA module
  - The EO 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**: $\sigma = 4.8$ ps per period $T_1 = 7.81$ ns.

Outline

Simplified jitter measurement

- Computing the jitter size from the slope is not suitable for hardware implementation
- Knowing that the dependence in the selected interval is linear, we can measure just one point of the curve, i. e. just one value $V_0 = 4V/T_1^2$ (e. g. for $M = 300$)
- The measured standard deviation was $\sigma_0 = 2\sqrt{V}/T_1$ = 5.01 ps

Important remarks

- The variance should not be computed for values M (not known in advance), whose mean values $c[i]$ are close to zero or one
- If the jitter is sufficiently small compared to the T_1 period, these cases are rare
- Solution: The shift register has several outputs around stage 300 => select M, for which $c[i]$ are close to 0.5

Model-based embedded entropy management

- We can now manage entropy rate at generator output:
  - By entering the known jitter size in the model presented in [1], we compute the value of frequency divider K_D, to ensure that the entropy per bit is higher than $H_{min} = 0.997$, according to the next expression:

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

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

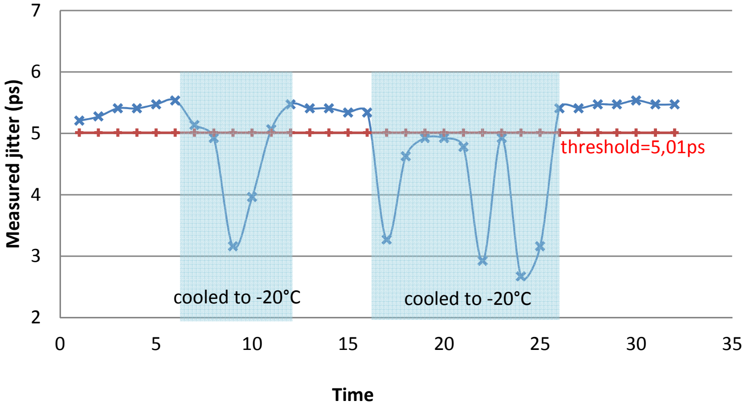
[1] M. Baudet *et al.*, On the Security of Oscillator-Based Random Number Generators, Journal of Cryptology, 2011

Discussion

- **The jitter measurement circuitry can serve for online testing**: for the given K_D, the jitter size σ_c shouldn't drop below 5.01 ps, in order to guarantee sufficient entropy rate at TRNG output
- The proposed dedicated test needs $N \cdot K = 120 \cdot 8192 = 1 \cdot 10^6$ periods T_2 to be finished = **less then 3 TRNG output bits!**
- Tests FIPS 140-1 would need 20,000 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 $K_D > 100,000$ (probably because the flicker noise).
- **It is sufficient to put three flip-flops at the TRNG output (delay), in order to get each output bit continuously tested.**

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

Conclusions

- We presented an original, simple and precise **method of jitter measurement** implementable in logic devices
- We demonstrated that in conjunction with a suitable statistical model, the measured jitter can be **used to estimate entropy** at the output of the generator
- We also showed that the proposed 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 **complies with AIS31** and ensures a **high level of security** by rapidly detecting all deviations from correct behavior

DGA

LABORATOIRE Hubert CURIEN UMR • CNRS • 5516 • ST-ETIENNE

Embedded Evaluation of Randomness in Oscillator Based Elementary TRNG

Viktor FISCHER
Jean Monnet University Saint-Etienne, France

David LUBICZ
DGA-Maitrise de l'information, France
Université de Rennes 1, Rennes, France

CHES 2014 – Busan, Korea

July 2014