(New) Challenges in Random Number Generation for Cryptography

Viktor FISCHER

Laboratoire Hubert Curien, UMR 5516 CNRS
Jean Monnet University, Member of University of Lyon
Saint-Etienne, France

fischer@univ-st-etienne.fr

Workshop on Randomness and Arithmetics for Cryptography on Hardware, April 2019

Basic RNG classes

- **Deterministic** (Pseudo-) random number generators (PRNG)
  - Algorithmic generators
  - Usually faster, with good statistical properties
  - Must be computationally secure, i. e. it should be computationally difficult to guess the next or previous values
- **Physical** (True-) random number generators (TRNG)
  - Using some physical source of randomness
  - Unpredictable, usually having suboptimal statistical characteristics
  - Usually slower
- **Hybrid** random number generators (HRNG)
  - Deterministic RNG seeded repeatedly by a physical random number generator
  - True RNG with algorithmic (e. g. cryptographic) postprocessing

RNGs in logic devices

- RNGs – usually a part of a Cryptographic SoC $\Rightarrow$ in logic devices
- Logic devices (ASICs or FPGAs)
  - Aimed at implementation of deterministic systems
  - Designed so that the deterministic behavior dominates
  - Some analog blocks are sometimes available (PLL, RC-oscillator, A/D and D/A converters, etc.)

Challenge #1

Implementation of PRNGs in logic devices is straightforward ... but ...

... finding and exploiting correctly a robust physical source of randomness needed in TRNGs is a challenging task

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

Classical versus modern TRNG design approach

- Two main security requirements on RNGs:
  - R1: Good statistical properties of the output bitstream
  - R2: Output unpredictability

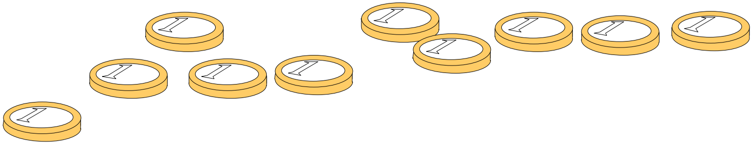
- Classical approach:
  - Assess both requirements using statistical tests – difficult
- Modern ways of assessing security:
  - Evaluate statistical parameters using statistical tests
  - Evaluate entropy using entropy estimator (stochastic model)
  - Test online the source of entropy using dedicated statistical tests

Objective of the talk

To show on practical examples

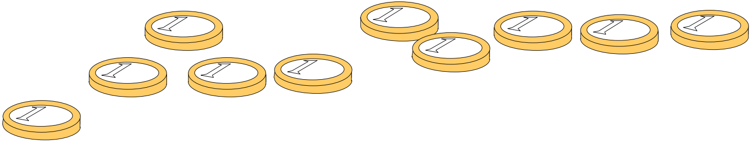
- Why the thorough security assessment is so important
- What are remaining challenges in TRNG design and evaluation

Fair tossing of fair coins – considered as an ideal TRNG 1/2



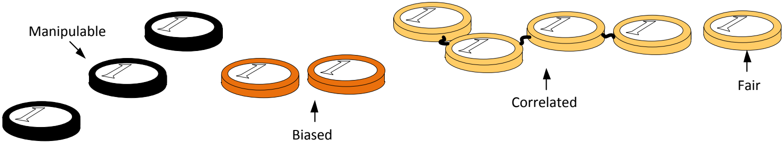
- How much entropy per trial, if ten coins are used?

Fair tossing of fair coins – considered as an ideal TRNG 2/2



- What can be the frequency of trials?
- Can you get 100 random bits per second, when using just ten coins?

Tossing (partially) unfair coins – realistic TRNG

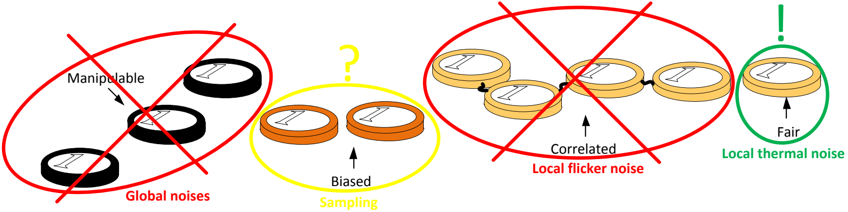


- How much entropy per trial, if:
  - One (independent) fair coin
  - Four correlated coins
  - Two biased coins
  - Three manipulable coins
- Can the output be manipulable, if the ten coins values are bit-wise XORed in order to get one output bit?

LABORATOIRE HUBERT CURIEN

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?

Conclusions regarding our study case

- Design of a RNG is rather a physical than a mathematical project
- The physical parameters of the source of randomness must be thoroughly evaluated:
  - Distribution of random values (bias)
  - Correlation
  - Dependence (if many sources)
  - Manipulability
  - Agility (spectrum)

Outline

1. Contemporary TRNG design challenges
   - Sources of randomness and entropy extraction methods
   - Stochastic models and entropy estimators
   - Postprocessing methods
   - Statistical tests – objectives and strategies

2. Security evaluation of RNGs in a certification process
   - Main approaches in RNG security certification
   - European AIS20/31 vs American NIST SP800-90

3. Conclusions

Outline

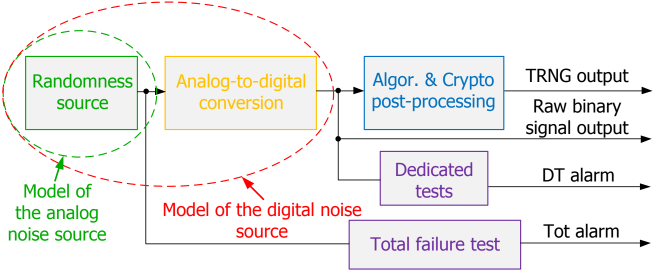
1. Contemporary TRNG design challenges
   - Sources of randomness and entropy extraction methods
   - Stochastic models and entropy estimators
   - Postprocessing methods
   - Statistical tests – objectives and strategies

2. Security evaluation of RNGs in a certification process
   - Main approaches in RNG security certification
   - European AIS20/31 vs American NIST SP800-90

3. Conclusions

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

Contemporary TRNG design



- Source of the digital noise
  - Should give as much entropy per bit as possible
  - Should enable sufficient bit-rate
  - Shouldn't be manipulable (robustness)
- Postprocessing
  - Algorithmic – enhances statistics without reducing the entropy
  - Cryptographic – for unpredictability when source of entropy fails
- Embedded tests
  - Fast total failure test with low probability of false alarms
  - Online tests detecting intolerable weaknesses

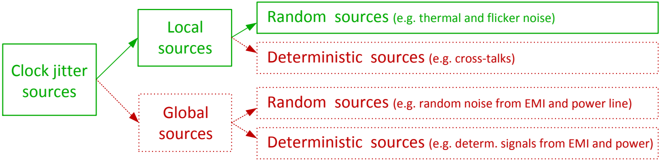
Sources of randomness in logic devices

- 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
  - **Oscillatory metastability**: ability of a bi-stable circuit (e.g. an RS flip-flop) to oscillate for an indefinite period
  - **Metastability**: ability of an unstable equilibrium electronic state to persist for an indefinite period in a digital system (rare)
  - **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 (needs analog blocks)

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

Sources of randomness: jittered 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!**

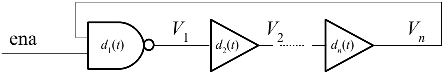
Challenge #2

Entropy should be estimated using only local non-manipulable uncorrelated sources (e.g. thermal noise)

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

Clock generators: Ring oscillators (ROs) 1/3

- Ring oscillators – single event oscillators [1]
  - One event (rising and falling edge) is propagated in the ring
  - Half period: sum of delays of individual ring elements
  - The most common free running oscillators in logic devices – easy to implement
  - Clock frequency easy to manipulate (temperature, power voltage) but not the jitter coming from the thermal noise



Challenge #3

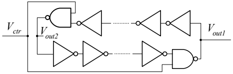
The clock jitter is caused by thermal noises but also by correlated low frequency noises, while the second tend to dominate

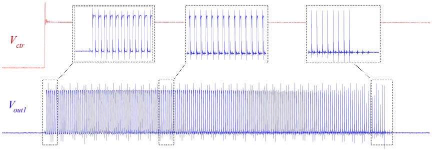
[1] V. Fischer, P. Haddad, and A. Cherkaoui, Ring Oscillators ans Self-Timed Rings in True Random Number Generators, in N. Yoshifumi (ed): Oscillator Circuits: Frontiers in Design, Analysis and Applications, IET 2016

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

Clock generators: Transition effect ring oscillators (TEROs) 2/3

- Two-event oscillators with collisions [1]
  - Easy to implement in logic devices
  - Two events (edges) are propagated in the ring until one reaches the second
  - Easy to convert to random numbers (number of periods)





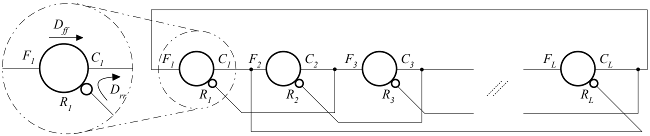
Challenge #4

Increase repeatability – number of periods (and thus entropy) differs significantly device by device

[1] V. Fischer, P. Haddad, and A. Cherkaoui, Ring Oscillators ans Self-Timed Rings in True Random Number Generators, in N. Yoshifumi (ed): Oscillator Circuits: Frontiers in Design, Analysis and Applications, IET 2016

Clock generators: Self-timed rings (STRs) 3/3

- Multi-event oscillators without collisions [1]
  - Using Muller cells – relatively easy to implement in logic devices
  - Several events (edges) are propagated in the ring – asynchronous logic avoids collisions
  - Frequency does not depend on number of ring elements



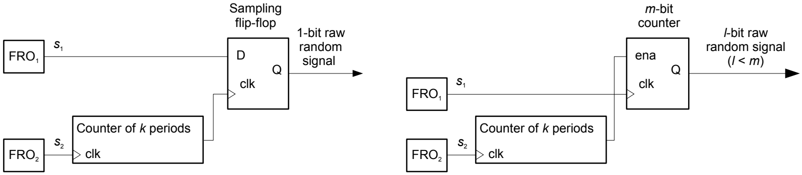
Challenge #5

Ensure the evenly-spaced mode (i.e. avoid the burst mode) to guarantee entropy

[1] V. Fischer, P. Haddad, and A. Cherkaoui, Ring Oscillators ans Self-Timed Rings in True Random Number Generators, in N. Yoshifumi (ed): Oscillator Circuits: Frontiers in Design, Analysis and Applications, IET 2016

Converting analog noises to a raw binary signal 1/3

- To eliminate global manipulable jitter sources, two identical free-running oscillators are used
- We compared two ways of randomness extraction [1]
  - Sampling the jittered clock signal
  - Counting periods of the jittered clock signal



Sampler based randomness extraction

Counter based randomness extraction

Challenge #6

- To find a RELIABLE method for extracting maximum entropy

[1] E.N.Allini et al., Evaluation and Monitoring of Free Running Oscillators Serving as Source of Randomness CHES 2018

Entropy Estimates from the 8-th order Markov chain model

Randomness extraction method: sampling the jittery clock

Jitter accumulation time	Markov chain	AIS 31 Procedure B	AIS 31 T8	NIST 800-90B	NIST 800-90B
Periods of s_2	min-entropy		Shannon entropy	IID	min-entropy
10 000	0.8102	failed	0.9844	non-IID	0.648
20 000	0.8105	failed	0.9851	non-IID	0.647
30 000	0.8102	failed	0.9847	non-IID	0.648
50 000	0.9369	failed	0.9992	non-IID	0.673
100 000	0.9012	failed	0.9935	non-IID	0.670

Randomness extraction method: counting the jittery clock periods

Jitter accumulation time	Markov chain	AIS 31 Procedure B	AIS 31 T8	NIST 800-90B	NIST 800-90B
Periods of s_2	min-entropy		Shannon entropy	IID	min-entropy
10 000	0.8089	failed	0.9966	non-IID	0.844
15 000	0.9769	passed	0.9998	non-IID	0.931
20 000	0.9865	passed	0.9999	IID	0.999
25 000	0.9907	passed	0.9999	IID	0.998
100 000	0.9910	passed	0.9999	IID	0.998

Conclusions regarding the digital noise source

- 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**
- The entropy harvesting method (digitization) must be **as efficient as possible** – the method using counter gives much better results
- Entropy should be **estimated using a stochastic model** – it cannot be measured

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

Stochastic models – objectives

- Stochastic model – definition:
  - Stochastic model – specifies a **family of probability distributions** that contains all possible distributions of the raw-random numbers
- Main objectives – characterize:
  - Probability of ones: $\Pr(X = 1)$
  - Probability of an n-bit vector: $\Pr(X_1 = x_1, X_2 = x_2, ..., X_n = x_n)$
  - ... and from them **the entropy**
- Two kinds of entropy can be evaluated:
  - **Entropy** – if exploited random variables are IID
  - **Conditional entropy** – if exploited random variables are non-IID

Challenge #7

- Propose a TRNG stochastic model based on some measurable parameters

Comprehensive example of a stochastic model

- Model of a free-running oscillators based elementary TRNG [1]
- 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
- Jitter variance per period T_1
- These measurements together with the model will constitute a basis for dedicated tests!

[1] M. Baudet *et al.*, On the security of oscillator-based random number generators. Journal of Cryptology, 2011.

Normal variance vs Allan variance 1/3

Normal variance – unbounded in the presence of low-frequency noises

- Estimate of the normal variance:

$$\sigma_y^2 = E(y^2) - E^2(y). \tag{2}$$

Allan variance – an average fractional frequency can be used

- Average frequency deviation $\overline{y}_k$ over a time interval of length τ
  - Corresponds to the fluctuations while counting the number of periods of the jittery signal over τ
- Estimate of the Allan variance:

$$\sigma_y^2(\tau) = \frac{1}{2(M-1)} \sum_{i=1}^{M-1} (\overline{y}_{i+1} - \overline{y}_i)^2. \tag{3}$$

$\hookrightarrow$ M : total number of $\overline{y}_k$'s.

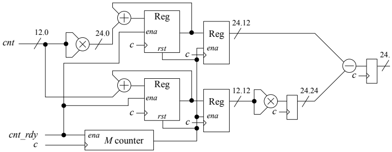
- For $\alpha = 0$, $\sigma_y^2(\tau)$ is an unbiased estimator of the variance even for a finite M

TOIRE
CURIEN
S • SAINT-ETIENNE

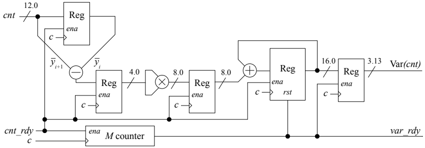
Normal variance vs Allan variance 2/3

Hardware implementations

- Statistical variance
- Allan variance



3 adders/subtractors, 2 multipliers

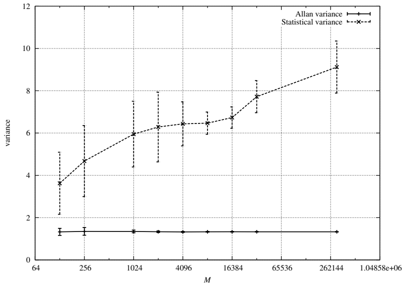


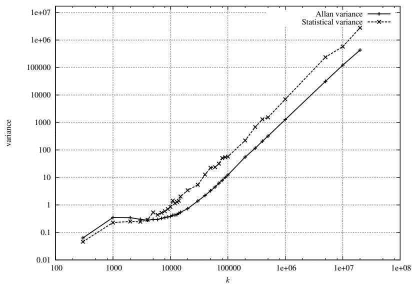
1 adder/subtractor, 1 multiplier

Comparison with the state-of-the-art methods

Method	Area		f_{max}	Power
	ALM/Regs	DSPs	[MHz]	[mW]
Haddad *et al.* (DATE14)	119/160	2	178.3	6-7
Fischer and Lubicz (CHES14)	169/200	4	187.7	7-8
Allan variance based method (CHES18)	49/117	1	238.5	4-5

Normal variance vs Allan variance 3/3





- Variance dependence on the number of samples *M*
  - Allan variance stable
  - Normal variance increases with *M*
- Variance dependence on accumulation period *k*
  - Allan variance always below statistical variance
  - Normal variance causes entropy overestimation
- Similar results for both types of free running oscillators studied[1]

[1] E. N. Allini *et al.*, Evaluation and monitoring of free running oscillators serving as source of randomness. CHES, 2018.

Postprocessing of the raw random signal

- Should make obtained numbers statistically and computationally indistinguishable from the output of an ideal TRNG
- The generated values can be
  - Biased (or not uniformly distributed)
  - Correlated
  - Entropy rate can be insufficient
- Main security objectives
  - Enhance above-mentioned statistical parameters
  - Internal memory of the postprocessing algorithm should maintain some entropy, before the total failure test will trigger alarm
  - Cryptographic postprocessing should ensure unpredictability (if the entropy source fails)

Challenge #8

- Obtain a high quality raw random signal so that the post-processing is not needed!

Statistical tests – objectives and strategies

- Statistical testing of the generator is necessary, but not sufficient – it **cannot substitute**
  - **Cryptanalysis** in the case of DRNGs
  - **Analysis of the entropy rate** in the case of the TRNGs
- Two phases of testing
  - **Off-line testing** (preliminary) during the design and security validation process (by developers and evaluators)
    - Using testing procedures required by security standards
    - Using general purpose (black box) statistical tests (optional)
  - **On-line testing** (operational) – testing when in use in a cryptographic application (testing by the application itself) usually using dedicated tests
    - Startup test(s)
    - Continuous test(s)
    - On-demand test(s)

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

Dedicated (white box) statistical tests 1/3

- Adapted to the generator's principle, more efficient in evaluation of its weaknesses
- Preferably based on the generator's statistical model
- One or more dedicated tests can constitute a basis of embedded tests
- At least the continuous test (the total failure test) should be a white box test adapted to the generator's principle

Challenge #9

- Propose efficient dedicated tests based on the stochastic model

Challenge #10

- Verify and demonstrate efficiency of the tests

Dedicated (white box) statistical tests 2/3

Total failure test (Continuous test)

- The total failure of the entropy means that the entropy rate at the generator's output has fallen to 0
- This catastrophic scenario must be detected very fast and **no further data can be output** once detected
- Triggering the total failure alarm has another important consequence: the generator must be reseted and the (long) startup procedure must be executed – **probability of false alarms must be very small**
- The speed and the robustness of the test can be more easily ensured if the testing point is **closer to the source of randomness**
- The larger latency of the test is allowed only if the numbers are buffered (e.g. in a FIFO)

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

Dedicated (white box) statistical tests 3/3

Online tests

- Online tests should detect intolerable weaknesses
- What means an intolerable weakness should be defined according to the generator's principle, e.g. from the model
- Online tests can be performed
  - Regularly
  - On demand
  - After an event (e.g. self-test of the cryptographic module)
  - Continuously (preferable, but expensive – power consumption)
- Once the online test alarm is triggered, the generator output must be stopped
- During the time interval between the randomness failure and the alarm, the generator must behave as a DRNG

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

Dedicated tests suitable for oscillator based TRNG

Recall

- The stochastic model of our oscillator based TRNG depends on
  - Variance of the jitter (σ^2)
  - Periods T_1 and T_2 and their relationship

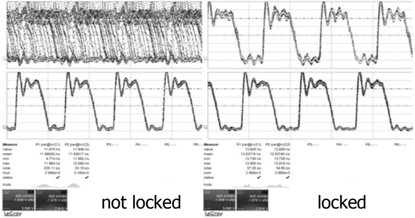
Solution

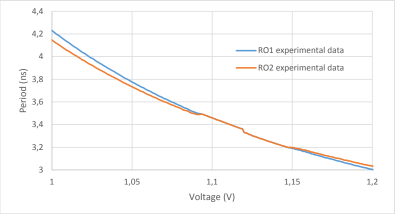
- The Online tests should measure the jitter variance and periods T_1 and T_2

Problem

- But how can the generator totally fail?

Mutual dependence of ring oscillator frequencies





Testing conditions

- Two similar ROs are implemented inside the device
- Frequencies are measured outside the device
- The power supply varies between 1.0 and 1.2 V

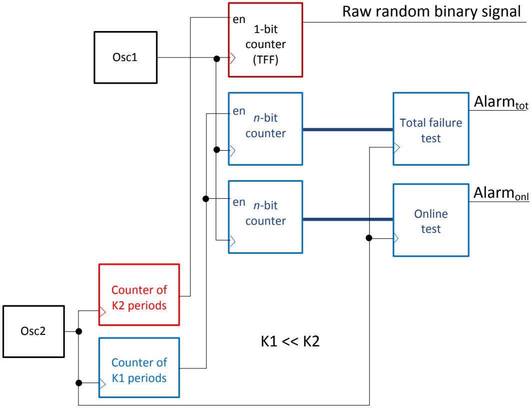
Results

- Frequencies approach and lock to the same value during some voltage interval.

[1] U. Mureddu *et al.*, Experimental Study of Locking Phenomena on Oscillating Rings Implemented in Logic Devices. IEEE TCAS I, 2019.

Oscillator based TRNG including dedicated tests

- **Online test** is based on the Allan variance evaluation
- **Total failure test** evaluates repetitions of counter values
  - Extremely **efficient** to detect locking
  - Extremely **fast** – latency few random bits



LABORATOIRE HUBERT CURIEN

Outline

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

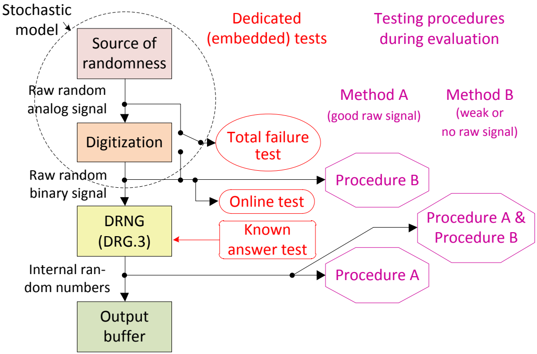
Main approaches in RNG security certification

- Approach of the German BSI (Federal Office for Information Security) – de facto standard in Europe
  - **AIS 20** / **AIS 31** – A proposal for functionality classes for random number generators, v. 1.0 (2001) and 2.0 (2011)
- Approach of the American NIST (National Institute for Standards and Technology)
  - **NIST SP 800-90A** – Recommendation for Random Number Generation Using Deterministic Random Bit Generators (2012)
  - **NIST SP 800-90B** – Recommendation for the Entropy Sources Used for Random Bit Generation (2018)
  - **NIST SP 800-90C** – Recommendation for Random Bit Generator (RBG) Constructions (**draft** from 2012)

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

Example of a high end AIS 20 / AIS 31 PTRNG class

PTG.3



Dedicated tests & entropy

- Total failure, online and startup test requirements as in PTG.2
- Shanon entropy of internal random numbers > 0,997
- Cryptographic post-proc. must be tested by a KAT

Evaluation procedures

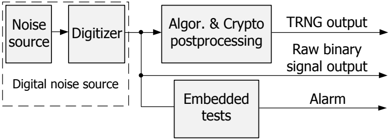
- Depending on availability and quality of the raw binary signal: Method A (preferable) **or** Method B

- Highest security – the information-theoretical security combined with the computational security

LABORATOIRE HUBERT CURIEN

Comparison of the European and American approaches 1/3

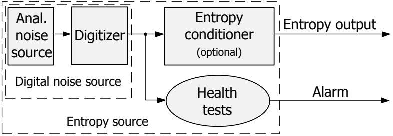
European approach (BSI)



Naming

- Digital noise source
- Algorithmic & cryptographic post-processing
- Digital noise source + Post-processing => Internal random numbers
- Tot test and on-line tests

American approach (NIST)



Naming

- Digital noise source
- Entropy conditioner (entropy extractor)
- Digital noise + Entropy conditioner + Health test => Entropy source
- Health tests

Comparison of the European and American approaches 2/3

Embedded tests

Tot test

- Fast and low false alarm probability
- Test not specified

On-line tests

- Detect non tolerable weaknesses

Health tests

Continuous tests (min. 2 required)

- Repetition count test
- Adaptive proportion test

On-demand tests

- Test not specified

Entropy estimation using a model

Stochastic model must be given

- For IID sources:
  Shannon entropy is computed
- For non-IID sources:
  Conditional entropy is computed

Entropy estimation using tests

For claimed IID sources

- Verification if IID
  - 11 + 5 tests
- Min-entropy estimation for IID

For non-IID sources

- Min-entropy estimation for non-IID
  - 10 statistical tests

Restart test

- One sanity check

Comparison of the European and American approaches 3/3

Testing by security evaluator

- Depending on the TRNG class, Procedure A and B is applied.
- For PTG.2 and PTG.3, the RAW binary signal must be available outside the TRNG (Procedure B).

Conclusion

More stringent approach, but more risky: bad model means bad entropy estimation and possibly bad dedicated test, which means weak generator. Unfortunately, the model construction and verification is not straightforward.

Testing by security evaluator

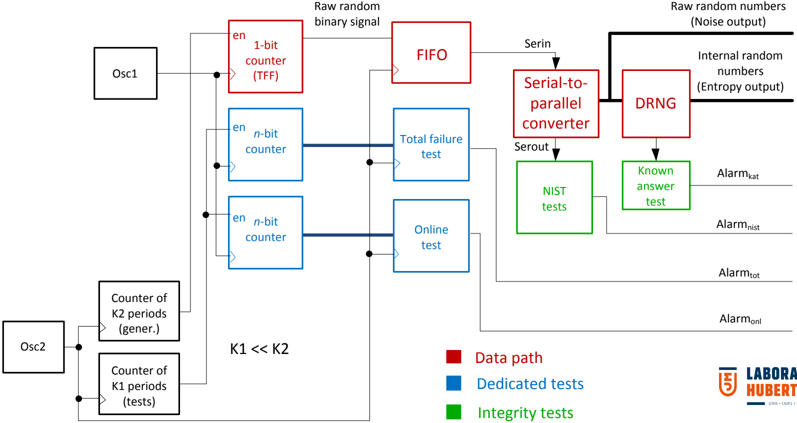
- The RAW binary signal does not need to be available outside the TRNG
(only inside for the health test)

Conclusion

Solution simpler for the designer, but entropy evaluation might not be precise: we obtain the solution that is somehow less risky, but also less precise (for non-IID sources, the entropy can be underestimated).

Towards compatibility with both European and American approach and high security requirements of French DGA 1/2

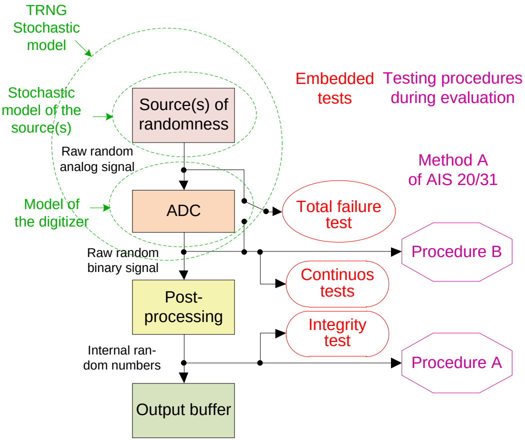
- **Dedicated tests** verify operation of the source of the digital noise
- **NIST tests** test operation of the source, FIFO and S2P converter
- **KAT test** verifies integrity of the DRNG



LABORATOIRE HUBERT CURIEN

Towards compatibility with both European and American approach and high security requirements of French DGA 2/2

- **Source of randomness is modeled** separately
- **NIST tests** and **KAT test** guarantee integrity of the entire TRNG



Outline

1. Contemporary TRNG design challenges
   - Sources of randomness and entropy extraction methods
   - Stochastic models and entropy estimators
   - Postprocessing methods
   - Statistical tests – objectives and strategies

2. Security evaluation of RNGs in a certification process
   - Main approaches in RNG security certification
   - European AIS20/31 vs American NIST SP800-90

3. Conclusions

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

Conclusions

- Designing robust generators giving high-quality true random numbers in logic devices **remains a challenge**
- Testing the source of randomness before entropy extraction **increases precision and speed of the tests and thus security**
- We have shown that **the whole TRNG data path** must be tested to ensure security
- **Efficiency of all embedded tests** must be verified

Last but not least ...

- We have confirmed these statements by many **practical results** published in proceedings of high-end conferences and in scientific papers

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

(New) Challenges in Random Number Generation for Cryptography

Viktor FISCHER

Laboratoire Hubert Curien, UMR 5516 CNRS
Jean Monnet University, Member of University of Lyon
Saint-Etienne, France

fischer@univ-st-etienne.fr

Workshop on Randomness and Arithmetics for Cryptography on Hardware, April 2019

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