# Design and evaluation of a physical random number generator

## Guideline for certification targeting high-security applications

Viktor FISCHER

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

fischer@univ-st-etienne.fr

CryptArchi, Smolenice, June 2017

# Motivation and Objectives

- French DGA (Direction Générale de l'Armement) is responsible for security in high-security cryptographic applications.
- French RNG evaluation scheme is based on the German document AIS 20/31.
- DGA considered that for high-end security applications some additional guideline is necessary to complete AIS 31 (the PTRNG part).
- In 2017, David Lubicz edited the document: "**Design and evaluation of a physical random number generator integrated in an electronic chip**"
- **Our objectives**
  - Present briefly the document (Viktor)
  - Illustrate the DGA document on a PLL TRNG design (Elie)

LABORATOIRE HUBERT CURIEN
UMR · CNRS · 5516 · SAINT ETIENNE

# Outline

1. Introduction
2. Physical noise
   - Requirement 1 – Identification of the source of randomness
   - Requirement 2 – Characterization of the physical noise
   - Requirement 3 – Experimental evaluation of input parameters of the noise model
   - Requirement 4 – Evaluation of stability of noise model parameters in time
3. Analog-to-digital converter
   - Requirement 5 – Availability of the statistical model of the complete TRNG
   - Requirement 6 – Setup of the RNG design parameters
   - Requirement 7 – Parametric statistical tests and their execution
   - Requirement 8 – Availability of a deterministic test
4. Conclusions

# Outline

1. Introduction
2. Physical noise
   - Requirement 1 – Identification of the source of randomness
   - Requirement 2 – Characterization of the physical noise
   - Requirement 3 – Experimental evaluation of input parameters of the noise model
   - Requirement 4 – Evaluation of stability of noise model parameters in time
3. Analog-to-digital converter
   - Requirement 5 – Availability of the statistical model of the complete TRNG
   - Requirement 6 – Setup of the RNG design parameters
   - Requirement 7 – Parametric statistical tests and their execution
   - Requirement 8 – Availability of a deterministic test
4. Conclusions

# Introduction

- The document describes and defines the essential elements of an approach to TRNG design that ensures its security and takes the most recent advances into account.
- The aim of presented approach is to attain the highest level of certainty for the quality of the randomness produced by a generator using an upper limit on the statistical bias that can be measured at the generator output.
- The approach is described in a series of requirements that are well-founded and argued.
- Some definitions that appear important and which are perhaps insufficiently clarified in the literature are also provided.

# Outline

1. Introduction
2. Physical noise
   - Requirement 1 – Identification of the source of randomness
   - Requirement 2 – Characterization of the physical noise
   - Requirement 3 – Experimental evaluation of input parameters of the noise model
   - Requirement 4 – Evaluation of stability of noise model parameters in time
3. Analog-to-digital converter
   - Requirement 5 – Availability of the statistical model of the complete TRNG
   - Requirement 6 – Setup of the RNG design parameters
   - Requirement 7 – Parametric statistical tests and their execution
   - Requirement 8 – Availability of a deterministic test
4. Conclusions

LABORATOIRE HUBERT CURIEN

# Introduction

- TRNG – physical device producing a series of unpredictable bits.
- The operation of the TRNG must rely on a random physical phenomenon known as analog physical noise and must include an analog-to-digital converter (ADC).
- We will first consider the analog physical noise as a source of randomness.

# Definition 1 – Internal stage of the generator

- Random number generator – a physical device $G$ of internal state $E : t \rightarrow V$ depending on time $t$, with value in a space of phases $V$ and producing a series of bits $b_1(t_1)b_2(t_2)\ldots$.
- The value of an output bit at a given time knowing the internal state is perfectly determined.
- Comments:
  - This means that the change in the internal state takes into account the full random nature of the generator.

# Requirement 1 – Identification of the source of randomness

- **The phenomenon of physical noise responsible for the unpredictable nature of generator operation must be clearly identified.**
- Comments:
  - Unidentified phenomena may contribute to the random nature of the operation of the TRNG, too.
  - They shouldn't be taken into account in entropy estimation.

# Definition 2 – Statistical model of the physical noise

- Statistical model of the physical noise – a stochastic model of time variable $t$ with value in the space of phases $V$ describing the change of $E(t)$.
- It may appear as a probability distribution $\mathbb{P}(E(t)|p_1, \dots, p_n, E(t_0) = \dots)$, with $t > t_0$ on $E(t)$, depending on parameters $p_1, \dots, p_n$ and preconditions on $E(t_0)$.
- We make the assumption that the distribution $\mathbb{P}(E(t)|p_1, \dots, p_n, E(t_0))$ contains all the information accessible to an observer (whatever his calculation power) with knowledge of the preconditions on $E(t_0)$.
- Afterwards, such a statistical model is denoted $M(t, p_1, \dots, p_n)$.

# Requirement 2 – Characterization of the physical noise

- **There must be a statistical model** $M(t, p_1, \ldots, p_n)$ **for the physical noise used.**
- Comments:
  - The parameters (e.g. temperature, supply voltage) and the preconditions (e.g. initial phase) are assumed to be known to the attacker.
  - They can be manipulated by the attacker but only within certain limits.
- Remarks:
  - The model can only be deduced from an explanation and physical modelling of phenomena.
  - A statistical analysis of the physical noise, e.g., using statistical tests is insufficient.

# Requirement 3 – Experimental evaluation of input parameters of the noise model

- **One must be able to evaluate experimentally the parameters $p_1, \ldots, p_n$ of the statistical model for physical noise $M(t, p_1, \ldots, p_n)$.**
- **One must be able to evaluate the measurement errors of these parameters.**
- Comments:
  - Parameters can be evaluated externally or internally.
  - External measurements can use high-end measurement tools, but:
    - Measurement can be unprecise, because of data interface.
    - It can be difficult to implement on a production line and complicate testing each device.
  - Here, the use of statistical tests is legitimate.

# Requirement 4 – Evaluation of stability of noise model parameters in time

- **The stability of the parameters $p_1, \ldots, p_n$ of the statistical model must be evaluated for physical noise with regard to:**
  - **physical environmental operating conditions of the RNG: temperature, supply voltage, electromagnetic environment;**
  - **technological environmental operating conditions of the RNG: installed alone on a circuit or with other circuits (e.g., enryption);**
  - **different integrations of the generator (depending on the target technology).**

  **Aging tests could also be performed.**

- Comments:
  - Requirements 3 and 4 can be called the technology qualification.
  - To perform it, circuits should be designed to ensure that:
    - measurements are as accurate as possible;
    - the circuit is tested in the most unfavourable environmental conditions possible.

# Outline

1 Introduction

2 Physical noise

- Requirement 1 – Identification of the source of randomness
- Requirement 2 – Characterization of the physical noise
- Requirement 3 – Experimental evaluation of input parameters of the noise model
- Requirement 4 – Evaluation of stability of noise model parameters in time

3 Analog-to-digital converter

- Requirement 5 – Availability of the statistical model of the complete TRNG
- Requirement 6 – Setup of the RNG design parameters
- Requirement 7 – Parametric statistical tests and their execution
- Requirement 8 – Availability of a deterministic test

4 Conclusions

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

# Introduction

- An analog-to-digital converter produces a series of bits that is a deterministic function of the internal state of the generator.

# Definition 3 – Statistical model of the complete TRNG

- A statistical model for the TRNG whose model of physical noise is $M(t, p_1, \ldots, p_n)$ is a stochastic model $N(t, p_1, \ldots, p_n, q_1, \ldots, q_m)$ with value in the series of bits with arbitrary length, where $p_1, \ldots, p_n$ are the parameters of the physical noise model and $q_1, \ldots, q_m$ are the parameters of the TRNG.
- Certain parameters $q_1, \ldots, q_m$ must be adjusted during component design (but cannot be manipulated by an attacker).

# Requirement 5 – Availability of the statistical model of the complete TRNG

- **There must be a statistical model for the TRNG.**
  - **This assumes all the conditions given above, including that there must be a statistical model for the physical noise.**
- Comments:
  - This assumes that all the previous requirements are fulfilled.
  - Validation of the model is not simple, especially when the physical noises are known only partially.
  - It is very difficult to take into account global deterministic noises.

LABORATOIRE HUBERT CURIEN
UMR • CNRS • 5516 • SAINT ETIENNE

# Requirement 6 – Setup of the RNG design parameters

- **Using the statistical model of the TRNG, it must be possible to adjust parameters $q_1, \ldots, q_n$ to limit the bias on the generator output bits with a defined value.**

- Comments:
  - The use of common statistical tests is once again entirely legitimate.

# Definition 4 – Selection of model parameters

- A parametric test for a TRNG of statistical models $N(t, p_1, \ldots, p_n, q_1, \ldots, q_n)$ is a test that verifies that parameters $p_1, \ldots, p_n, q_1, \ldots, q_n$ are in a certain domain that ensures a sufficient entropy rate. The tests are instantaneous if they can operate at the same time as the RNG.
- With this definition, the following requirement can be set

# Requirement 7 – Parametric statistical tests and their execution

- **Parametric tests must run at startup and continuously.**
- Comments:
  - A common statistical test cannot be interpreted like a parametric test
  - In this case, it is useless and even dangerous.

# Definition 5 – Deterministic test

- A deterministic test for a TRNG is any test that verifies the integrity of the sampling device that associates deterministically an output bit with the value of the internal state.

- With this definition, we can write the next requirement

# Requirement 8 – Availability of a deterministic test

- **There must be tests of deterministic functions that verify proper operation of the functional elements of the TRNG.**
- Comments:
  - Proper operation of the digitizer must be included in this test.

# Outline

1. Introduction
2. Physical noise
   - Requirement 1 – Identification of the source of randomness
   - Requirement 2 – Characterization of the physical noise
   - Requirement 3 – Experimental evaluation of input parameters of the noise model
   - Requirement 4 – Evaluation of stability of noise model parameters in time
3. Analog-to-digital converter
   - Requirement 5 – Availability of the statistical model of the complete TRNG
   - Requirement 6 – Setup of the RNG design parameters
   - Requirement 7 – Parametric statistical tests and their execution
   - Requirement 8 – Availability of a deterministic test
4. Conclusions

LABORATOIRE HUBERT CURIEN

# Conclusions

- Requirements presented in this document represent an extension of those given in AIS 31 (requirements of AIS 31 remain valid).
- Because the highest security levels are targeted by the document, comparing to AIS 31, some additional requirements are given:
  - Statistical model of the source of randomness must be given.
  - Deterministic part of the whole TRNG (not only of the post-processing) must be tested.
  - Parametric tests must be based on the statistical model of the TRNG.
  - General purpose statistical tests should not be used as parametric tests.

# 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

HECTOR

LABORATOIRE
HUBERT CURIEN
UMR • CNRS • 5516 • SAINT ETIENNE