HECTOR TRNG design approach and its demonstration

V. Fischer[1], O. Petura[1], U. Mureddu[1], N. Bochard[1], M. Laban[2]

[1]Hubert Curien Laboratory, University of Lyon, France
[2]MICRONIC S.A., Bratislava, Slovakia

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644052

HECTOR

Outline

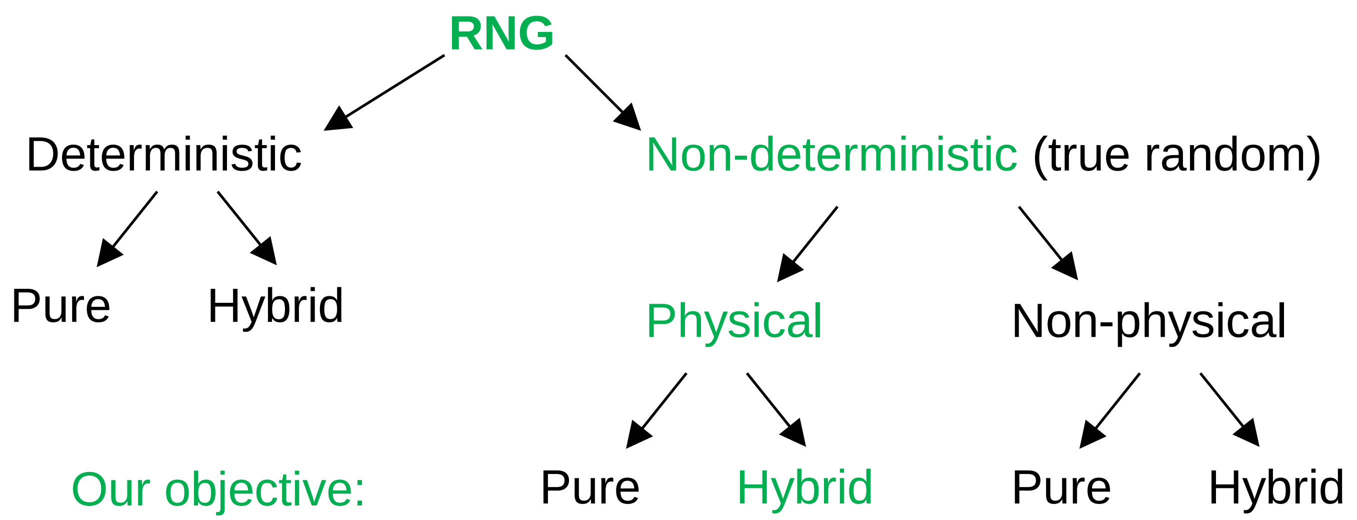
- Introduction – random number generators for cryptography
- Standards for random number generator design
- Illustration of a standard design on HECTOR Demonstrator 1
- Demonstration
- Conclusions

Introduction

- Random number generators (RNGs) constitute essential part of (hardware) cryptographic modules
- Generated random numbers are used as:
  - Cryptographic keys (high security requirements)
  - Masks in countermeasures against side channel attacks
  - Initialization vectors, nonces, padding values, …
- Two main security requirements on RNGs:
  - R1: Good statistical properties of output numbers
  - R2: Unpredictability of output values

Classification of RNGs

- Deterministic RNG (DRNG) – algorithmic generator started with a seed
- True random number generator (TRNG) – non-deterministic (truly random)
  - Physical TRNG (PTRNG) – uses some random physical phenomena
  - Non-physical TRNG (NPTRNG) – uses some non-deterministic events (RAM contents, user interaction (mouse, keyboard), hard disk seek time, etc.)



Evaluation of security requirements

R1: Statistical quality - evaluated using **statistical tests**

- General purpose (black box) statistical tests
  - Standard tests (their speed depends on their precision)
    - FIPS 140-1
    - DIEHARD
    - NIST SP 800-22
- Dedicated (white box) statistical tests (faster and reliable)

R2: Unpredictability – evaluation depends on the generator class

- **Physical unpredictability** - evaluated using **entropy estimation**
  - Entropy is estimated using the stochastic model

- **Computational unpredictability** - evaluated using **cryptoanalysis**
  - Approved cryptographic algorithms are recommended

Outline

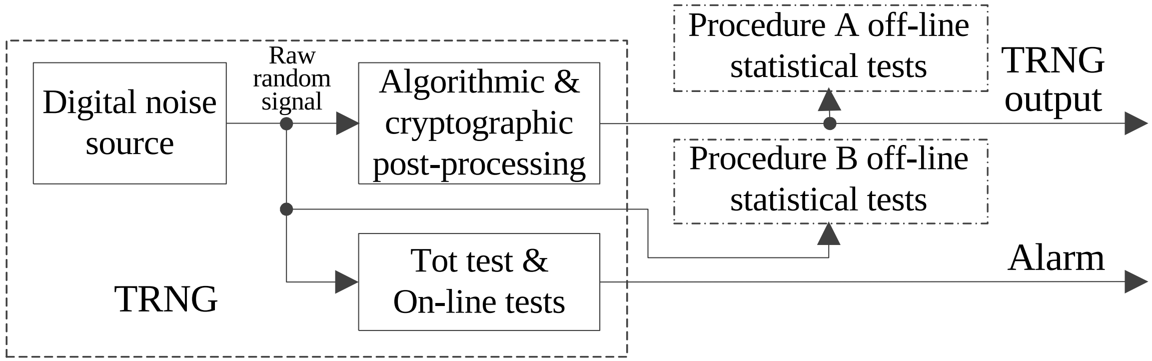
- Introduction – random number generators for cryptography
- Standards for random number generator design
- Illustration of a standard design on HECTOR Demonstrator 1
- Demonstration
- Conclusions

Security standards concerning the TRNG design

- Unlike other cryptographic primitives, TRNGs cannot have standard architectures
- Instead, standard design approach is required
- Currently, two standards are available:
  - **AIS 20/31** of German Federal Office for Information Security (German acronym BSI)
  - **NIST SP 800-90B** of American National Institute for Standards and Technology (NIST)
- The two standards have different design approach, but solutions can be found to fulfill requirements of both of them

European RNG design style

- AIS 20/31 design style



- **Digital noise source** – generates raw random signal
- **Algorithmic post-processing** – enhances statistical properties of generated numbers (increases entropy rate)
- **Cryptographic post-processing** – cryptographic algorithm ensuring computational unpredictability when the source of randomness fails
- **Total failure test** – fast and robust continuous test , no numbers are output if this test fails
- **Online tests** – preferably dedicated tests, based on the stochastic model
- **Off-line tests** (Procedure A and Procedure B) – see later

RNG classes according to AIS 20/31

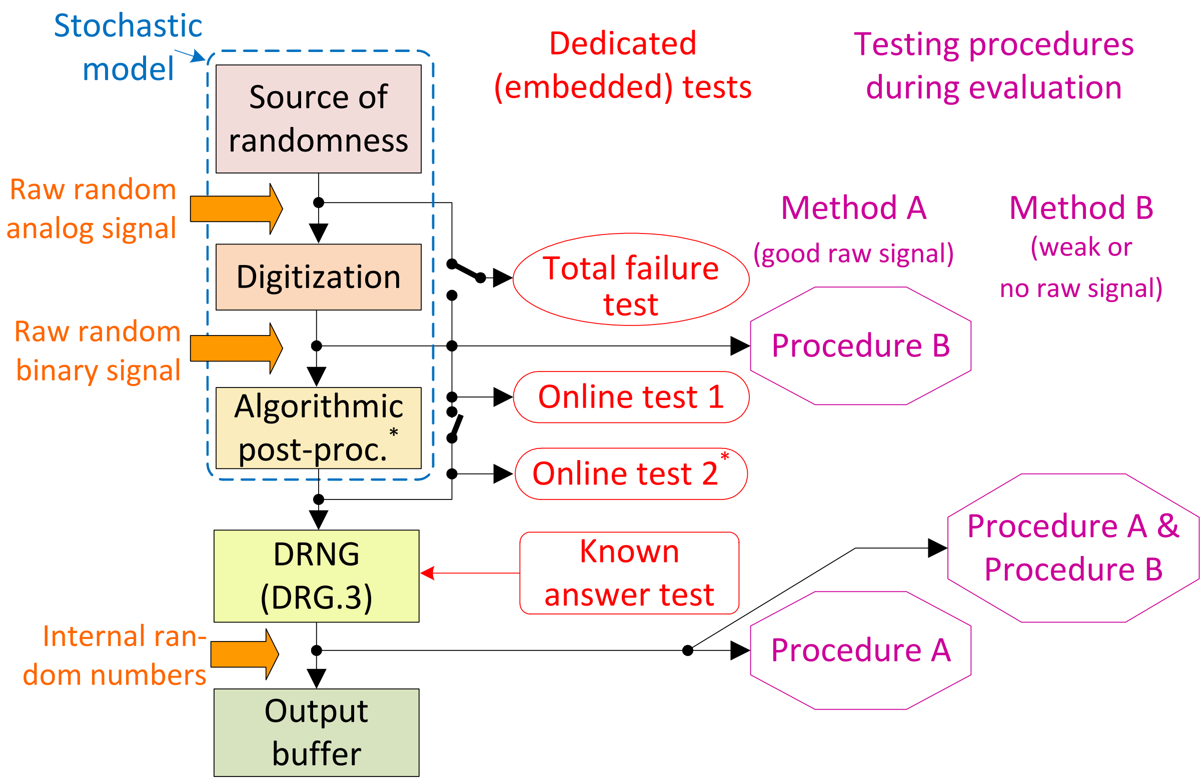
RNG classes

- Three physical TRNG classes
  - **PTG.1** – Physical RNG with internal tests that detect a total failure of the entropy source and non-tolerable statistical defects of the internal random numbers
  - **PTG.2** – PTG.1 + a stochastic model of the entropy source and statistical tests of the raw random numbers (instead of the internal random numbers)
  - **PTG.3** – PTG.2 + cryptographic post-processing (hybrid PTRNG) – HECTOR objective

- One non-physical RNG class
  - **NTG.1**
- Four deterministic RNG classes
  - **DRG.1** to **DRG.4**

Out of HECTOR scope

Class PTG.3 – the highest AIS 31 security class



Stochastic model

- Must be used to estimate entropy

Dedicated tests & entropy

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

Evaluation procedures

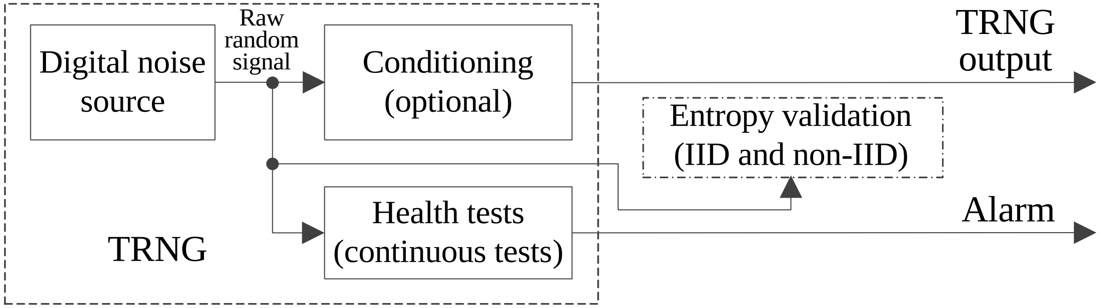
- Depending on availability and quality of the raw binary signal: Method A (preferable) or Method B

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

* Algorithmic post-processing and Online test 2 are optional

American RNG design style

- NIST SP 800-90B design style



  - **Digital noise source** – generates raw random signal
  - **Conditioning** – enhances statistical properties of generated numbers (increases entropy rate): by vetted or non-vetted algorithms
  - **Health tests** – fast and robust continuous tests, no numbers are output if these test fail, two tests are recommended (other equivalent or better are allowed):
    - Repetition count
    - Adaptive proportion
  - **Off-line tests** – entropy validation on two branches: IID and non-IID

Recommendation of the French DGA-MI (DoD)

- Recommendations for high-end TRNGs (first draft in progress)
- Additional requirements on high-security TRNGs comparing to AIS 31
  - Only the source of the digital noise is considered (not the post-processing)
  - Stochastic model of the source of randomness is required (not only of the whole TRNG)
  - All the deterministic parts of the generator must be tested by a KAT (not only the cryptographic post-processing)

HECTOR

Outline

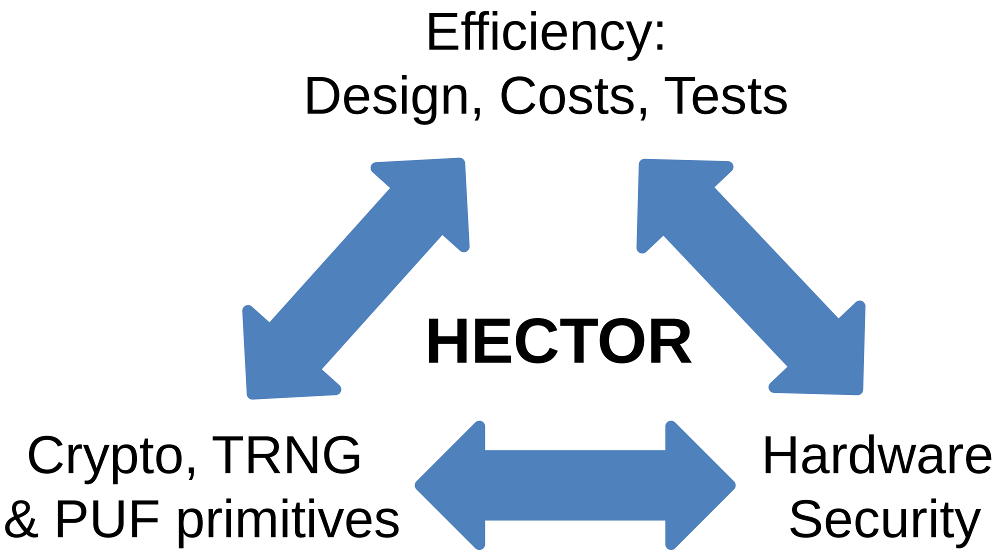
- Introduction – random number generators for cryptography
- Standards for random number generator design
- Illustration of a standard design on HECTOR Demonstrator 1
- Demonstration
- Conclusions

HECTOR – Hardware Enabled CrypTO and Randomness

- European Union's Horizon 2020 research and innovation programme under grant agreement number 644052
- 3-year project starting from March 2015
- 9 partners (3 universities, 3 big companies, 3 SME):
  - Technicon GMBH, Villach, Austria (coordinator)
  - Katholieke Universiteit Leuven, Belgium
  - Université Jean Monnet Saint-Etienne, France
  - Thales Communications & Security SAS, Gennevilliers, France
  - STMicroelectronics Rousset SAS, Rousset, France
  - STMicroelectronics SRL, Agrate Brianza, Italy
  - Micronic AS, Bratislava, Slovakia
  - Technische Universitaet Graz, Graz, Austria
  - Brightsight BV, Delft, Netherlands

HECTOR – Hardware Enabled CrypTO and Randomness

- HECTOR core problem
  - Find solutions for the tension between mathematical security, implementation security and efficiency:

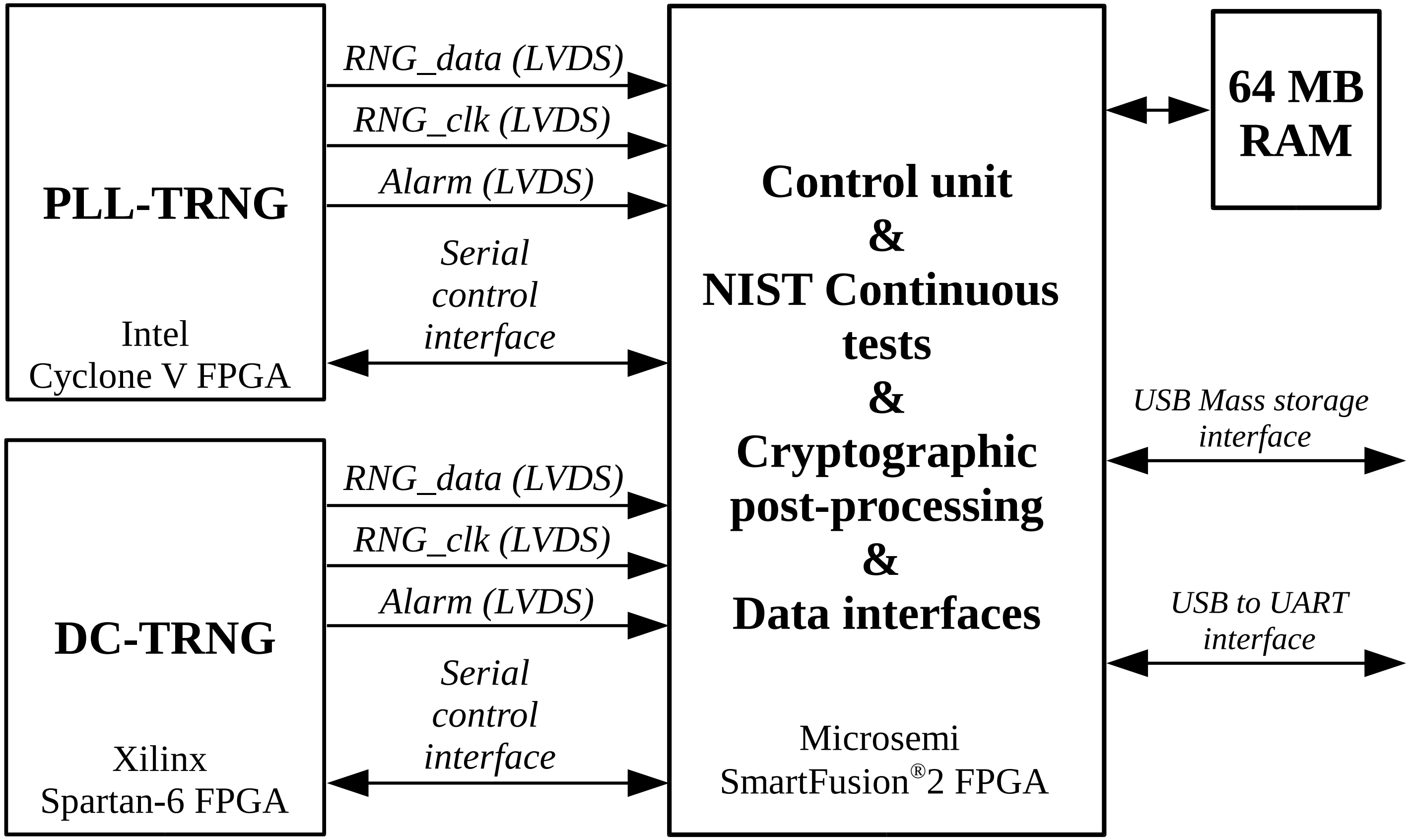


HECTOR – Hardware Enabled CrypTO and Randomness

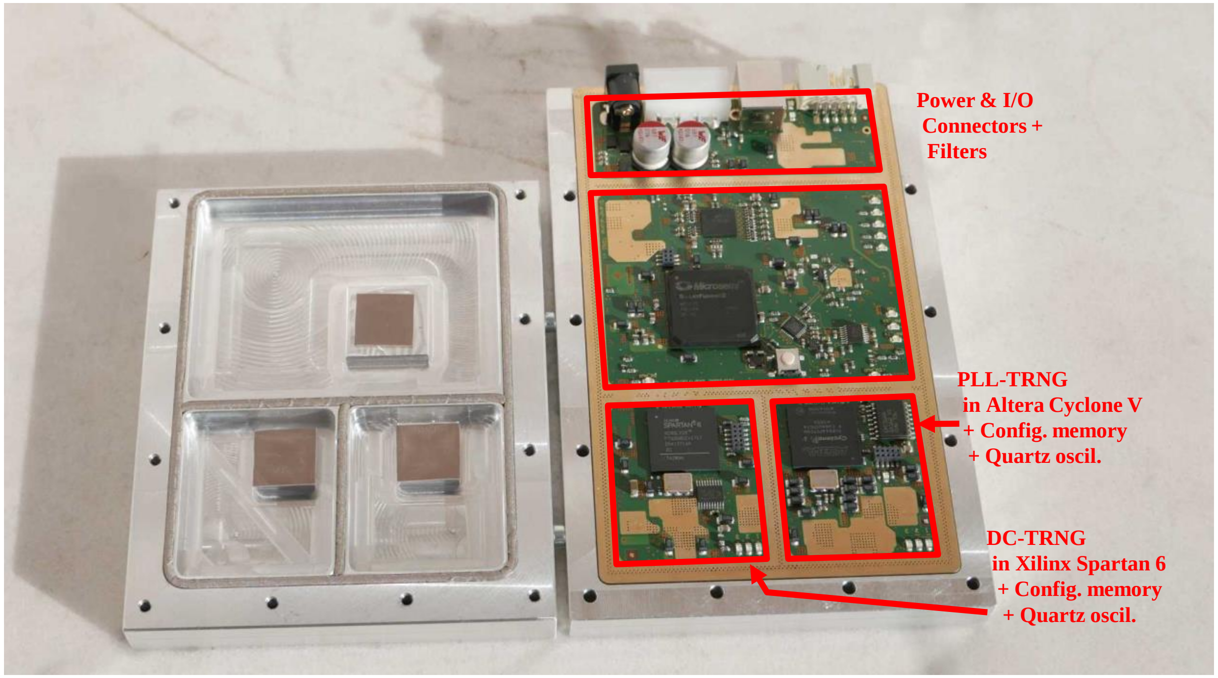
- Main initial objectives in TRNG design
  - Hardware **RNG design approach** based on thorough entropy estimation and management
  - **Stochastic models** of RNGs that can be used to build **efficient and fast dedicated embedded tests**
  - Verify the **robustness** of the proposed TRNGs **against passive and active attacks**
  - Validate AIS31 **certification feasibility** and process simplification by actually going through the full process for a HECTOR TRNG design with an accredited certification lab
- Additional objective
  - Propose RNG, which is compliant with AIS20/31, NIST SP 800-90B and French high security RNG design recommendations

HECTOR – Demonstrator 1

- Functional diagram

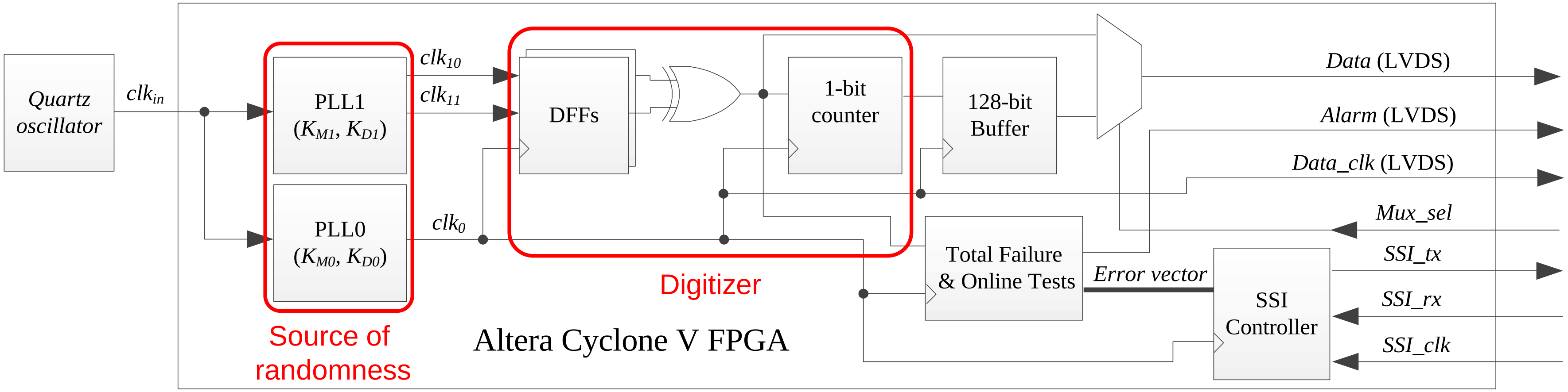


- Three FPGA areas separated by a ground plate
- Three separated chambers inside a metallic shielding



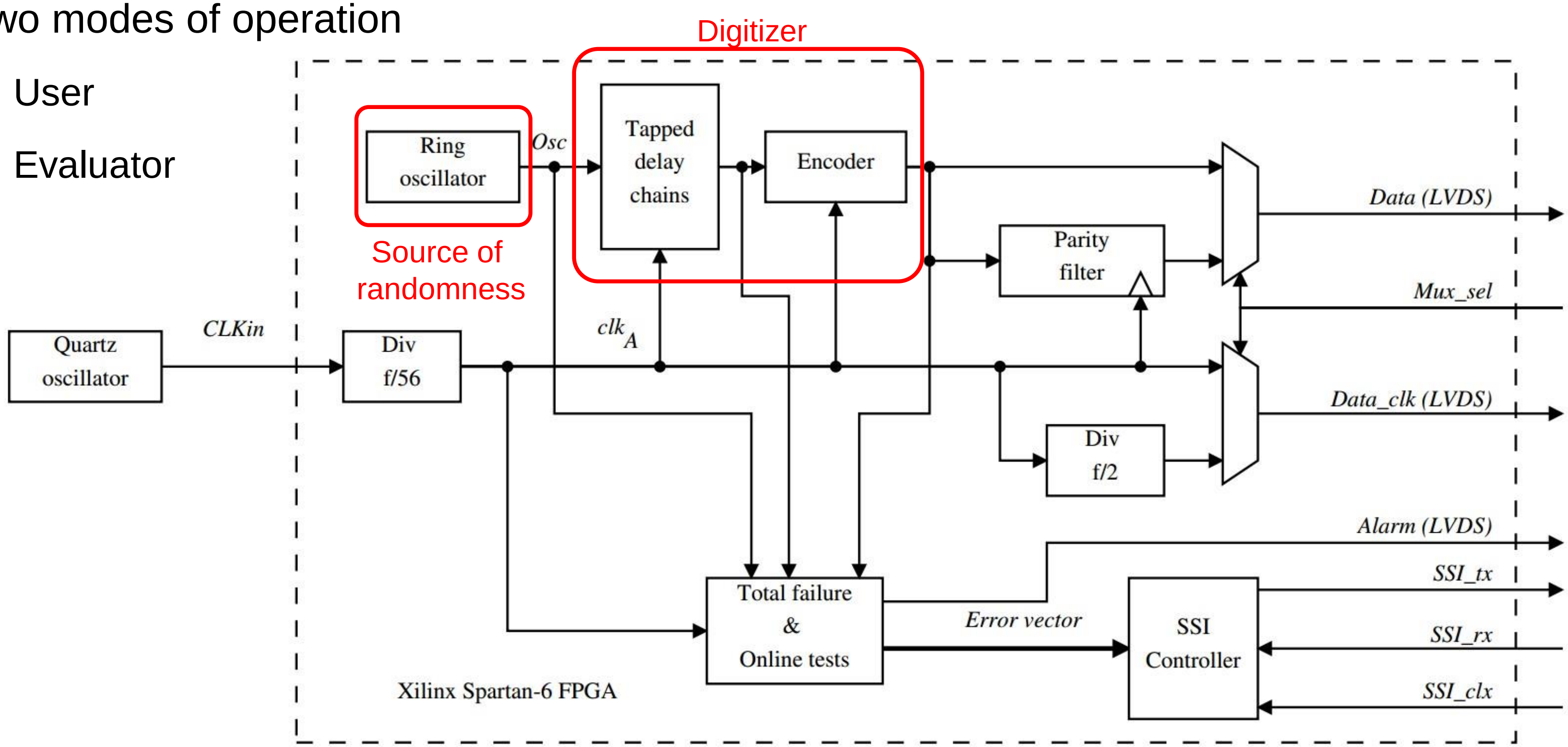
PLL-TRNG core

- Source of randomness – differential jitter between outputs of two PLLs
- Fast data interface (LVDS) and serial control interface (SSI)
- Two modes of operation:
  - User mode – only the raw random binary signal is output
  - Evaluator mode – other internal signals are available
- Dedicated embedded tests (parametric statistical tests)
  - Total failure test
  - Two online tests



DC-TRNG core

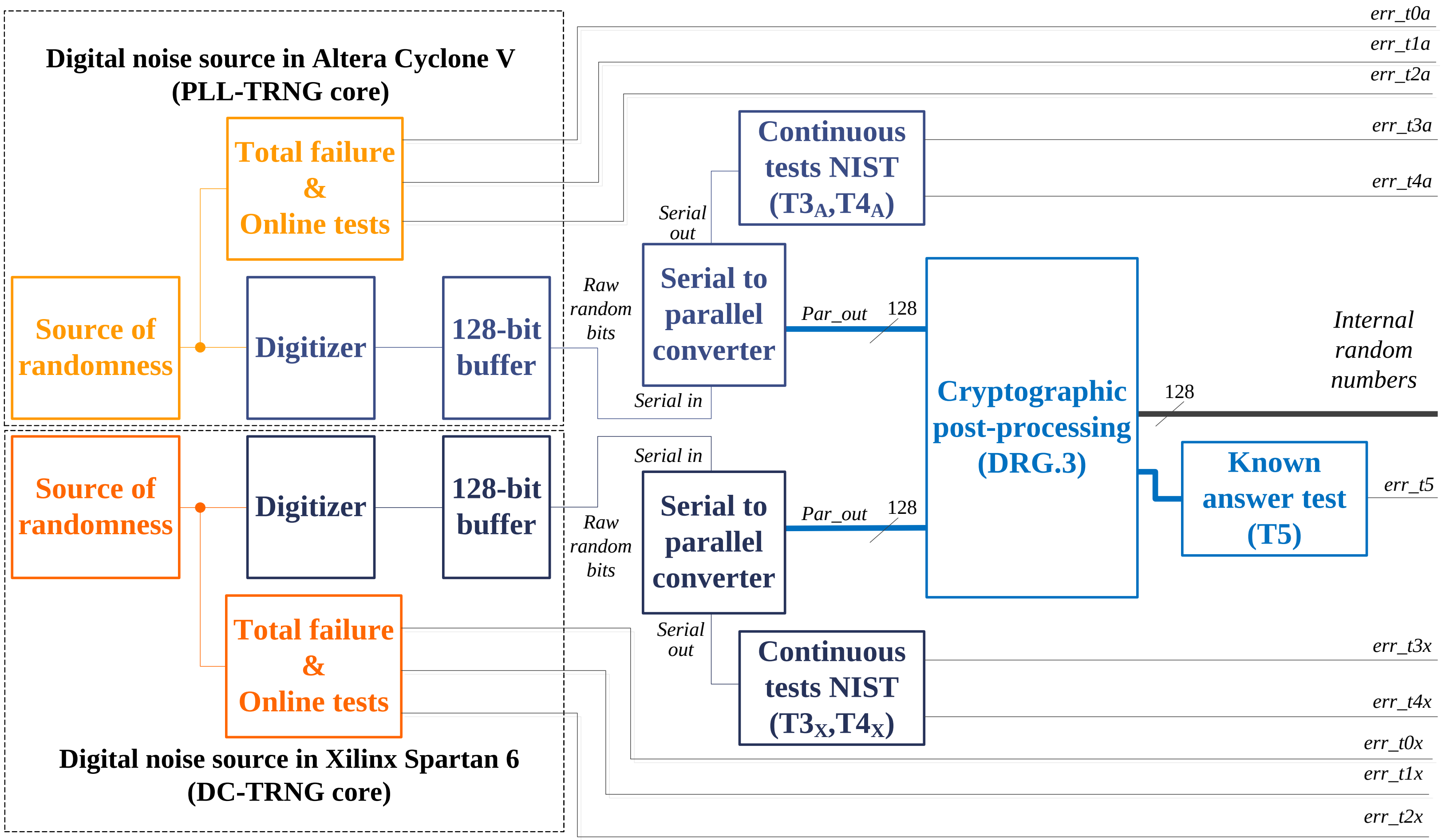
- Source of randomness – jitter of the clock generated in a ring oscillator
- Dedicated embedded tests (parametric statistical tests)
  - Total failure test
  - Two online tests
- Two modes of operation
  - User
  - Evaluator



HECTOR TRNG including embedded tests

HECTOR TRNG contains four essential parts:

- Two sources of the digital noise
- Embedded tests
- Cryptographic post-processing
- Data interface



Embedded tests in HECTOR TRNG

Two total failure tests

PLL-TRNG: T0a: $P_1 > 0$ (Number of random samples during one T_Q)
DC-TRNG: T0x: Detects edges of the ring oscillator clock signal

Four online tests

PLL-TRNG: T1a: $4 < P_1 < K_D/4$ (P_1 computed from 4080 T_Q periods)
T2a: $228 < P_2 < 1280$ (during 4080 T_Q periods)
DC-TRNG: T1x: $35 < N_{111} < 93$ (number of overlapping templates “111”)
T2x: $185 < C_1 < 326$ (number of XORed couples of bits)

Continuous tests (NIST SP 800-90B)

T3: Repetition count test with cutoff value $C_R = 51$
T4: Adaptive proportion test with cutoff value $C_A = 1380$

Known answer test (KAT)

T5: KAT test of the cryptographic post-processing block

Startup procedure

Generated data have to pass Tests T0 to T5

Outline

- Introduction – random number generators for cryptography
- Standards for random number generator design
- Illustration of a standard design on HECTOR Demonstrator 1
- Demonstration
- Conclusions

Demonstration

Two kinds of access to HECTOR Demonstrator 1

- Physical device + tools
  - Hardware – TRNG cores + tests + control unit
  - Firmware – controls data acquisition and exchange
  - Software – controls access to the demonstrator from the host PC (in TCL)
- Random number generator as a service

  https://trng.technikon.com/

Outline

- Introduction – random number generators for cryptography
- Standards for random number generator design
- Illustration of a standard design on HECTOR Demonstrator 1
- Demonstration
- Conclusions

Conclusions

- The HECTOR TRNG fulfills all requirements specified by industrial partners
- It is compliant with the three available documents
  - AIS20/31
  - NIST SP 800-90B
  - Requirements of French DGA

Question:

Can all TRNGs comply with these recommendations? The clear response is: NO.

- Possible problems:
  - A mixture of true- and pseudo-randomness in the raw signal
  - Non-deterministic randomness extraction process
  - Stochastic model not depending on measurable parameters

"The **HECTOR** project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 644052."

If you need further information, please contact the coordinator:
TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55   Fax: +43 4242 233 55 77
E-Mail: coordination@hector-project.eu

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.