FROM RESEARCH TO INDUSTRY

cea tech

TRNG - EVALUATION & CERTIFICATION

WRAC'H 2019 | DUMAS Cécile | 15 avril 2019

OUTLINE

- **Evaluation Lab**
- **Random Number Generators**
- **Evaluation of RNG**
- **Conclusion & Perspectives**

FRENCH CERTIFICATION SCHEME

ITSEF **I**nformation **T**echnology **S**ecurity **E**valuation **F**acility

CESTI **C**entre d'**É**valuation de la **S**écurité des **T**echnologies d'**I**nformation

- **Several ITSEFs and several types of product**

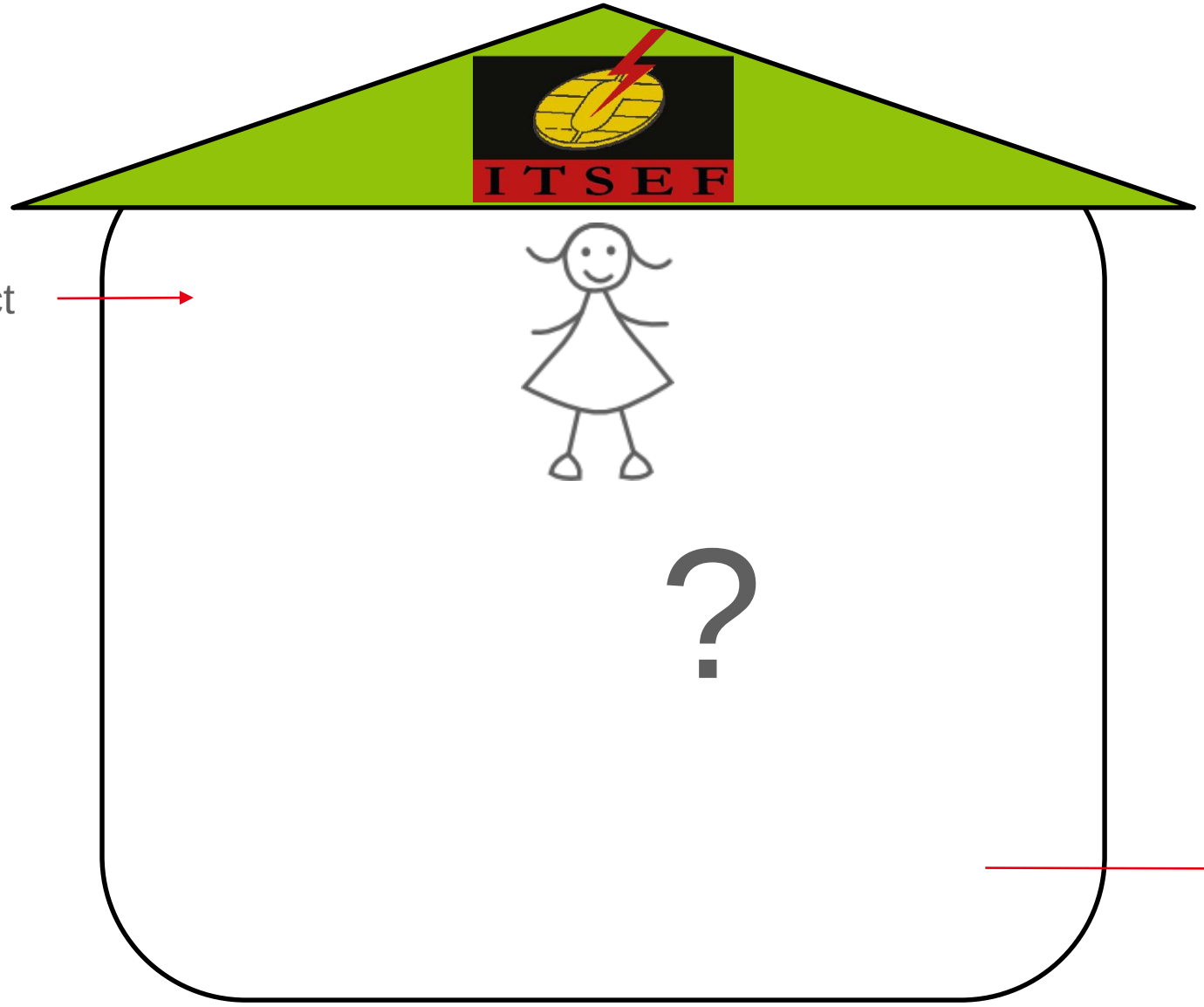
→ Leti into CEA Grenoble: Hardware ITSEF

Leti ITSEF

- Center established in 1999
- Scope of Approval: Hardware ITSEF
  - Electronic Components and Embedded Software
  - Hardware device with security boxes
  - Site certification
- Evaluation Standard
  - Common Criteria : CC version 3.1 ; up to EAL7
- Licensed by private schemes
  - EMVCo, VISA, MASTER-CARD, NXP-MIFARE, BAROC, FIDO

ACCREDITATION N°1-1294
PORTEE DISPONIBLE SUR
WWW.COFRAC.FR

ITSEF – EVALUATION TASKS



ITSEF – EVALUATION TASKS

Product
= Smart card

Applications
- Banking
- Identity
- Health
- PayTV
- …

Functions
- Encryption / decryption
- Signature
- Authentication
- Key generation / exchange
- …

Mechanisms
- Symmetrical algorithms
- Asymmetrical algorithms
- Hash functions
- Random number generator

Hardware / Software

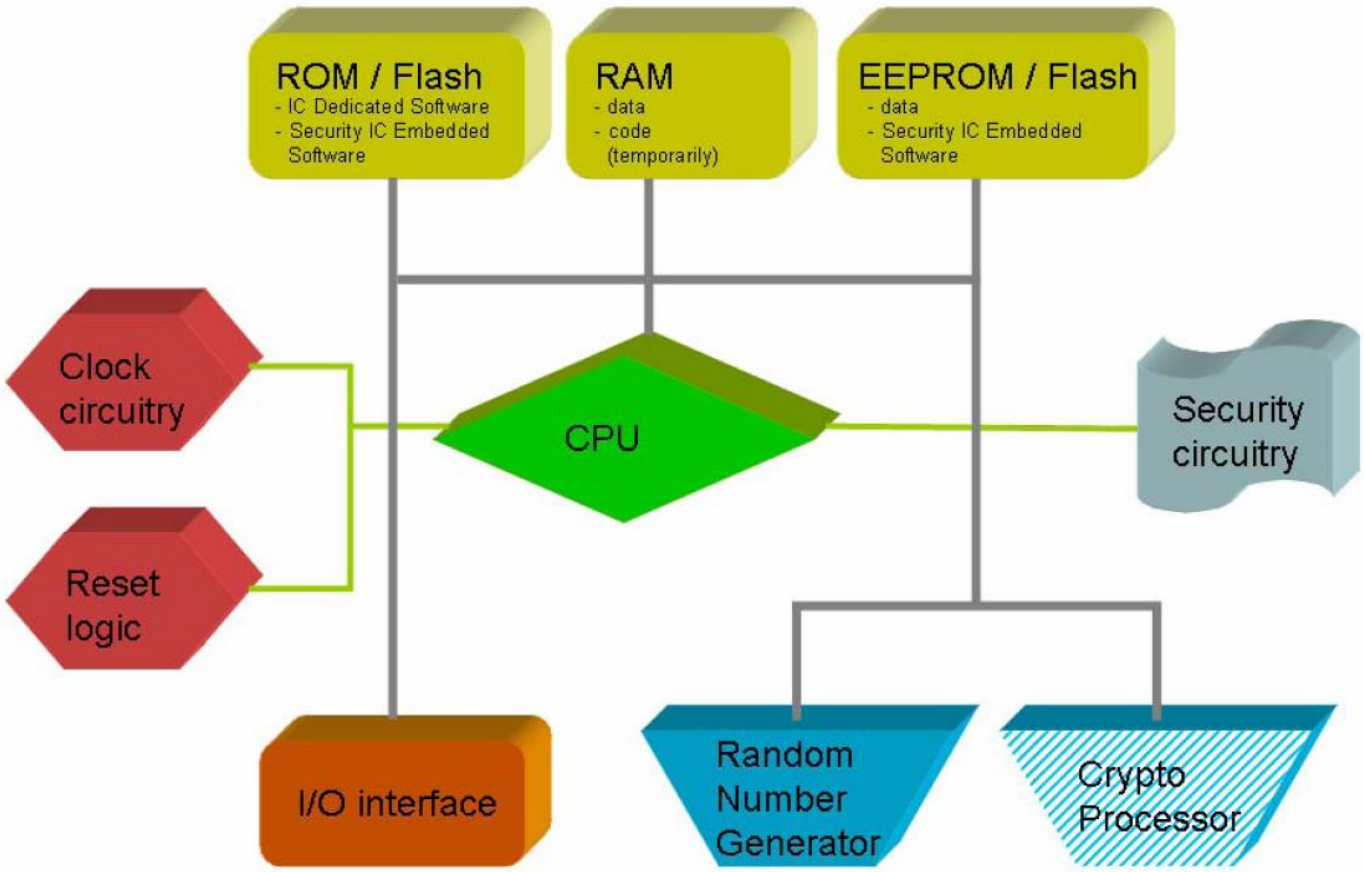
→ Report

ITSEF – EVALUATION TASKS

ITSEF

Product
= Smart card

Applications
- Banking
- Identity
- Health
- PayTV
- …



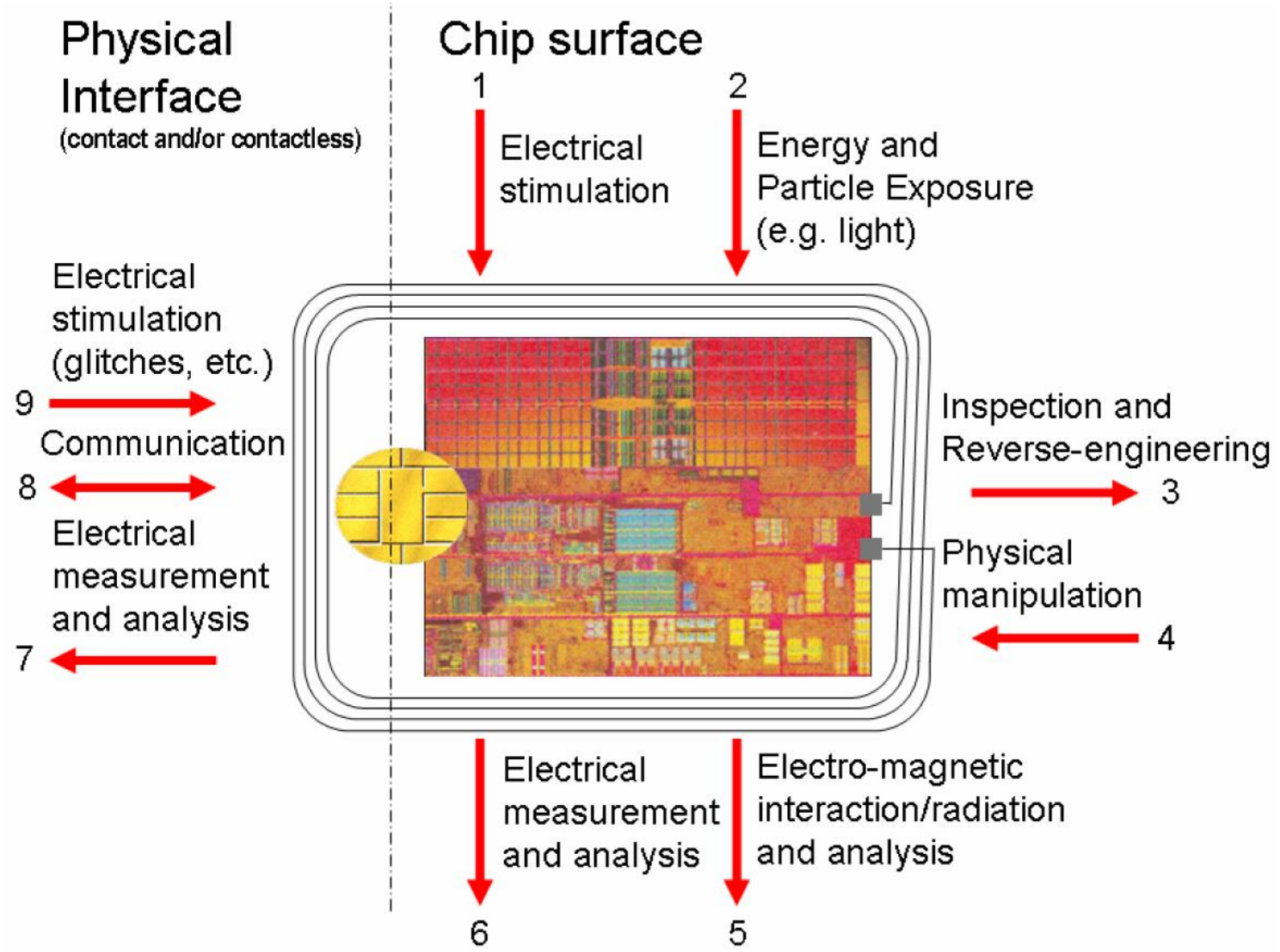
Source: Security IC Platform Protection Profile - BSI-PP-0084

ITSEF – EVALUATION TASKS

Product –
= Smart card

Applications

Banking
Identity
Health
PayTV
…



Source: Security IC Platform Protection Profile - BSI-PP-0084

ITSEF – EVALUATION TASKS

ITSEF

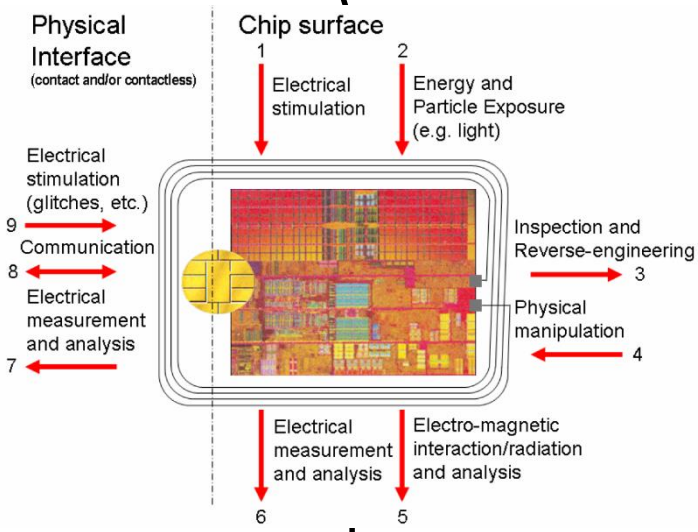
Product
= Smart card

Functions
- Encryption / decryption
- Signature
- Authentication
- Key generation / exchange
- …

Mechanisms
- Symmetrical algorithms
- Asymmetrical algorithms
- Hash functions
- Random number generator

Hardware / Software

Conformity
- Document analysis
- Code analysis



Efficiency
- Functional testing
- Penetration testing

Report

OUTLINE

- Evaluation Lab
- **Random Number Generators**
- **Evaluation of RNG**
- **Conclusion & Perspectives**

RANDOM NUMBER GENERATOR

- Random numbers in smart cards
  - Key generation
  - Challenge generation
  - Generation of initialization vectors, nonces, padding, ...
  - Countermeasures against side channel attacks

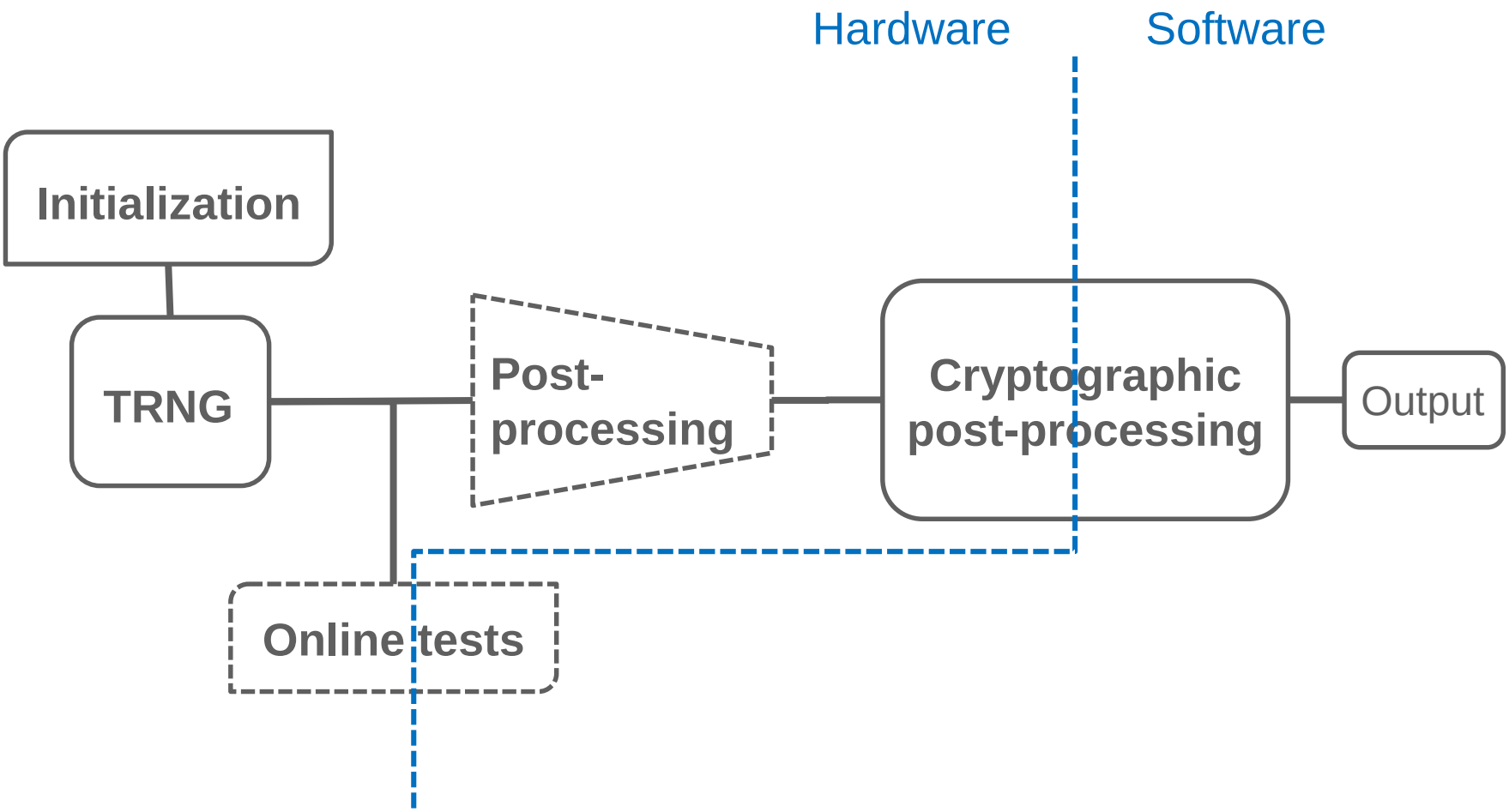
- To play 421, the result of a die roll shall be
  - Uniform
  - Independent
  - Unpredictable

→ **Expected properties of the random numbers**

RANDOM NUMBER GENERATOR

- Deterministic (Pseudo-) random number generators (DRNG)
  - Algorithmic
  - Good statistical properties
- Physical (True-) random number generators (TRNG)
  - Using some physical source of randomness
  - Physics is not deterministic
  - Moderate statistical properties
- Hybrid random number generators
  - TRNG with algorithmic (e. g. cryptographic) post-processing
  - DRNG seeded repeatedly by a TRNG

RNG ARCHITECTURE



RNG – EVALUATION TASKS

Product
= Smart card with a RNG

Conformity
- Document analysis
- Code analysis

- Initialization
- TRNG
- Online tests
- Post-Processing
- Crypto post-processing

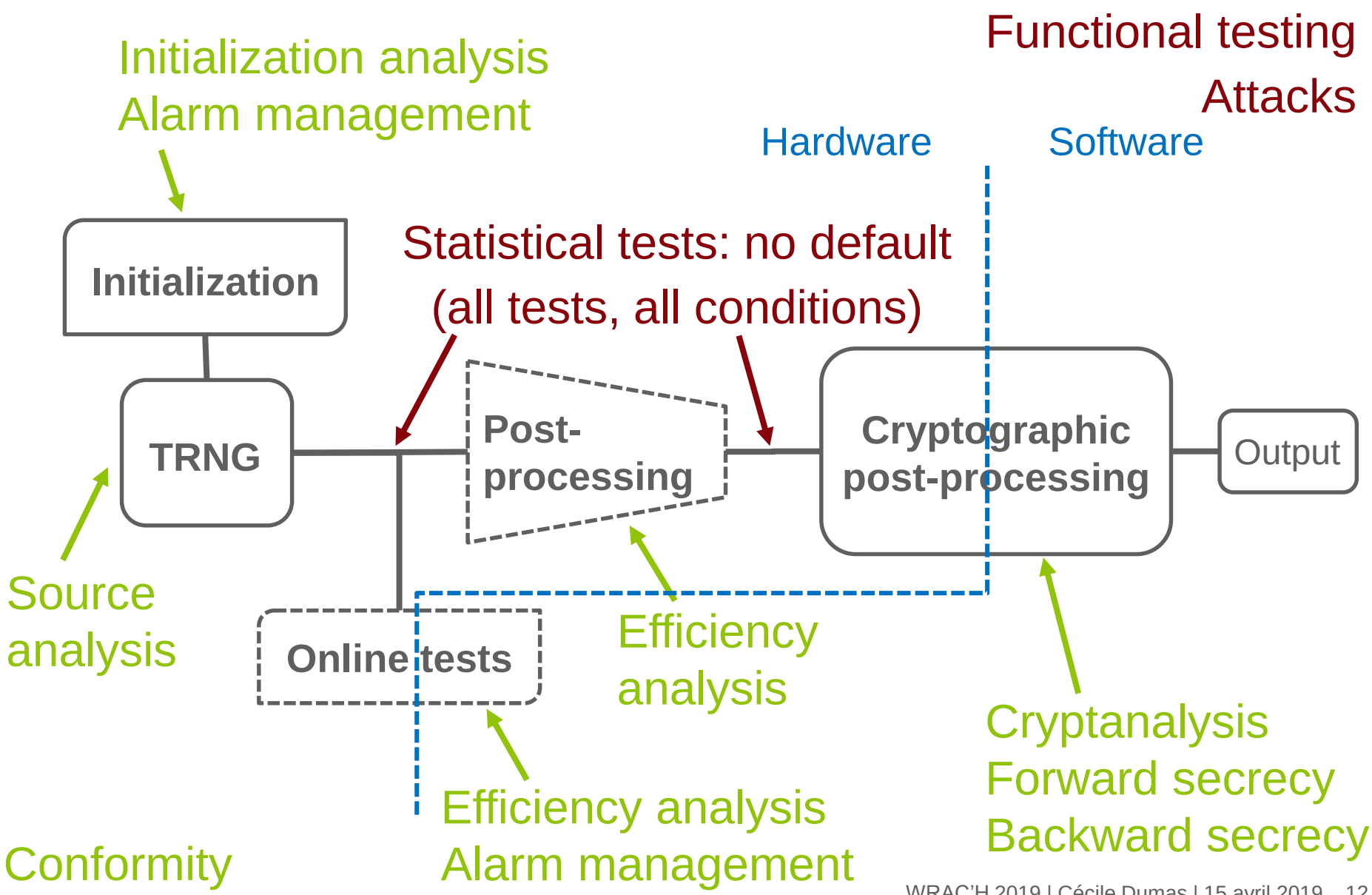
- Initialization
- TRNG
- Online tests
- Post-Processing
- Crypto post-processing

Efficiency
- Functional testing
- Penetration testing
- Statistical testing

TRNG non deterministic !!

Report

RNG EVALUATION TASKS



EVALUATION NORMS

- **Common Criteria**
  - Security Functional Requirements (Family FCS_RNG)
- **Evaluation**
  - RGS - French Scheme
    Référentiel Général de Sécurité
  - AIS 20 31 - German Scheme
    Anwendungshinweise und Interpretationen zum Schema

→Talk of Werner Schindler, BSI Germany, tomorrow

OUTLINE

- Evaluation Lab
- Random Number Generators
- **Evaluation of RNG**
- Conclusion & Perspectives

RNG EVALUATION TASKS

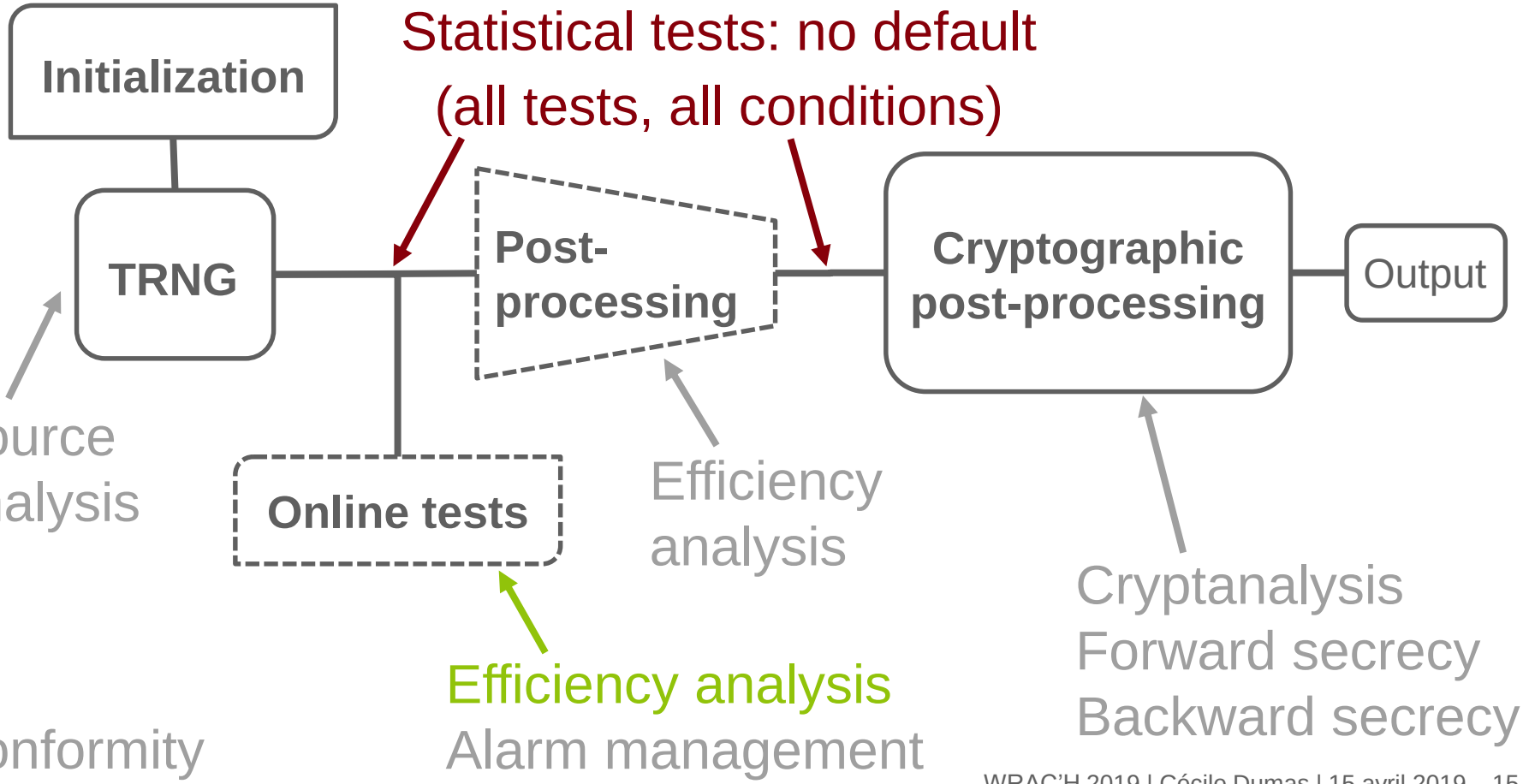
Functional testing

Environment alteration

Attacks

Initialization analysis
Alarm management

THIS TALK



OUTLINE

- Evaluation Lab
- Random Number Generators
- **Evaluation of RNG**
  - **Acquisition**
  - **Statistical Tests**
  - **Online Tests**
  - **Penetration Tests**
- **Conclusion & Perspectives**

RANDOM NUMBERS ACQUISITION

- **Need to acquire random numbers**
  - After source
  - After post-processing
  - All configurations (voltage, clock frequency, etc.)

  → Acquire several sequences

- **Statistical testing**

  → Acquire several very large sequences

  → Acquire several very large continuous sequences

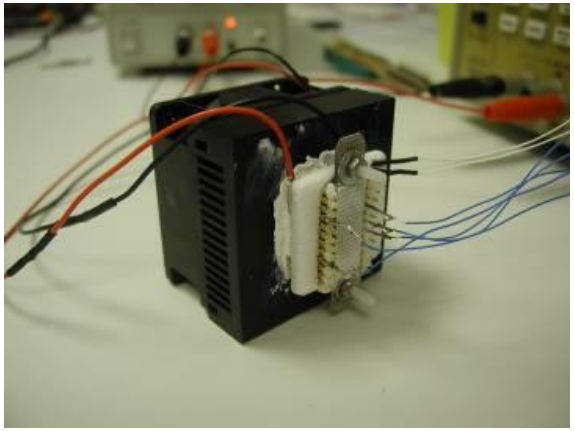
- **Several devices have to be tested**

RANDOM NUMBERS ACQUISITION

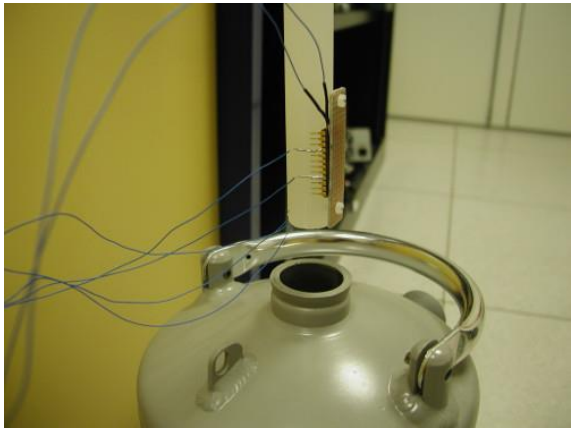
- **All environmental conditions have to be tested**

Source: M. Sourcarros, Analyse des générateurs de nombres aléatoires dans des conditions anormales d'utilisation, rapport de thèse - 2006

Resistor heater
ambiant ~ 120°C



Peltier cooler
-25°C ~ ambiant



Liquid nitrogen
-190°C ~ ambiant

- **Acquisition compaign of several very large continuous sequences**

RANDOM NUMBERS ACQUISITION

- **Acquisition effort for the developer**
  - The random numbers must be accessible from the source
  - The random numbers must be output without stopping the TRNG

  or
  - Large sequences must be stored before outputting

- **Acquisition effort for the evaluator**
  - 30-50 files
  - 100 MB per file → ~ 4 GB
  - 2-3 hours per file → ~ five days
  - The data is stored for a long time

  → At each evaluation we keep 4 GB of really nothing, for a long time!

OUTLINE

- Evaluation Lab
- Random Number Generators
- **Evaluation of RNG**
  - Acquisition
  - **Statistical Tests**
  - Online Tests
  - Penetration Tests
- Conclusion & Perspectives

STATISTICAL TESTS

- **Uniformity, independence, unpredictability**
  - No universal test
    Focus on one property of uniform i.i.d. random variables

- **Statistical test**
  - Defines a random variable and the expected range of values.
  - Test result = FAIL or SUCCESS
  - SUCCESS = No detected defect ≠ Randomness

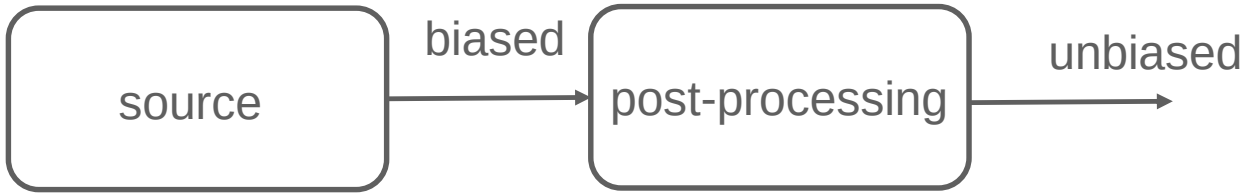
- **Batteries**
  - FIPS140-1 and FIPS140-2 ⇐ 20,000 bits
  - DIEHARD ⇐ ~80,000,000 bits
  - NIST SP800-22 ⇐ ~1,000,000,000 bits
  - AIS31 test suite ⇐ ~100,000,000 bits
  - Tests U01 (L'Ecuyer)

  - Characterization tests → Selection of devices under tests
  - Adapted tests

Leti ITSEF statistical tool

ADAPTED TESTS

- **An example: a biased source**



  - How evaluate this Bernouilli source?
  - Majority of statistical tests fail

Example
$P_1 = 0.46$ before post-processing
- AIS31: T1, T2, T3, T6, T8 fail
- TestU01: 50 / 57 tests fail

  - Other defaults than bias?

- **Need to know the statistical properties of the source**
  - Is the post-processing sufficient?
  - Bring confidence in the source modelling

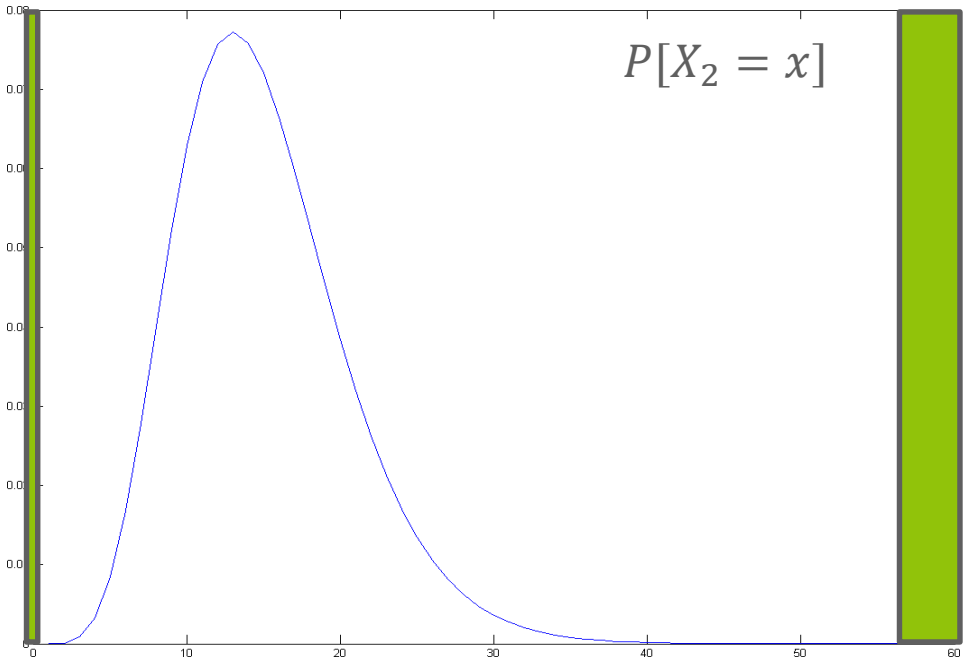
→ **Adapted tests**

ADAPTED TESTS

- **Tests adapted with the Bernouilli distribution**

- **Example poker test (FIPS140-1, AIS31 T2):**
  - $X_2 = \frac{16}{5000} \times \sum_{i=0}^{15} f(i)^2 - 5000$ $f(i)$ pattern occurrence number follows a χ^2 distribution with 15 degrees of freedom
  - The test passes if $1.03 < X_2 < 57.4$
  - This corresponds to:

$Pr[X_2 > 57.4] = 7.0184 \times 10^{-7}$
$Pr[X_2 < 1.03] = 3.1236 \times 10^{-7}$

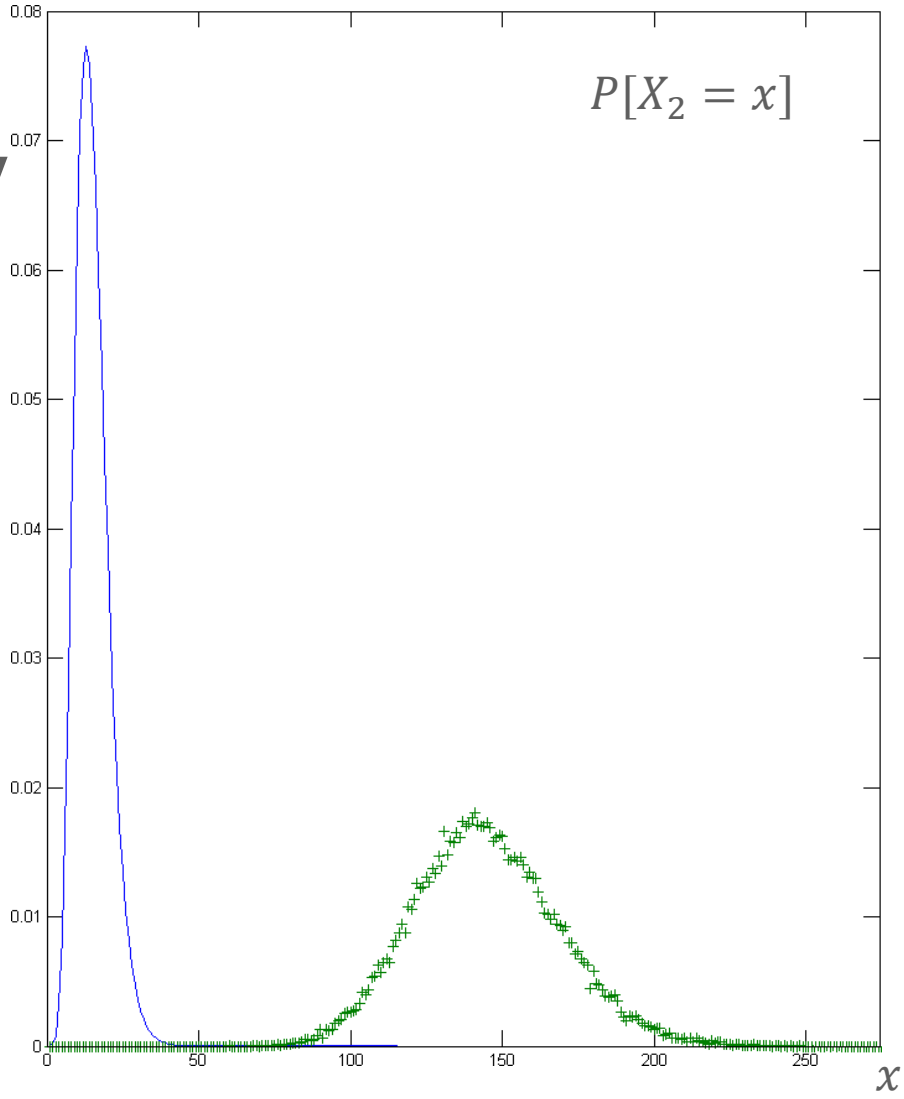


ADAPTED TESTS

- **With the biased sequence**
  $$P_1 = 0.46$$
  the test fails with high probability

- Expected probability of the pattern frequency

$$p(i) = \frac{1}{16}$$



ADAPTED TESTS

- **Adapted poker test**
  - Expected probability

    $p(i) = {P_1}^{\pi(i)}(1-P_1)^{4-\pi(i)}$

    where $\pi(i)$ is the Hamming weight of i

  - $X'_2 = \sum_{i=0}^{15} \frac{\left(f(i)-5000\times p(i)\right)^2}{5000\times p(i)}$

    follows a χ^2 distribution with 15 degrees of freedom

  - The test collects several X'_2 and compares them to the expected distribution

Examples

$p(0000) = (1-P_1)^4$

$p(0001) = P_1(1-P_1)^3$

$p(0011) = {P_1}^2(1-P_1)^2$

ADAPTED TESTS

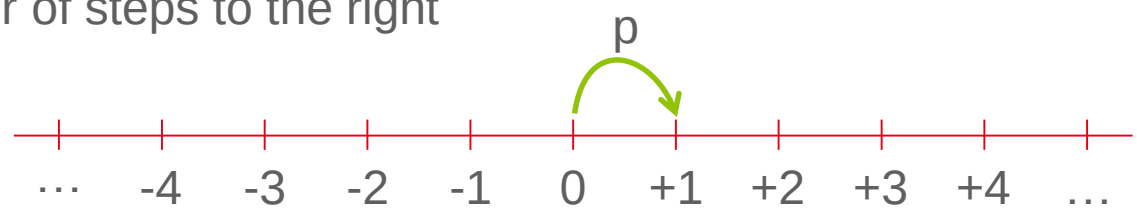
- **Repetition of Poker test (FIPS140-1, AIS31 T2)**
  - Number of patterns

de44432885f6e081ed69b565788e38e9…

- **Repetition of Runs test (FIPS140-1, AIS31 T3)**
  - Number of runs and gaps

1111011010110111010110101101011110001000

- **Random Walk (TestU01)**
  - Statistic H: number of steps to the right



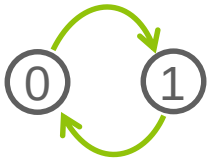
- **Hamming Weight (TestU01)**
  - Number of $\pi(i)$ values

de44432885f6e081ed69b565788e38e9…
33111211112423011332232223113213 2

  - Number of $(\pi(i), \pi(j))$ values

de44432885f6e081ed69b565788e38e9…
33111211112423011332232223113213 2

ADAPTED TESTS

Generated method	P_1	AIS31 failed Tests	TestU01 failed tests	Adapted tests for $P_1 = 0{,}46$
Biased sequence	0.46	T1, T2, T3 T6 T8	50 / 57	4 tests pass
Markov order 1 $\alpha = 0.5$  $\beta = 0.58$	0.46	T1, T2, T3 T5 T6 T8	51 / 57	4 tests fail
Biased sequence with 1/10 pattern 0100 replaced by 0010	0.46	T1, T2, T3 T6 T8	50 / 57	3 tests pass 1 test fails (adapted Poker)

OUTLINE

- Evaluation Lab
- Random Number Generators
- **Evaluation of RNG**
  - Acquisition
  - Statistical Tests
  - **Online Tests**
  - Penetration Tests
- Conclusion & Perspectives

ONLINE TESTS

- **Goal: detect non-tolerable statistical weaknesses of the source**
  - → Degradation
  - → Expected default
- **Is this online test suitable to detect this default sufficiently soon?**
  - → How many random bits are generated before detection?
- **Detection depends on the call frequency of the online tests**
  - → How many online tests are performed before detection?
  - → Minimal number of online tests to ensure a good probability of detection?

→ **Estimation of the probability of detection of the online test** p

ONLINE TESTS

- **Goal: detect non-tolerable statistical weaknesses of the source**
  - → Degradation
  - → Expected default
- **Is this online test suitable to detect this default sufficiently soon?**
  - → How many random bits are generated before detection?
- **Detection depends on the call frequency of the online tests**
  - → How many online tests are performed before detection?
  - → Minimal number of online tests to ensure a good probability of detection?

→ **Estimation of the probability of detection of the online test p**

$N =$ number of online tests to reach a detection

N follows a geometric law of parameter p

$P[N \leq k] = 1 - (1-p)^k$

If a good probability of detection is 95%

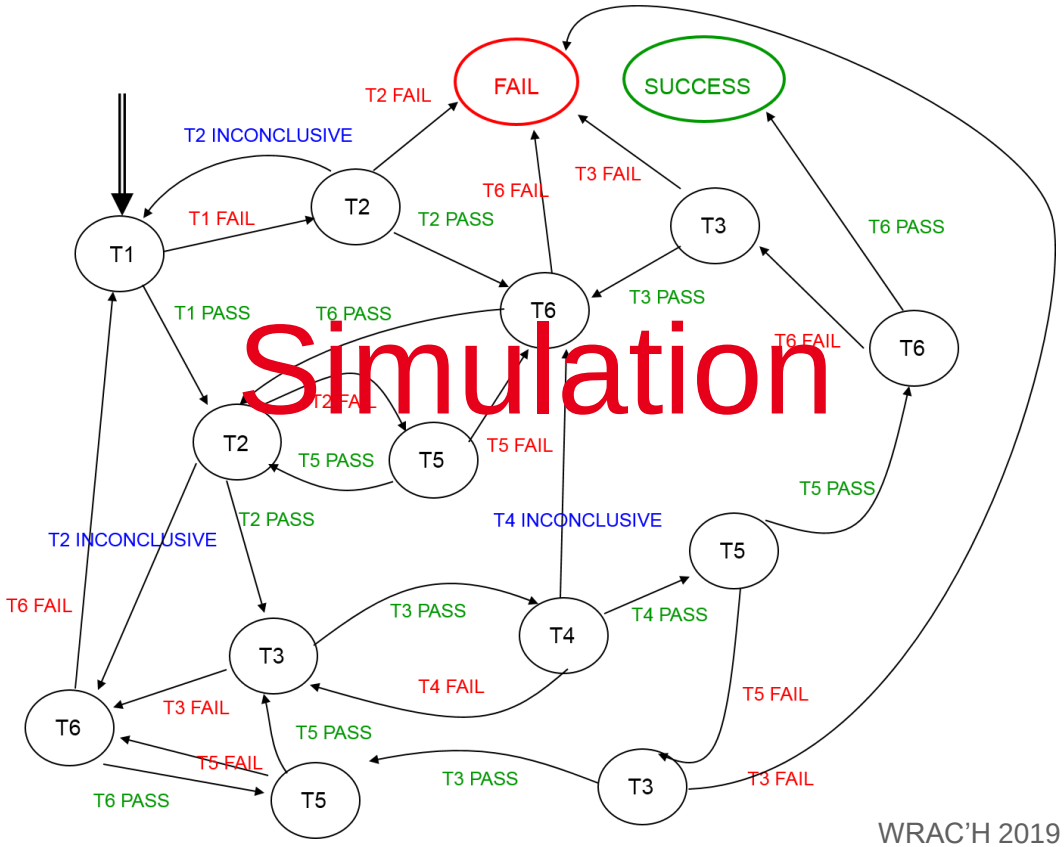
$$k = \frac{\log(1-0.95)}{\log(1-p)}$$

ONLINE TESTS

- Estimation of the probability of detection of the online test p

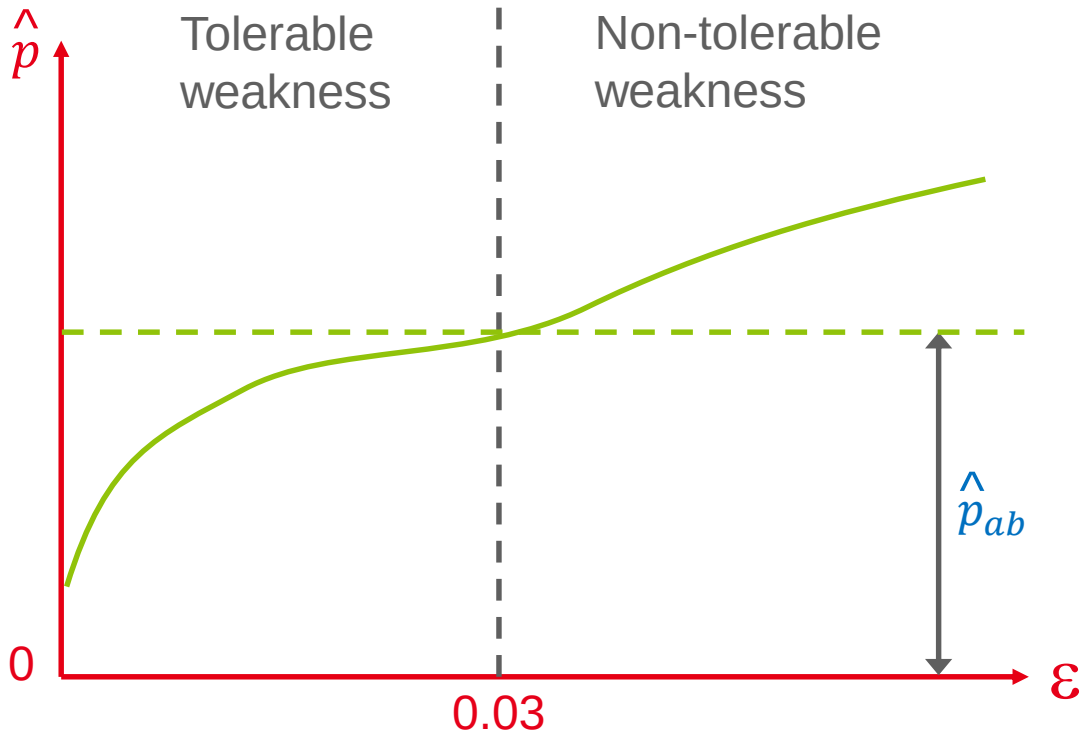
→ Study of the statistics defined by the online test

- But sometimes the online test is a very complex procedure!



ONLINE TESTS - SIMULATION

- **Simulation of the Online test**
- **Simulation of a source with increasing degradation**
  → For example increasing bias ε
- **Estimation of probability of detection** p
  → $\hat{p}$ = Mean number of times the online tests returns FAIL



$\hat{p}_{ab}$ probability of the detection of a non-tolerable weakness

$$k = \frac{\log(1 - 0.95)}{\log(1 - \hat{p}_{ab})}$$

→ Minimal number of online tests for 95% of detection

→ Minimal number of generated bits for 95% of detection

OUTLINE

- Evaluation Lab
- Random Number Generators
- **Evaluation of RNG**
  - Acquisition
  - Statistical Tests
  - Online Tests
  - **Penetration Tests**
- **Conclusion & Perspectives**

ATTACKS

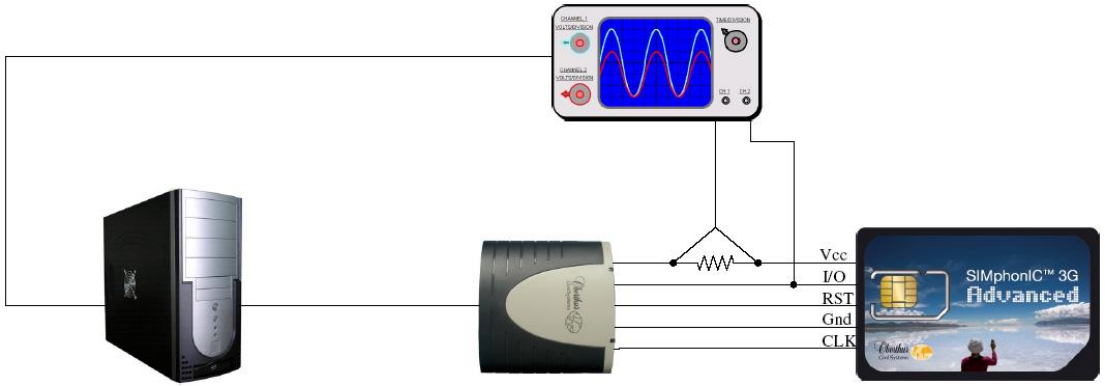
- **Threats**
  - Total failure
  - Randomness quality degradation
  - Random number leakage

- **Attack methods**
  - Observation
  - Perturbation
  - Environment alteration
    - Temperature
    - Clock frequency
    - Voltage

} A combination of these methods

PROFILING ATTACK ON RNG: PRINCIPLE

- **Measure during random number generation**
  - Power consumption
  - Electromagnetic radiation
  - …

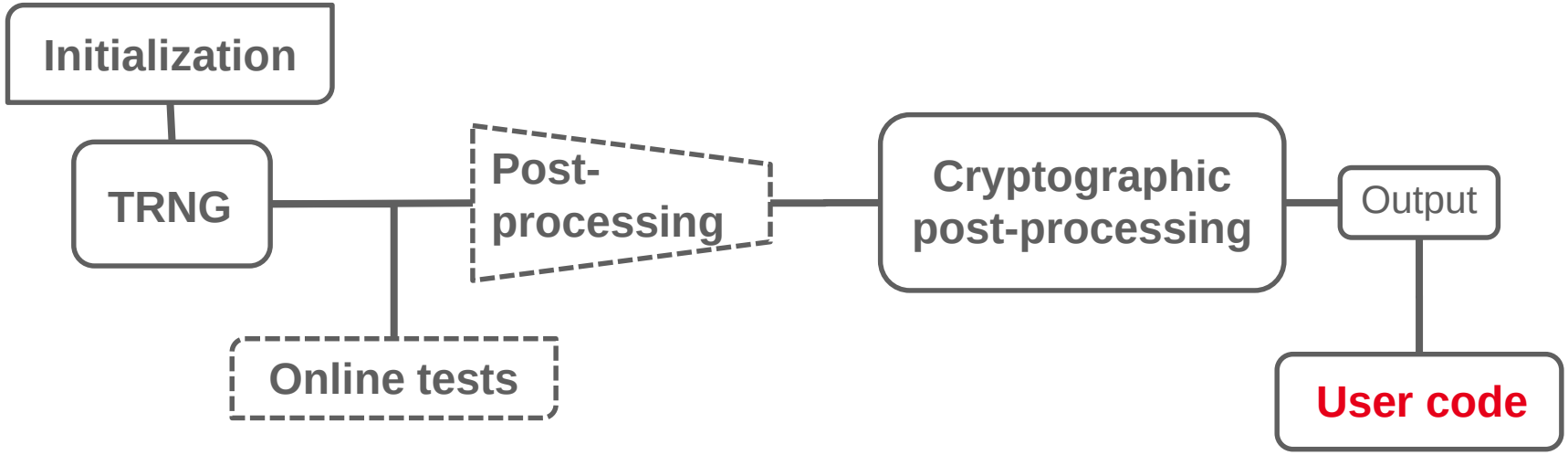


Source: C. Giraud, Attaques de cryptosystèmes embarqués et contre-mesures associées, rapport de thèse - 2007

- **Two phases**
  - Profiling
    - Characterization of the leakage with respect to known bits (learning)
  - Attack
    - Retrieving unknown random bits thanks to the profiling

PROFILING ATTACK ON RNG: REMARKS

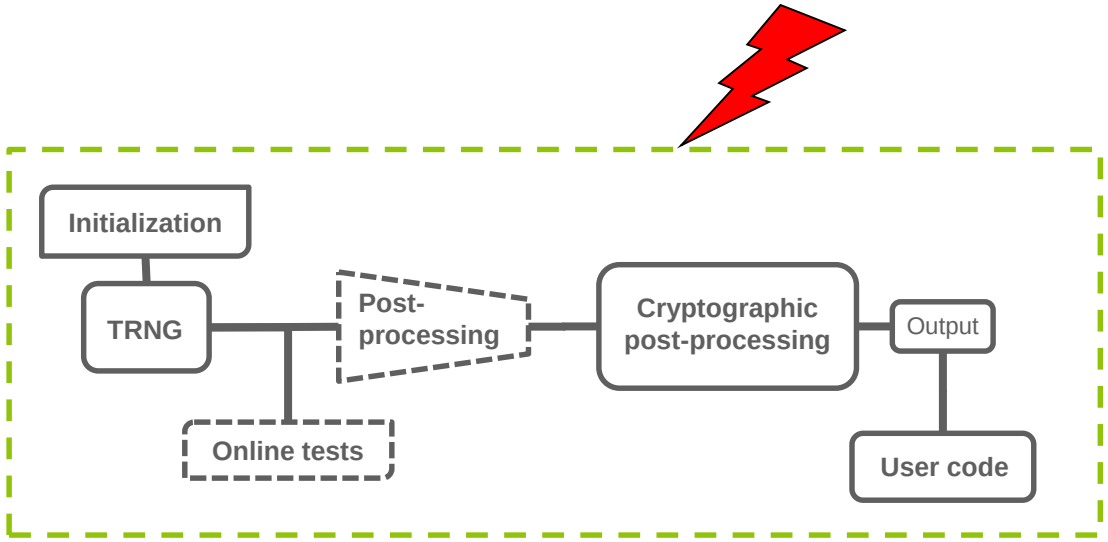
- **A random is not generated twice! (a priori)**
  → Success in only one observation
- **The RNG continously generates random numbers**
  → Difficulty of synchronization
- **Caution**



→ Everything may leak!

PERTURBATION ATTACK ON RNG

- **Fault injection**
  - Laser



- **Perturbation**
  - Random number register
    example: reset a bit
    → Need of multiple faults
    → Need of statistical tests

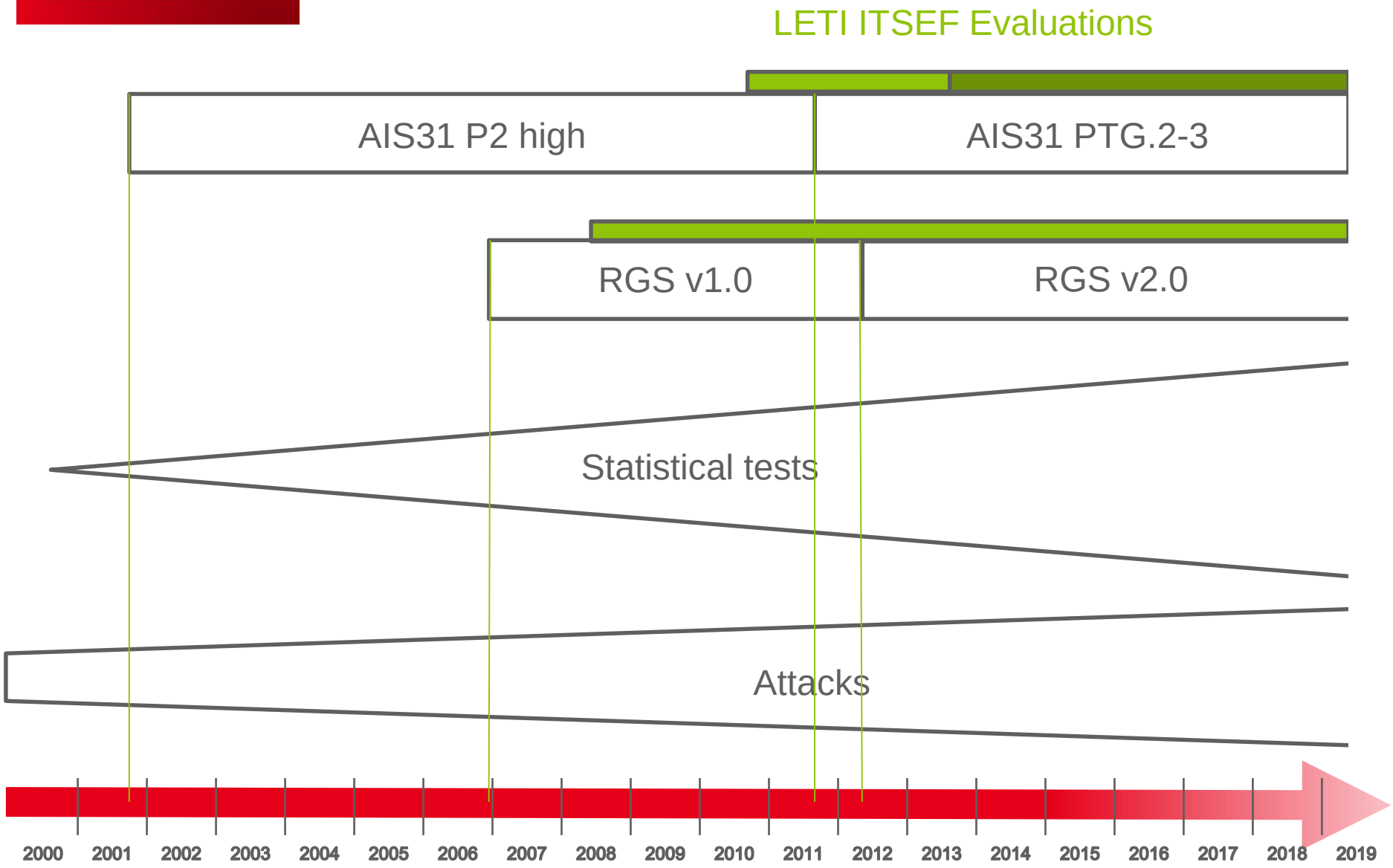
  - Control registers
    example: change the configuration
    → Need of only one fault
    → Visible effect

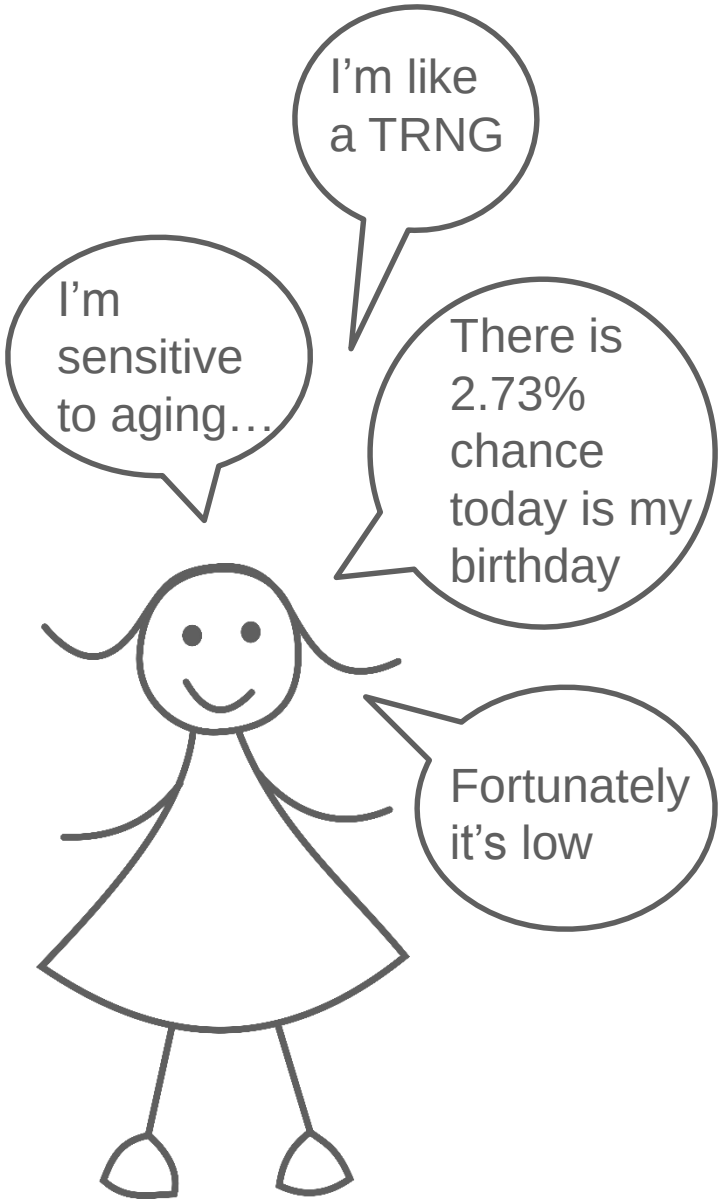
  - The user code
    examples:
    - Bypass the call of RNG
    - Bypass the post-processing
    - Bypass the call of the Online test

OUTLINE

- Evaluation Lab
- Random Number Generators
- Evaluation of RNG
- **Conclusion & Perspectives**

CONCLUSION


LETI ITSEF Evaluations
AIS31 P2 high
AIS31 PTG.2-3
RGS v1.0
RGS v2.0
Statistical tests
Attacks
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019



THANK YOU!

QUESTIONS?

Commissariat à l’énergie atomique et aux énergies alternatives
17 rue des Martyrs | 38054 Grenoble Cedex
www.cea-tech.fr

Établissement public à caractère industriel et commercial | RCS Paris B 775 685 019