

PUF RELIABILITY

AN INNOVATIVE TEST HARNESS FOR VALIDATION

Valentin PELTIER

Lukas VLASAK

1.

Introduction to PUF & Objectives

2.

Characterization process & Automation

3.

Accelerated aging procedure

4.

Analysis & Data exploration

5.

Conclusion

A series of red geometric shapes, including rectangles and parallelograms, arranged in a dynamic, overlapping pattern on the left side of the slide. Some shapes have thin white outlines and shadows, giving them a 3D appearance.

1. INTRODUCTION TO PUF & OBJECTIVES

HARDWARE SECURITY BASIC PRINCIPLE: FIRST PROVISIONING

**Mission
and value
chain
coverage**



Security is handled by different providers at each step of the value chain

- First provisioning is the step in which we **inject the most important security assets**
- Such **assets needs to be kept secret**, from designer to final user
- Each party cannot **trust** each other in order to prevent the whole security of the system

**HOW TO MAINTAIN TRUST ON THE SENSITIVE ASSETS
INJECTED DURING FIRST PROVISIONING?**

HOW TO STORE SENSITIVE INFORMATION

CRITICAL SECURITY PARAMETER (CSP) STORAGE ON SECURITY CHIPS.

- Traditional methods for storage:
 - OTP components
 - Non-Volatile Memories
 - Hard coded in the RTL

STORED VALUES MAY BE EXTRACTED AND COPIED

- Advanced memory read-out
- Reverse-engineering
- Physical attacks such as Probing

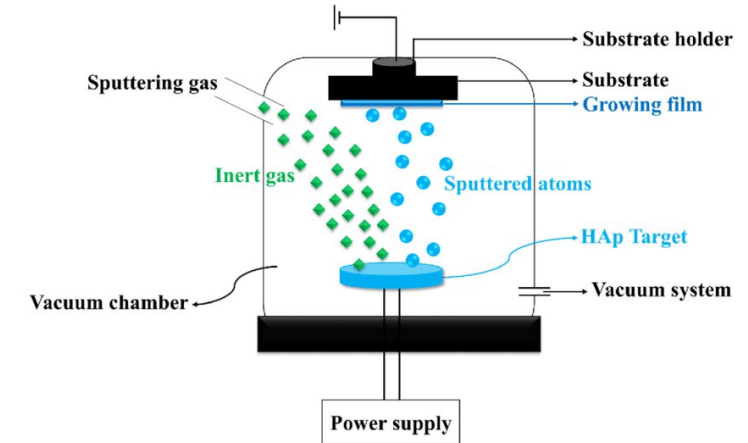
CAN WE STORE INFORMATION WITH SOMETHING DIFFERENT THAN A MEMORY?

PHYSICAL UNCLONABLE FUNCTION: A COMMON SOLUTION TO THOSE ISSUES

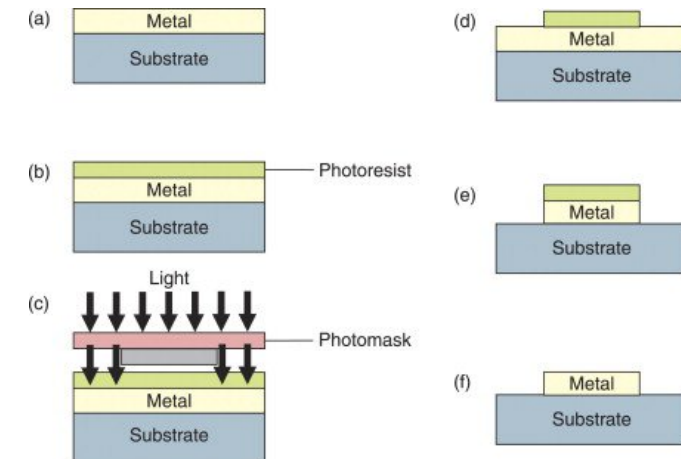
SEMICONDUCTOR MANUFACTURING STEPS GENERATES RANDOM PATTERNS ON THE CHIP

- Trench structures
- Thermal effect
- Lattice structures
- ...

- Those patterns can be leveraged on as the chip footprint that will be used to generate the sensitive information
- This way we don't trust anyone and prevent ourselves from attacks



Physical Vapor Deposition



Photolithography

PUF ARE DEFINED AS CHALLENGE-RESPONSE PROTOCOLS (CRP)

- The biggest the challenge domain is the “strongest” the PUF is seen
- A “**weak**” PUF use a small set of CRPs, meaning that an attacker may be able to retrieve all of them if he has access to the device
- On the other hand, the “**strong**” PUF use a lot of CRPs so the attacker cannot retrieve all of them

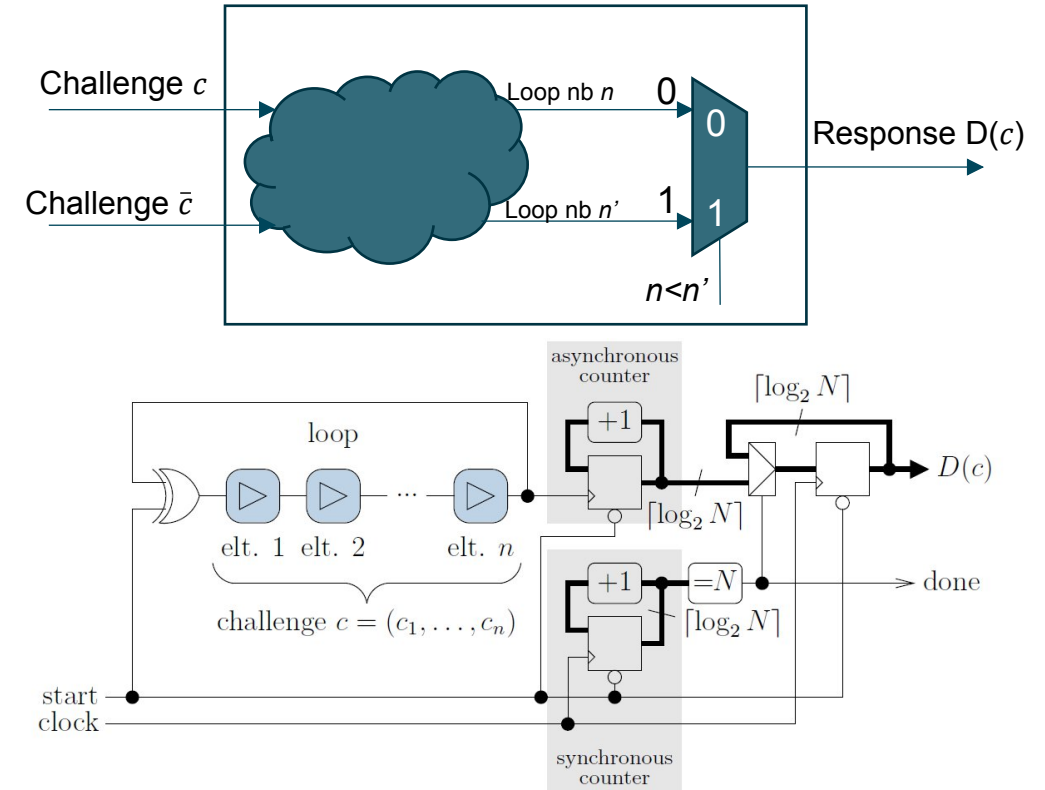
USAGES

- Weak PUF are usually used to store a small number of cryptographic keys
- Strong PUF are used as a building block of an authentication protocol

PUF type	Weak PUF/Strong PUF
SRAM	WEAK
VIA	WEAK
METAL	WEAK
NVM	WEAK
RO	STRONG
LOOP (Secure-IC)	STRONG

LOOP PUF WORKING PRINCIPLE

- The LOOP PUF look at the **propagation delay** (or oscillation number) inside the system
- Two complementary challenges c and \bar{c} are sent to the PUF
- Arbitrary if $\text{delay}(c) > \text{delay}(\bar{c})$ then the output is a 0. The output is a 1 for the opposite situation
- LOOP PUF specificity is that it allows to repeat this checking to improve the reliability of the PUF

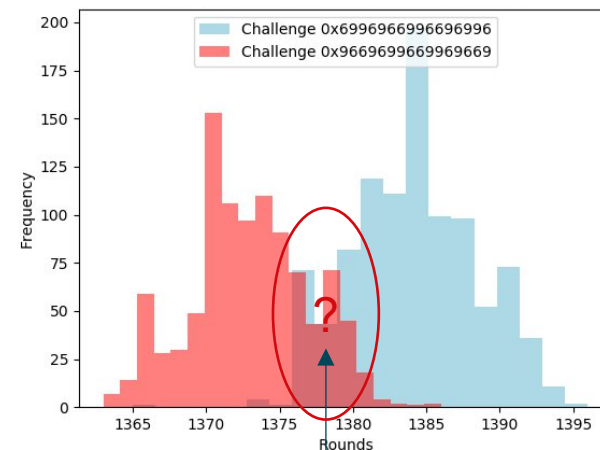
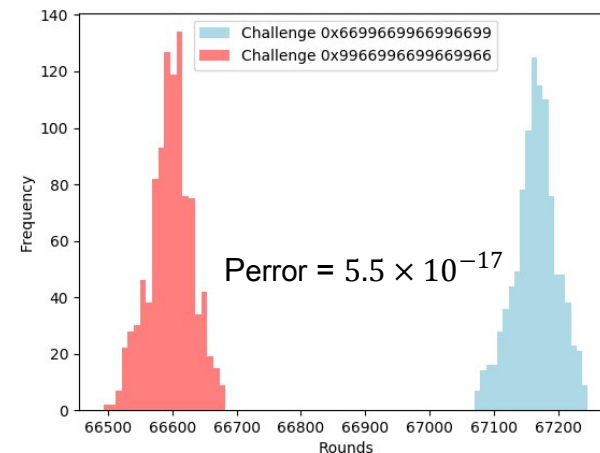


- PUF reliability is defined within the ISO/IEC 20897 standard
- The following criteria should be guaranteed:
 - **Unicity**
 - Bits sequence returned from two devices should be always different (physical dependency)
 - **Entropy**
 - Bits sequence returned should be unpredictable (randomness)
 - **Stability**
 - Bits sequence returned should be always the same (repeatability)

HOW TO MAINTAIN STEADINESS?

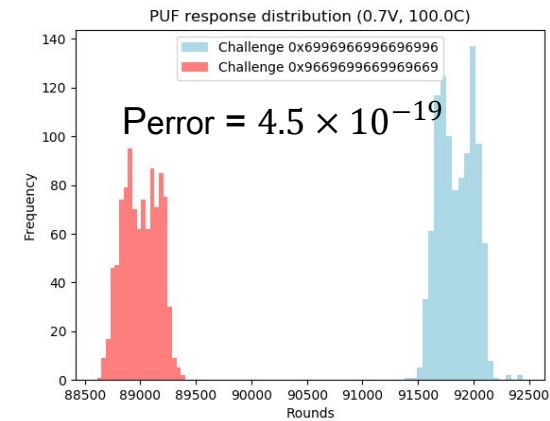
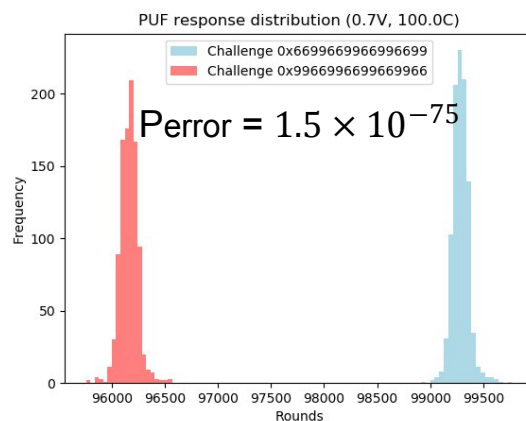
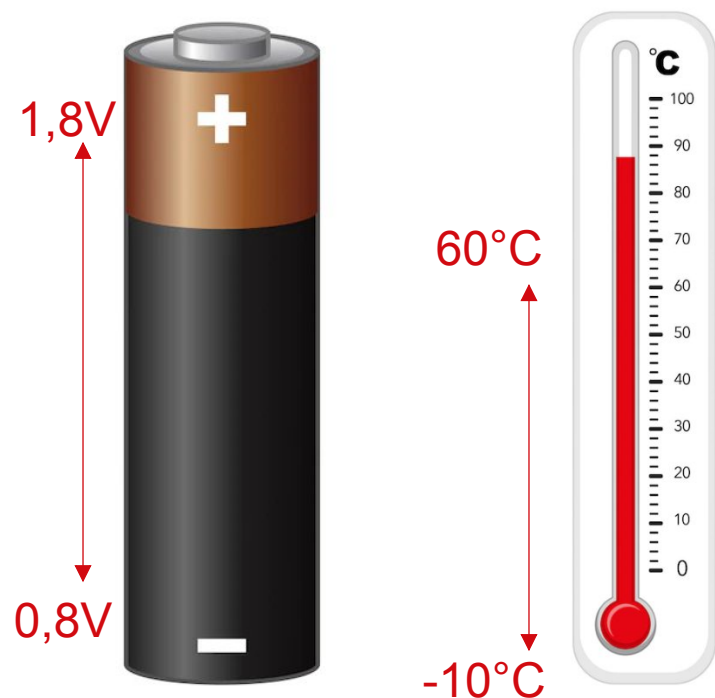
- For a given Challenge set c and \bar{c} , output (c and \bar{c} comparison) need to remain the same overtime and trials, whatever the environment conditions
- If the error rate is too big the PUF will lose its reliability, and the output will be random
- To avoid such, we can increase the number of looping performed by the IP (latency), at the cost of multiplying the response time, and we can ensure to have enough relevant challenges

Frequency distribution of a set of PUF responses for 1000 iterations



Sometimes $f_c > f_{\bar{c}}$, key bit is 1
Sometimes $f_c < f_{\bar{c}}$, key bit is 0

- PUF reliability whatever the **voltage** and **temperature** variation during **all** along the life cycle



- ☾ **ASSESS LOOP PUF RELIABILITY** (entropy, stability, unicity)
 1. Define a test harness sequence including physical constraints
 2. Define a relevant strategy for data analysis
 3. Explore which parameters and constraints affect reliability



2. CHARACTERIZATION PROCESS & AUTOMATION

PUF can be requested through two separate requests:

- **Enrollment**

- Refers to the process of selecting and record a reference response to a given input (challenge) from a PUF circuit



- **Rebuild**

- This operation reconstructs the key, without performing the enrollment procedure

We define the following operation making the Enrollment:

- ***Challenge request***

- Basic operation of PUF sources which, from an input challenge, return what is called a measurement (= oscillation number)

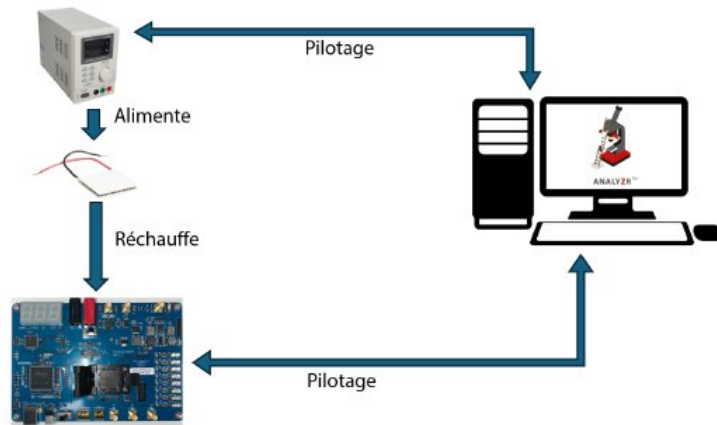
- 63 chosen challenges are stored locally
 - These challenges form a Hadamard matrix*, all with a Hamming weight of 32, and the distance between two challenges is exactly 32 => it excludes mathematical relation between two challenges
- Elementary *Challenge request* operations are applied for all challenges c and their complement \bar{c}
- **Select the 32 challenges** such that the difference between c and \bar{c} is the largest (=> key, helper data)
 - $f(c) - f(\bar{c})$ where f is the *Challenge request* (= oscillation number)
 - e.g.: 130  115 is selected, whereas 112  113 not

*Hadamard matrix: a square matrix whose entries are either +1 or -1 and whose rows are **mutually orthogonal**

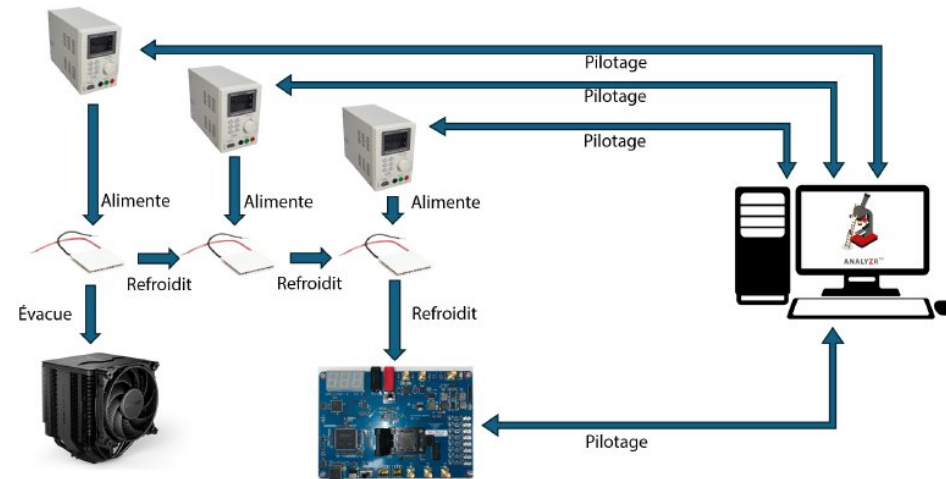
To perform the PUF analysis, several parameter are arbitrary explored (Characterization process):

- The **latency** indicates the number of clock cycles for the device to take a measurement
- The system will also be put through its limits in terms of **voltage** and **temperature** to observe the effects regarding PUF behavior
- A large number of requests (100) are sent to the PUF to gather enough data to be statistically relevant
- The main acquisition loop is as follow:
 - for *latencies* 10, 30, 50, 70 and 90 (Kilo clock cycles)
 - for *voltages* 0.95, 1.00 and 1.05 (Volts)
 - for *temperatures* 0°, ambient (~35°C), and 85°C
 - do $100\ f(c) - f(\bar{c})$ for all 63 challenges ($f = \text{Challenge request}$ \oplus oscillation number)

- Latency is a PUF input parameter controlled with the acquisition software
- Voltage is programmed from the acquisition software
- Temperature is monitored through a PID* system controlled by the acquisition software
 - It consists of a computer-controlled power supply that powers a **Peltier effect module** positioned on FPGA surface

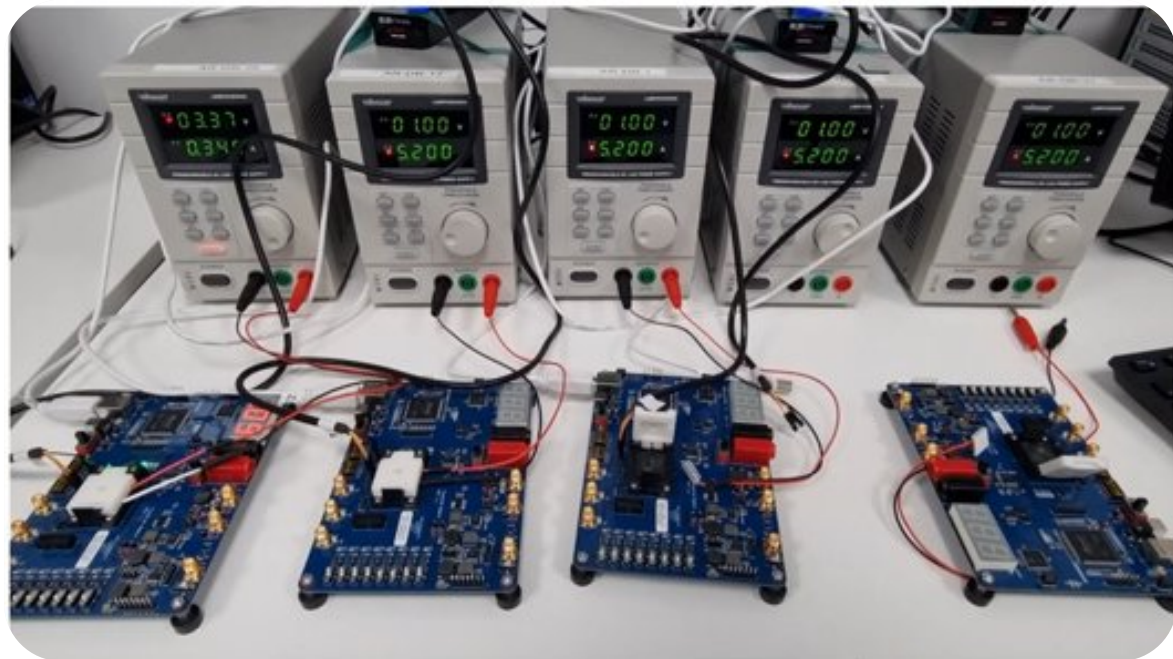


Connection for high temperature (85°C) = warming

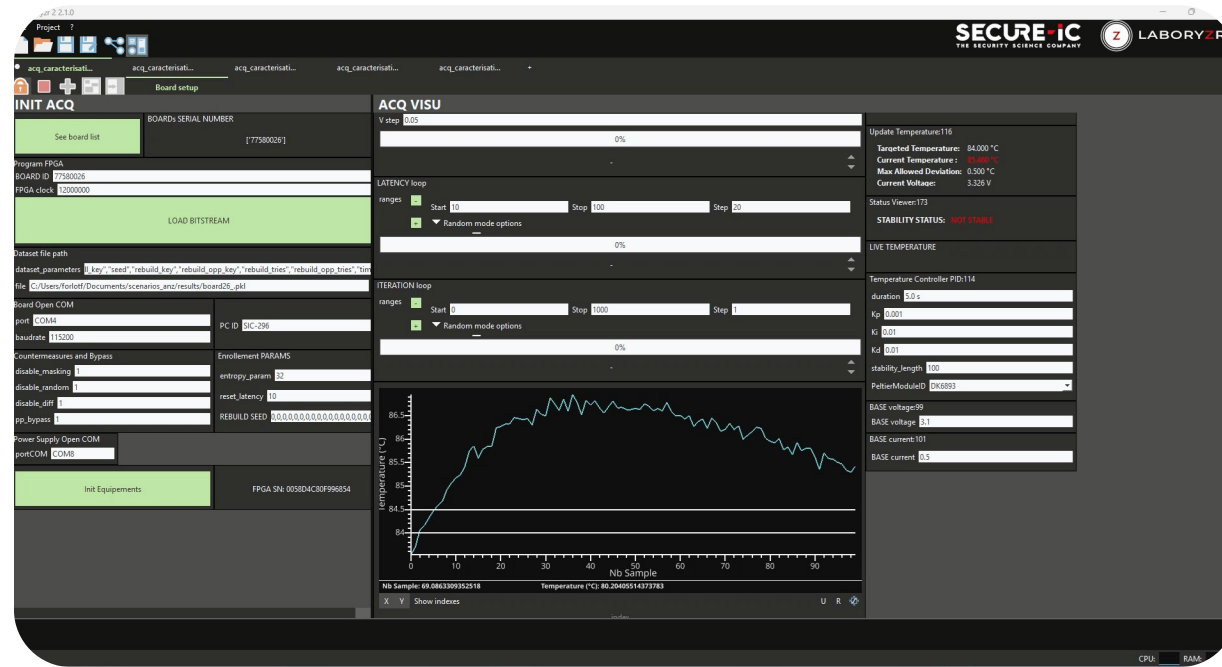


Connection for low temperature (0°C) = cooling

*PID: proportional–integral–derivative controller



FPGAs evaluation board and warming system connected to power control unit



Cooling system (a part of)

Secure-IC ANALYZR™ software from LABORYZR™ tools



ANALYZR™

- To assess unicity and stability, setup is repeated and compared across **100 FPGAs**. A half (50) include two characterization process, separated by an accelerated aging procedure.



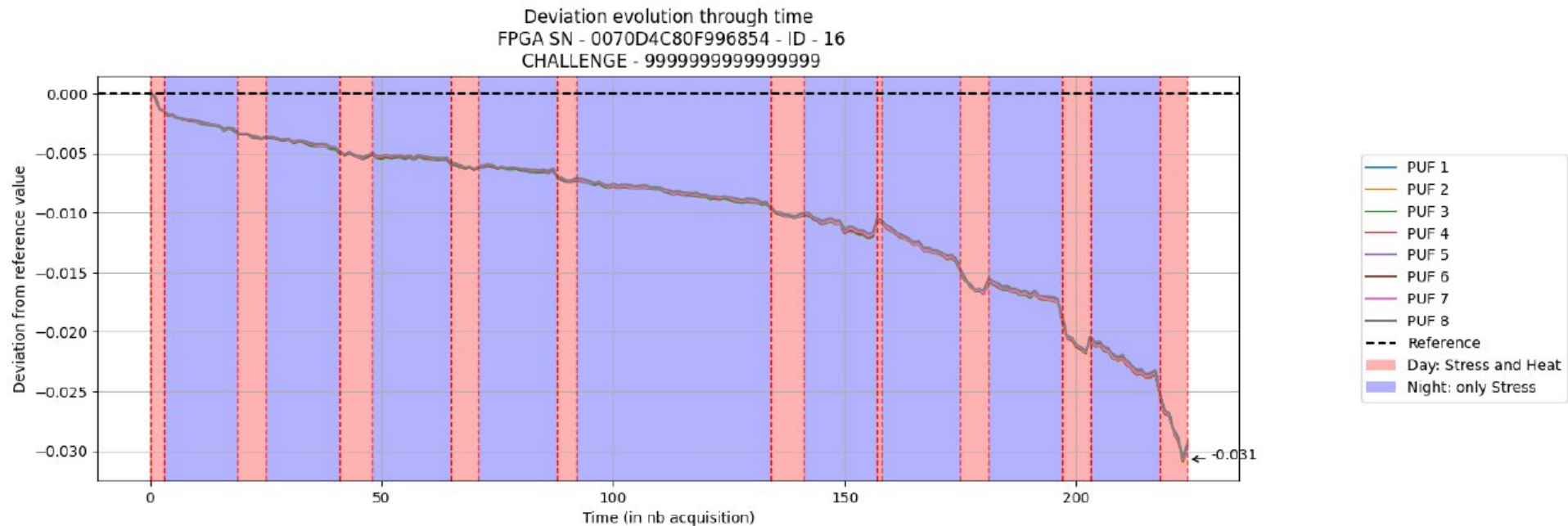
3. ACCELERATED AGING PROCEDURE

- To accelerate the natural aging process, an artificial aging procedure has been adopted based on experiments [1] for similar targets incorporating ring oscillators
- **NBTI** (Negative Bias Temperature Instability) and **HCI** (Hot Carrier Injection) are two major aging mechanisms that affect transistors in integrated circuits
- Combination of temperature, voltage, and logic activity accelerates degradation mechanisms such as NBTI and HCI

[1] Zeyu Li, Zhao Huang, Quan Wang, Junjie Wang, and Nan Luo. Implementation of aging mechanism analysis and prediction for xilinx 7-series fpgas with a 28-nm process. Sensors, 22(12), 2022.

- Accelerated Aging Scenario
 - Temperature stress: 85°C or 75°C (alternatively)
 - Voltage stress: 1.05V
 - Functional stress: Aging bitstream designed to continuously use more than 99% of the FPGA LookUp Tables (LUTs)
 - Stress is applied for **10 successive days, 24 hours** continuously.
 - PUF is evaluated **right after** end of accelerated aging process (**without recovery**)
- Continuous Monitoring:
 - Measurements on PUF-bitstream are performed every 60 minutes to monitor aging effect evolution

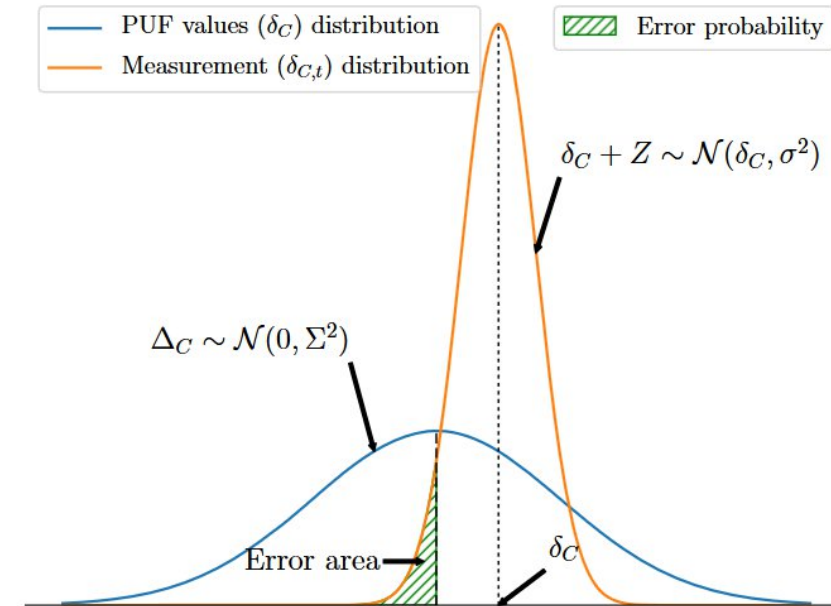
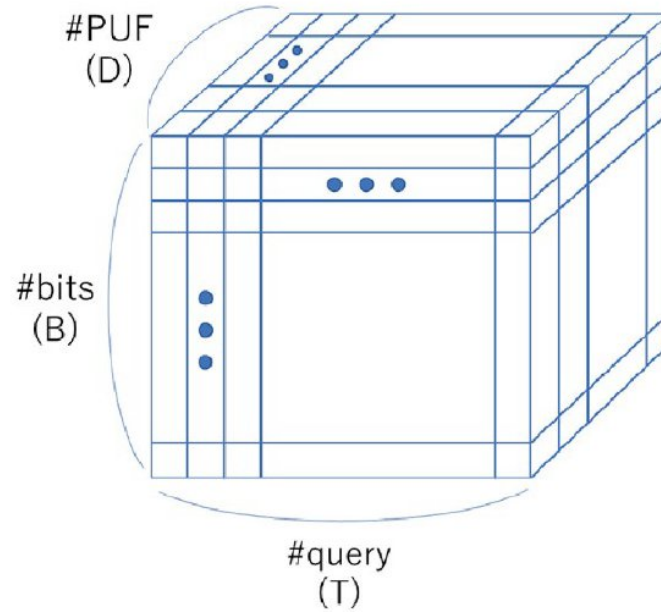
- The metric used to measure aging procedure effect is the evolution of **relative deviation** between measurements at a given time and the original measurement



Deviation from reference value over the time



4. ANALYSIS & DATA EXPLORATION



- ISO/IEC NP 20897. Information technology - security techniques - security requirements, test and evaluation methods for physically unclonable functions for generating nonstored security parameters.

■ Stability

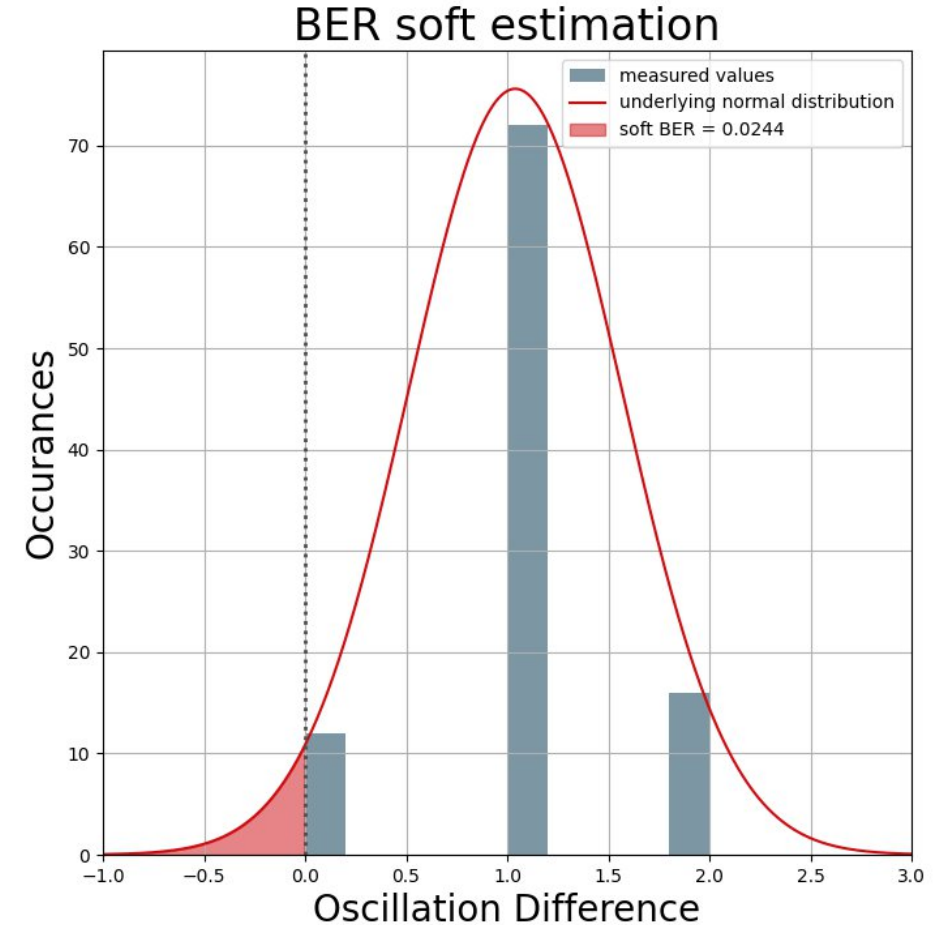
- Success rate
 - Fail criterion: < 90%
- Intra HD:

$$\frac{1}{T} \sum_{i=1}^T \frac{HD_{\text{intra}}(R, R_i)}{B} \in [0, 1]$$

- On key (derived from raw data)
 - **Optimal value: 0**
 - Fail criterion: > 1
- BER
 - On raw data
 - Never 0
 - Probabilistic evidence
 - Fail criterion:

$$\#\{(p, c) \in PUF \times Chal \mid BER_p(c) < .001\} < 32$$

- Tetsufumi Tanamoto, Satoshi Takaya, Nobuaki Sakamoto, Hirotugu Kasho, Shinichi Yasuda, Takao Marukame, Shinobu Fujita, and Yuichiro Mitani. *Physically unclonable function using initial waveform of ring oscillators on 65 nm cmos technology*
- Alexander Schaub, Jean-Luc Danger, Sylvain Guilley, and Olivier Rioul. *An improved analysis of reliability and entropy for delay pufs.*



■ Randomness – NIST SP800-22

- Monobit Test



- Frequency within a block Test



- Runs Test



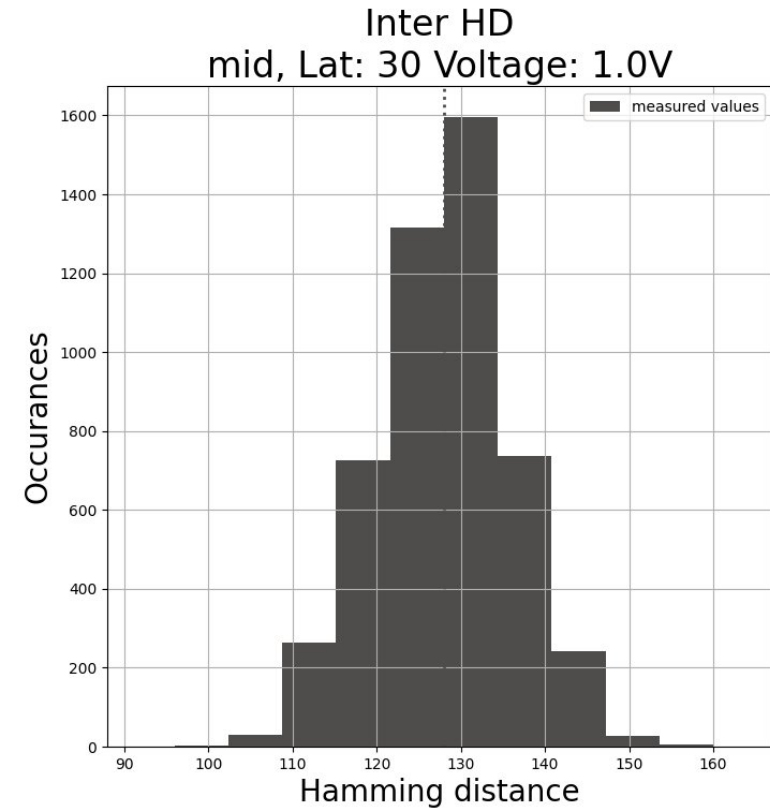
- *National Institute of Standards and Technology. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical Report 800-22 Rev 1a, U.S. Department of Commerce, Washing*

■ Uniqueness

- Inter HD:

$$\frac{2}{D(D-1)} \sum_{i=1}^{D-1} \sum_{j=i+1}^D \frac{HD_{inter}(R_t^i, R_t^j)}{B} \in [0, 1]$$

- For $D > 100$ devices
 - Fail criterion: > 60 or < 40
- Normal distribution with
 - $\mu = 0.5 B$
 - $\sigma = \sqrt{(B)/2}$
 - Fail criterion: value x with $6\sigma < |\mu - x|$



- Tetsufumi Tanamoto, Satoshi Takaya, Nobuaki Sakamoto, Hirotsugu Kasho, Shinichi Yasuda, Takao Marukame, Shinobu Fujita, and Yuichiro Mitani.
Physically unclonable function using initial waveform of ring oscillators on 65 nm cmos technology

■ Stability – BER

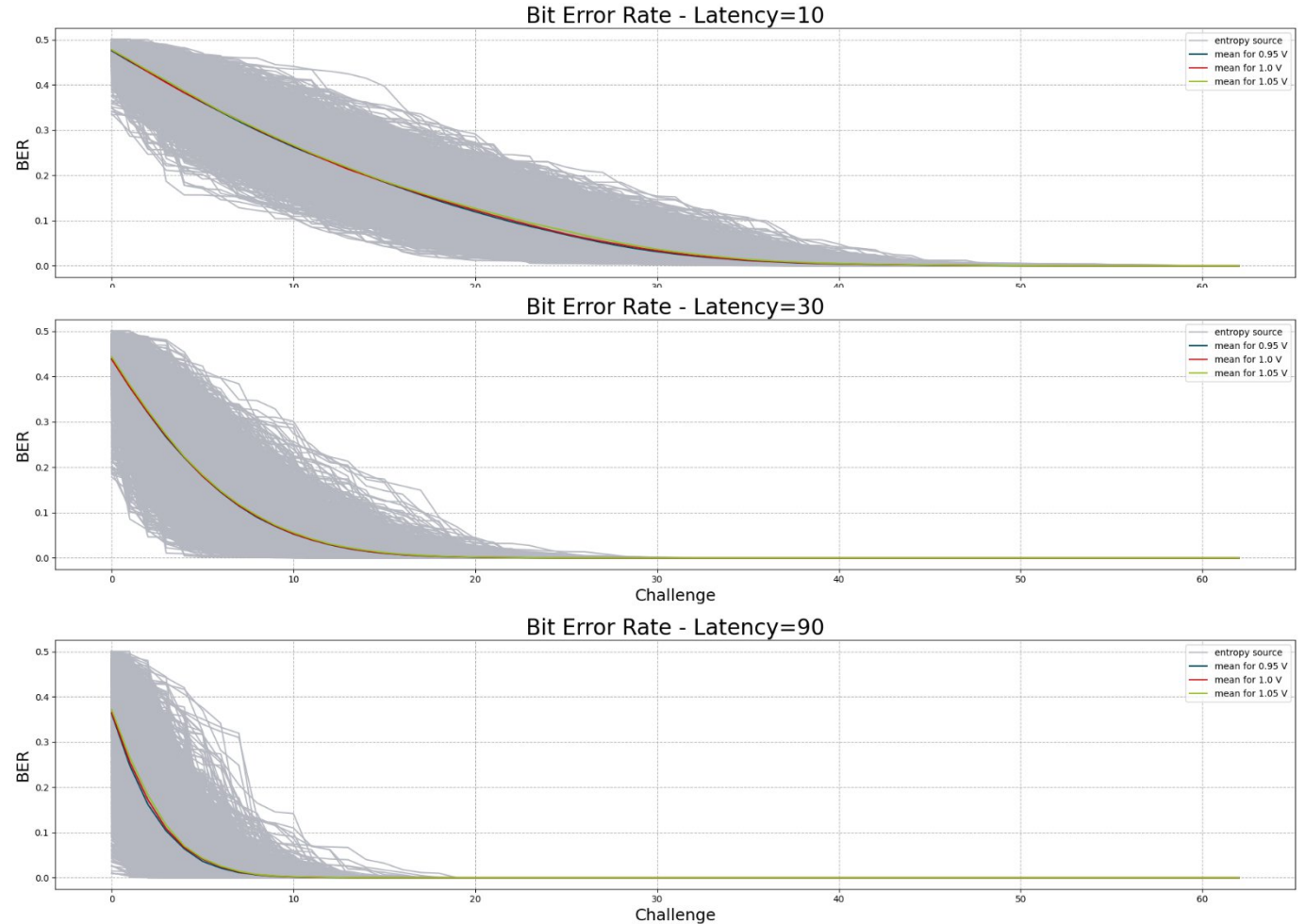
Latency 10: 44
(Min: 15)



Latency 30: 800
(Min: 33)



Latency 90: 800
(Min: 44)



100 FPGA with 8 PUF entropy sources each are tested for 63 challenges

■ Stability - BER

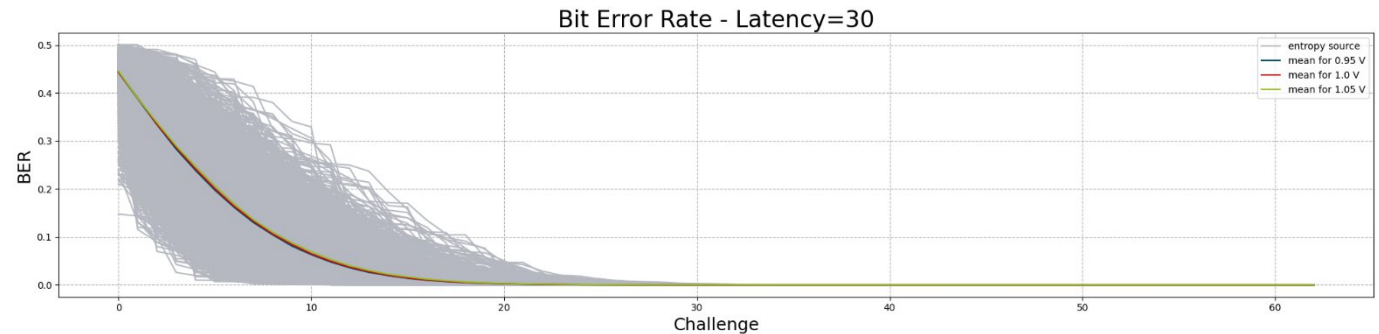
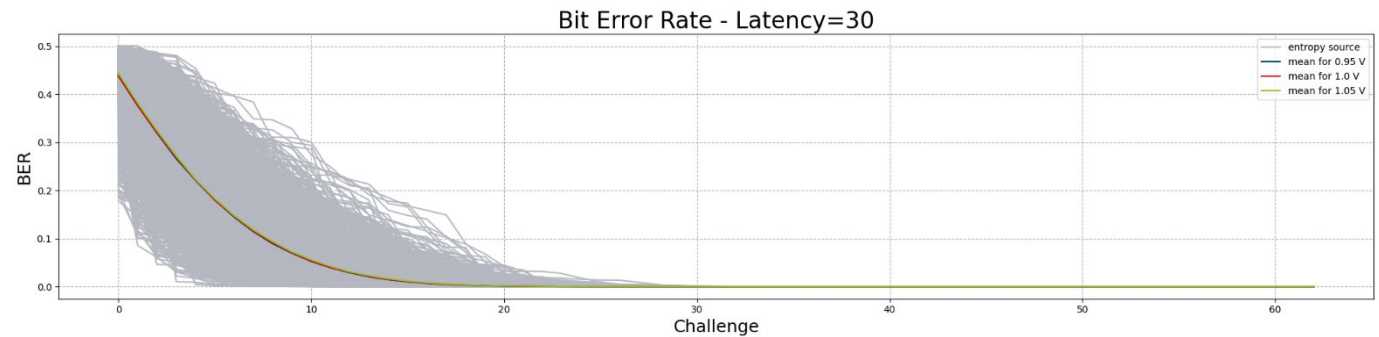
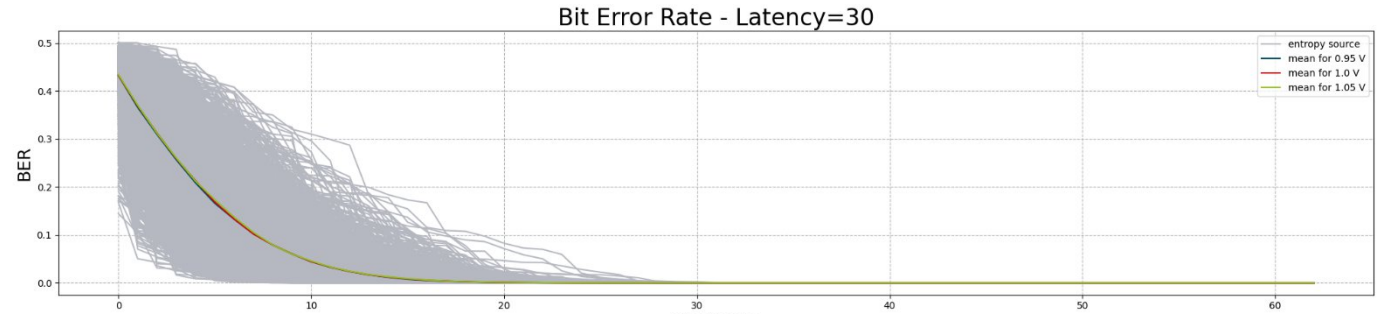
Cold: 800
(Min: 33)



Room Temperature: 800
(Min: 33)



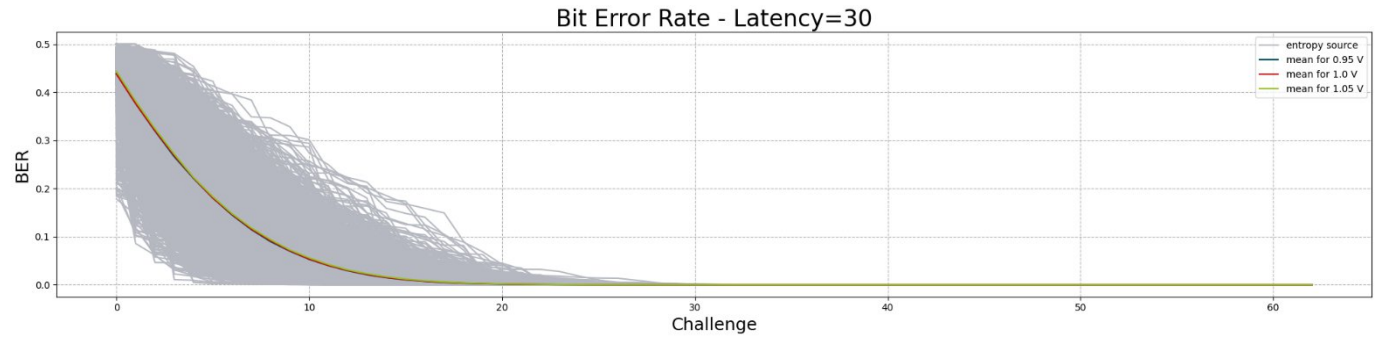
Hot: 799
(Min: 31)



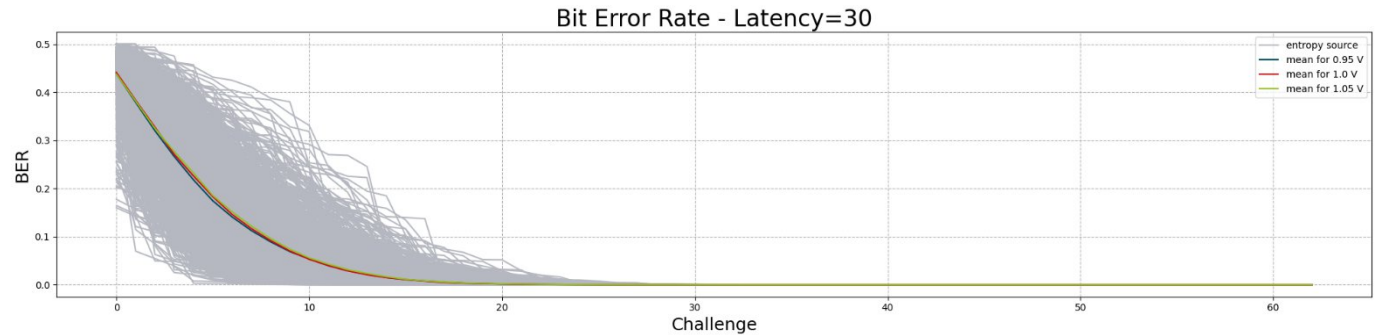
100 FPGA with 8 PUF entropy sources each are tested for 63 challenges

■ Stability - BER

Before aging: 800
(Min: 33)

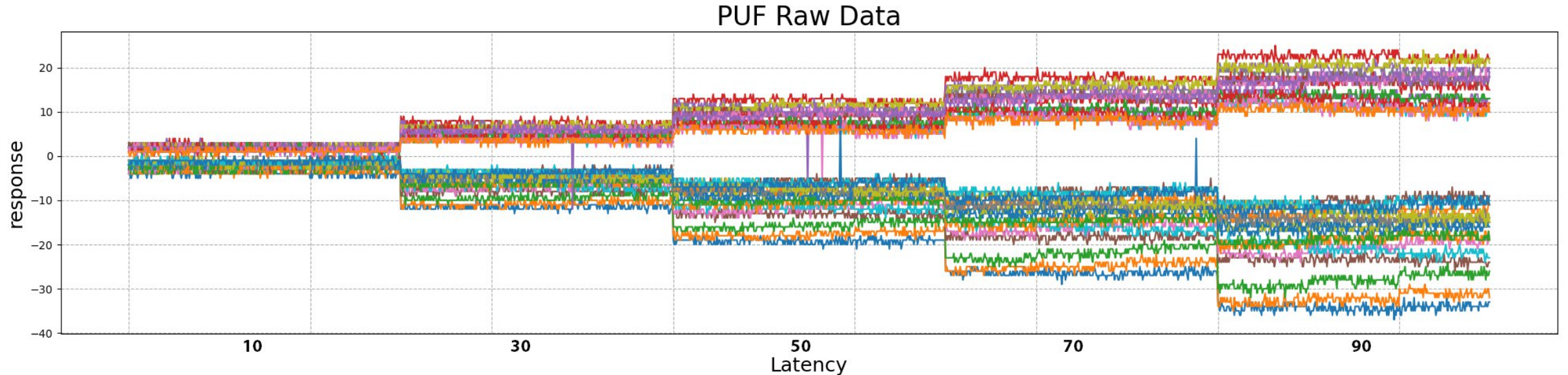


After aging: 400
(Min: 34)



50 aged FPGA with 8 PUF entropy sources each are tested for 63 challenges

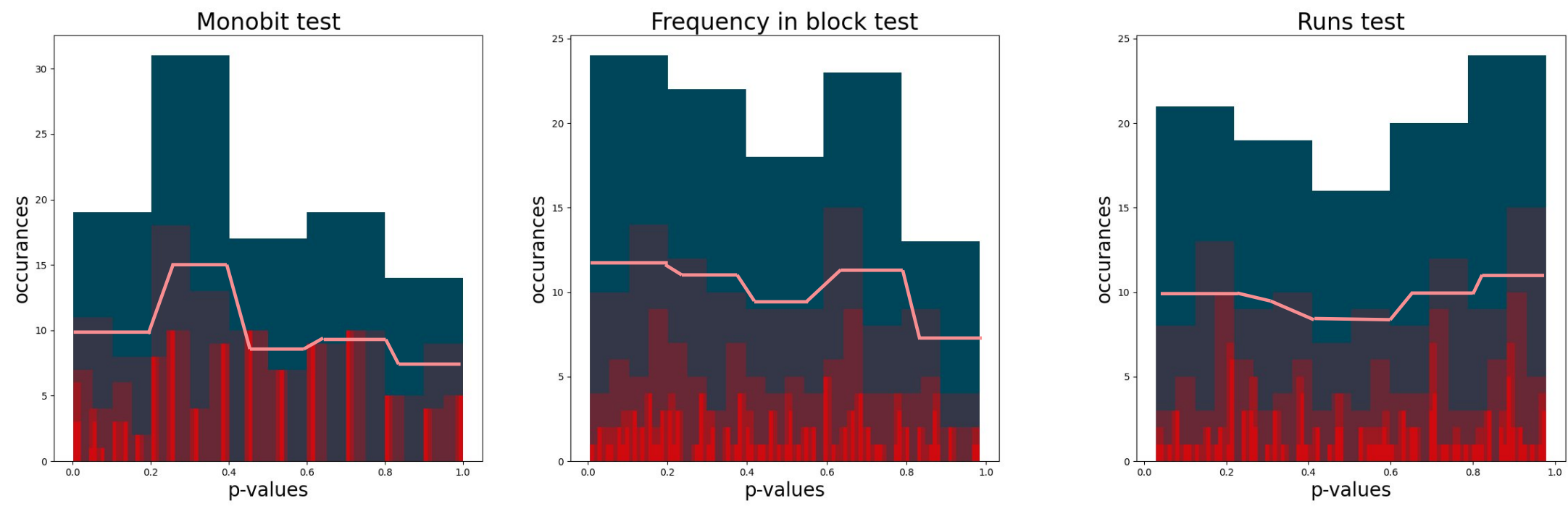
■ Stability challenges



Fix:

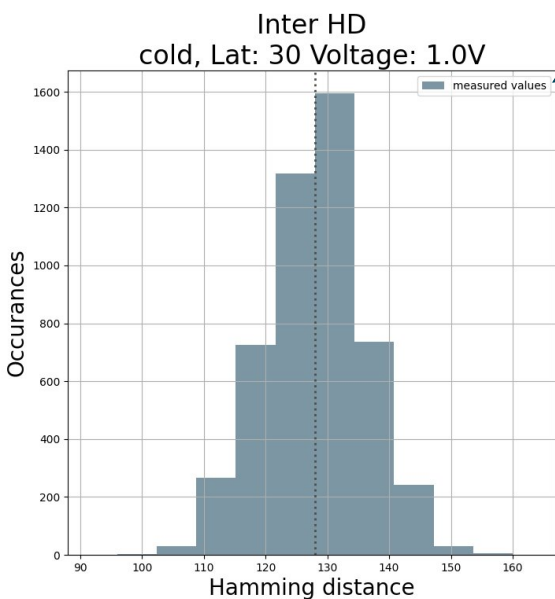
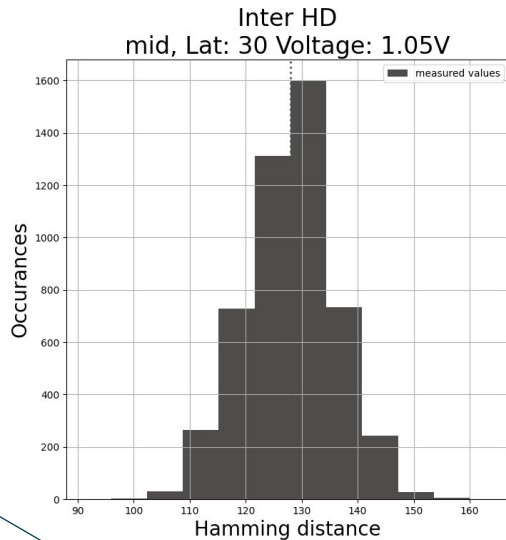
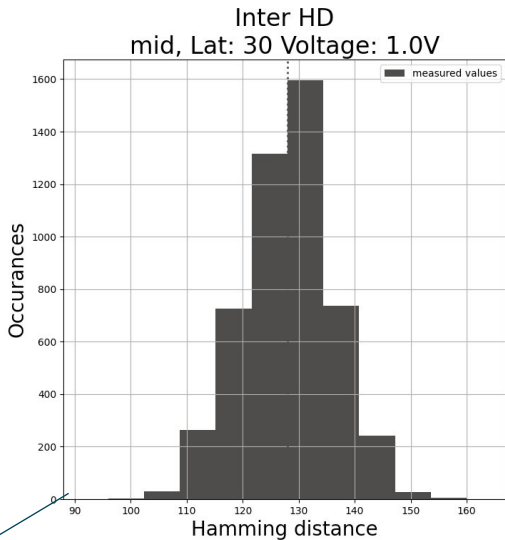
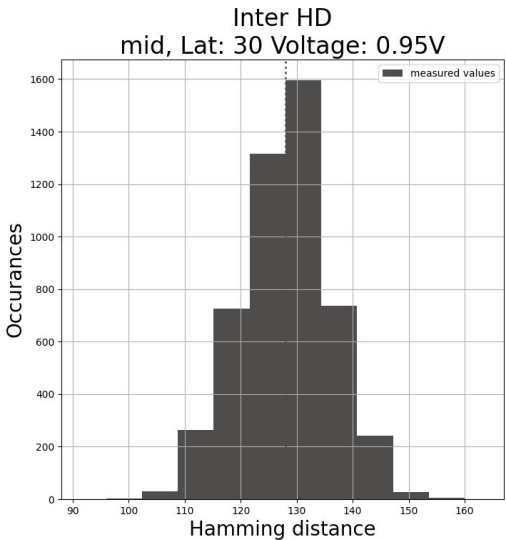
- inbuild error correction already fixes most of the unstable keys
- rebuild verification with hashed key
- retry
- 100% stability

■ Randomness



TESTING METRICS

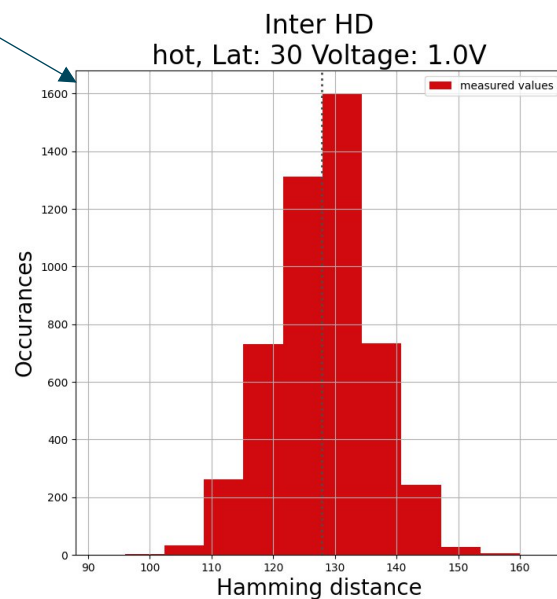
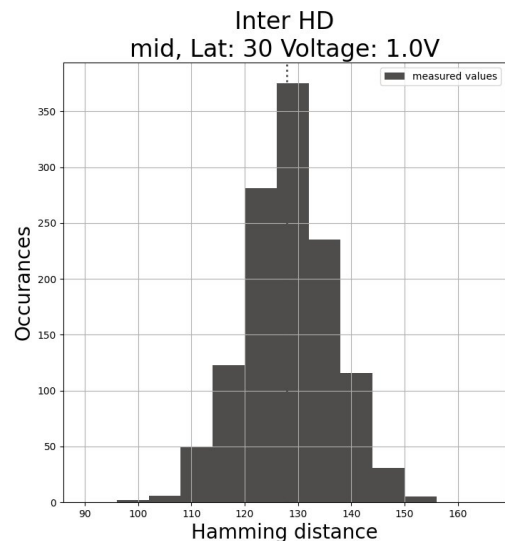
■ Uniqueness



cold

aging

hot



Abstract red geometric shapes, including rectangles and parallelograms, arranged in a dynamic, overlapping pattern on the left side of the slide.

5. CONCLUSION

- We have
 - gathered different evaluation metrics from literature
 - Stability
 - Randomness
 - Unicity
 - defined precise evaluation criteria
 - performed an automated campaign on 100 FPGA devices controlling for
 - Latency
 - Voltage
 - Temperature
 - Aging (2 months)
 - Explored and gathered output data
 - *(with excellent results for our design)*

- This work has received funding from European IPCEI Framework, BPI French contract “Soitec-SIC” n° DOS0220776 - DOS0220774
- Author: Khaled Karray, François Forlot, Idris Rais-Ali, Oualid Trabelsi, Lukas Vlasak

THANK YOU FOR YOUR ATTENTION

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
TAIWAN	sales-TAIWAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com

FOLLOW US ON SOCIAL MEDIA

