SECURE-IC
THE SECURITY SCIENCE COMPANY

Entropy and Reliability of the Loop-PUF

Speaker: Sylvain GUILLEY, Ph.D.,

Co-Founder & CTO

Date: November 20th, 2024

Place: Couvent des Jacobins, Rennes

Reference: Product SCZ_IP_PUF_200

European Cyber Week by Pole d'Excellence Cyber
THE SOVEREIGN CYBER & DEFENCE AI FORUM

Version 3.0

1. INTRODUCTION

SECURE-iC
THE SECURITY SCIENCE COMPANY

PUF: WHY?

CHALLENGE

- **Critical Security Parameter (CSP) storage on crypto chips.**
  - Traditional methods for storage:
    - OTP components
    - Non-Volatile Memories
    - directly in the RTL

DRAWBACK

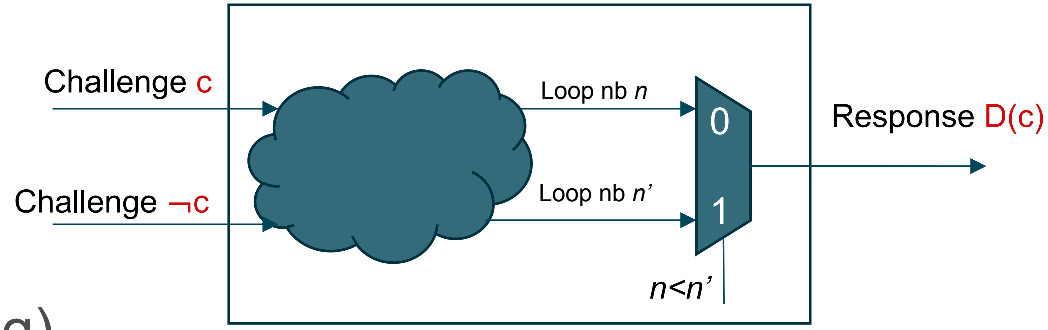
- **Stored values may be extracted and copied**
  - By memory read-out advanced techniques
  - By reverse-engineering techniques
  - With Physical attacks such as Probing

SOLUTION

- **Physically Unclonable Function (PUF)**
  - PUF generates volatile secret keys for a system
  - No need to inject keys

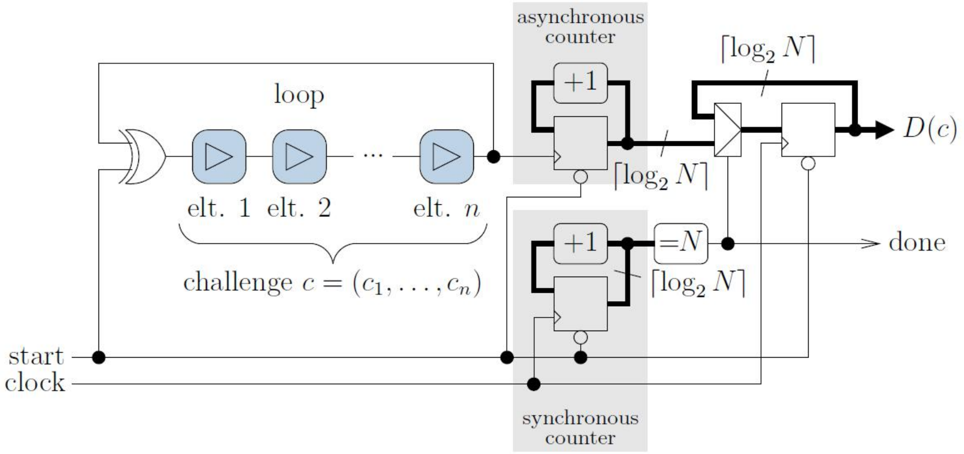
INTRODUCTION

- Generation of statistically independent sets of bits
- For a Challenge *c*, PUF generates a Response D(*c*) which depends on:
  - *c* and ¬*c* values
  - device physical properties due to manufacturing process variations
- Easy to evaluate
- But impossible to duplicate (physical cloning)
- And impossible to emulate (mathematical cloning)



High-level representation of PUF entropy source

- The output must be:
  - Random
  - Unique for a given device
  - Stable and repeatable
  - Unpredictable even with physical access



SECURE-IC : WORLD CLASS EXPERT ON PUF

- 40 scientific publications related to PUF
- 30 Patents related to PUF

Title	Application Number	Application Date	Status
SYSTEM AND METHOD FOR GENERATING SECRET INFORMATION USING A HIGH RELIABILITY PHYSICALLY UNCLONABLE FUNCTION	CN201711403449.2	22/12/17	Granted
SYSTEM AND METHOD FOR GENERATING SECRET INFORMATION USING A HIGH RELIABILITY PHYSICALLY UNCLONABLE FUNCTION	EP16306808.3	23/12/16	Pending
SYSTEM AND METHOD FOR GENERATING SECRET INFORMATION USING A HIGH RELIABILITY PHYSICALLY UNCLONABLE FUNCTION	KR10-2017-0178851	22/12/17	Granted
SYSTEM AND METHOD FOR GENERATING SECRET INFORMATION USING A HIGH RELIABILITY PHYSICALLY UNCLONABLE FUNCTION	US15/849949	21/12/17	Pending
SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION DERIVED FROM AN IMAGING SENSOR	CN201811219192.X	19/10/18	Granted
SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION DERIVED FROM AN IMAGING SENSOR	EP17306440.3	20/10/17	Pending
SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION DERIVED FROM AN IMAGING SENSOR	US16/161511	16/10/18	Granted
SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION	EP16306765.5	21/12/16	Granted
SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION	EP 16306765.5 DE	21/12/16	Granted
SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION	EP 16306765.5 FR	21/12/16	Granted
SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION	EP 16306765.5 GB	21/12/16	Granted
SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION	CN201780079544.3	20/12/17	Pending
SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION	US16/470209	20/12/17	Pending
SECRET KEY GENERATION USING A HIGH RELIABILITY PHYSICALLY UNCLONABLE FUNCTION	CN201711404471.9	22/12/17	Pending
SECRET KEY GENERATION USING A HIGH RELIABILITY PHYSICALLY UNCLONABLE FUNCTION	EP 16306809.1 DE	23/12/16	Granted
SECRET KEY GENERATION USING A HIGH RELIABILITY PHYSICALLY UNCLONABLE FUNCTION	EP 16306809.1 FR	23/12/16	Granted
SECRET KEY GENERATION USING A HIGH RELIABILITY PHYSICALLY UNCLONABLE FUNCTION	EP 16306809.1 GB	23/12/16	Granted
SECRET KEY GENERATION USING A HIGH RELIABILITY PHYSICALLY UNCLONABLE FUNCTION	KR10-2017-0178852	22/12/17	Granted
SECRET KEY GENERATION USING A HIGH RELIABILITY PHYSICALLY UNCLONABLE FUNCTION	US15/850231	21/12/17	Pending
EMBEDDED TEST CIRCUIT FOR PHYSICALLY UNCLONABLE FUNCTION	EP15306063.7	01/07/15	Pending
EMBEDDED TEST CIRCUIT FOR PHYSICALLY UNCLONABLE FUNCTION	HK17106383.3	27/06/17	Pending
EMBEDDED TEST CIRCUIT FOR PHYSICALLY UNCLONABLE FUNCTION	CN201680047612.3	01/07/16	Granted
EMBEDDED TEST CIRCUIT FOR PHYSICALLY UNCLONABLE FUNCTION	KR1020207020795	16/07/20	Pending
EMBEDDED TEST CIRCUIT FOR PHYSICALLY UNCLONABLE FUNCTION	US15/739820	01/07/16	Granted
DEVICE AND METHOD FOR TESTING APHYSICALLY UNCLONABLE FUNCTION	CN201710223312.2	07/04/17	Granted
DEVICE AND METHOD FOR TESTING APHYSICALLY UNCLONABLE FUNCTION	EP16305419.0	08/04/16	Pending
DEVICE AND METHOD FOR TESTING APHYSICALLY UNCLONABLE FUNCTION	KR10-2017-0045415	07/04/17	Pending
DEVICE AND METHOD FOR TESTING APHYSICALLY UNCLONABLE FUNCTION	US15/480729	06/04/17	Granted
CONNECTED SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION	EP18305929.4	11/07/18	Pending
CONNECTED SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION	CN201980046401.1	27/06/19	Pending
CONNECTED SYNTHETIC PHYSICALLY UNCLONABLE FUNCTION	US17/258143	27/06/19	Pending

STANDARDS

- Secure-IC is member of the Working Groups WG2 and WG3 of the Technical Committee ISO/IEC JTC 1/SC 27 which works on **ISO/IEC 20897** Security requirements, test and evaluation methods for physically unclonable functions for generating non-stored security parameter.
- Two parts:
  - ISO/IEC 20897-1:2020 Information security, cybersecurity and privacy protection — Physically unclonable functions. Part 1: Security requirements
  - ISO/IEC 20897-2:2022 Information security, cybersecurity and privacy protection — Physically unclonable functions. Part 2: Test and evaluation methods
- Editing committee:
  - (Lead) Sylvain Guilley
  - Hirofumi Sakane
  - Soshi Hamaguchi
  - Yousung Kang

Revision soon.

Call for contributions to be circulated.
Wish to write formal SFRs.

SECURE-IC'S PUF DEPLOYMENT

§ **ASIC**

- 65nm
- 55nm
- 40nm
- 28nm
- 22nm
- 14nm
- Foundries: ST, UMC, TSMC, Samsung, SMIC, GF

§ **Use-cases**

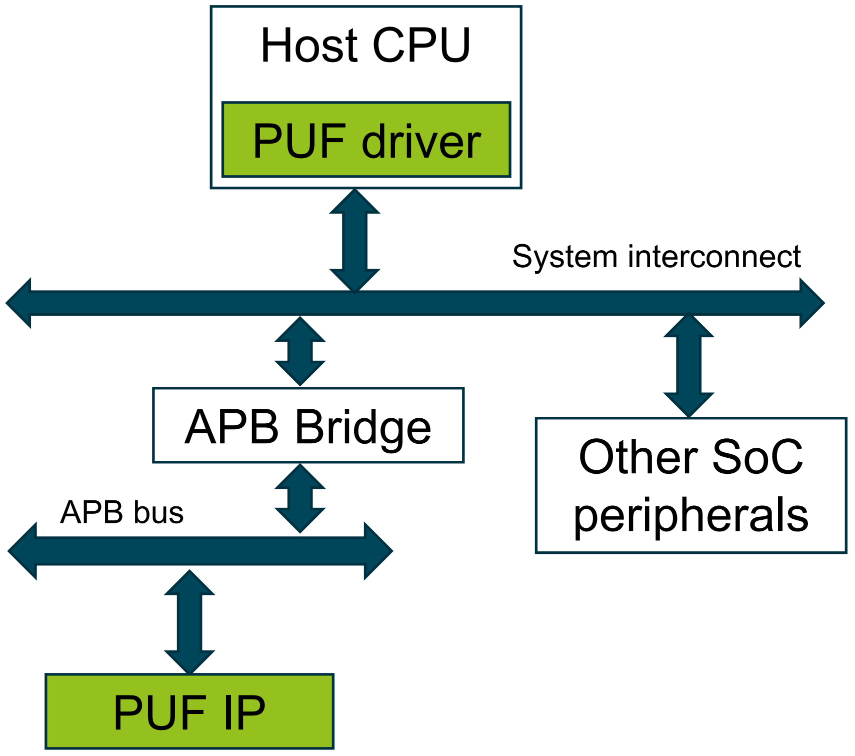
- Smart-meter/Connected Device
- Governmental component
- Crypto chip

§ **PUF error probability is defined with customer (usually $<10^{-9}$)**

2. OVERVIEW

SECURE-IC'S PUF INTERFACE

- Interface with AMBA wrapper (APB)
  - Provided by Secure-IC
- Control through registers



Provided by Secure IC

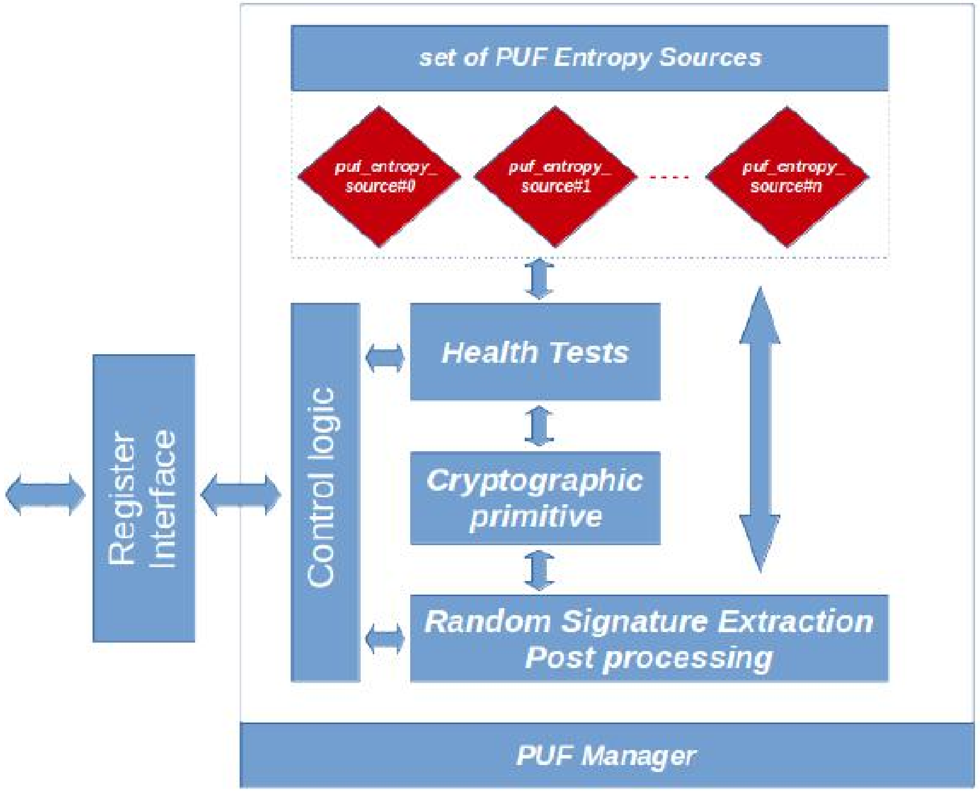
Not provided by Secure IC

3. ARCHITECTURE

ARCHITECTURE

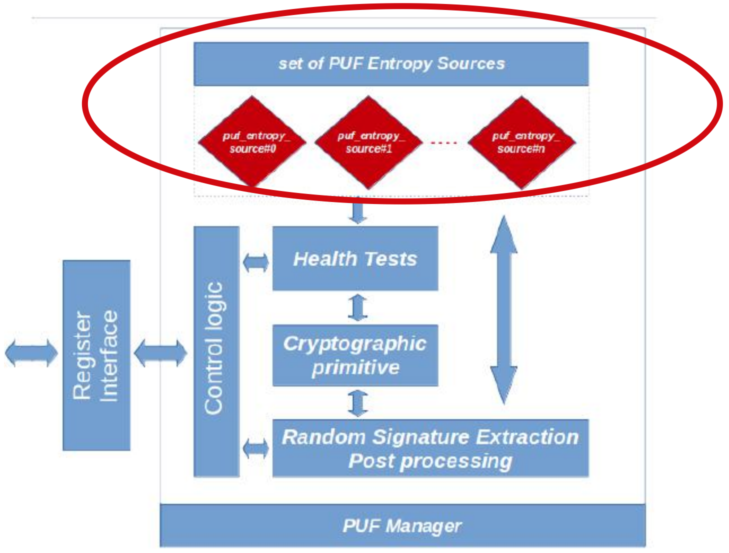
§ **2 main components delivered by Secure-IC:**

- PUF Manager
- Set of PUF Entropy Sources



SECURE-iC THE SECURITY SCIENCE COMPANY

ARCHITECTURE



§ PUF Entropy source

- Based on loop
- Each entropy source generates 32 bits (need 8 entropy sources to generate 256 bits key)
- Principle of key rebuilding:

“Bit-Challenge” = set of elementary commands c=(c1,…,cn)

Used to generate 1 bit through comparison of two sequential measurements

32 bit-challenges are run sequentially to get each bit of the key

Sequential measurement of frequency using c and $\underline{c}$

If $f_c > f_{\underline{c}}$, key bit is 1

Else $f_c < f_{\underline{c}}$, key bit is 0

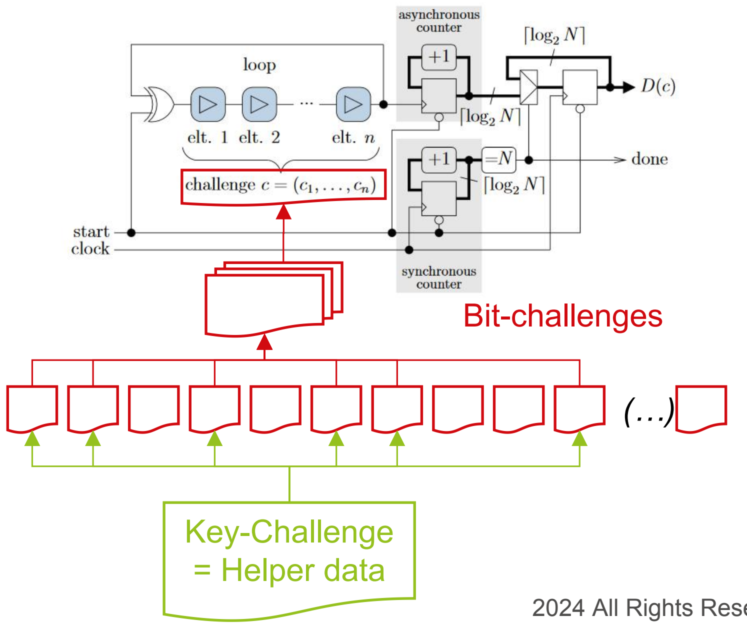
Key is rebuilt

Used to select 32 “Bit-Challenges” among 63 available bit-challenges

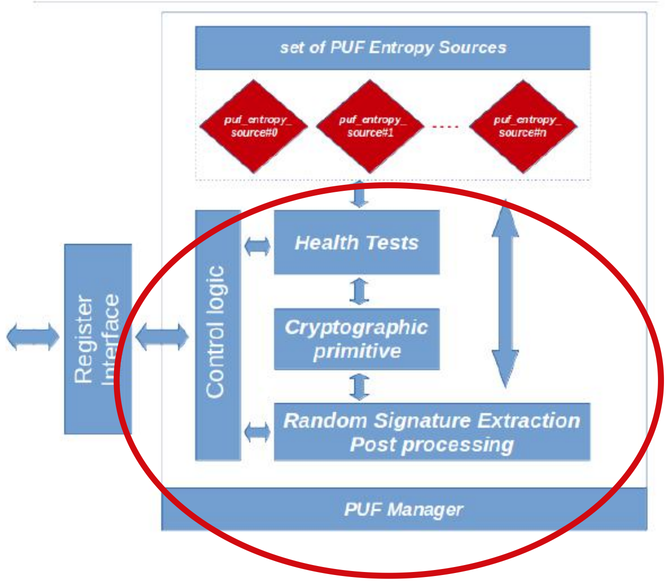
“Key-Challenge”

Helper Data

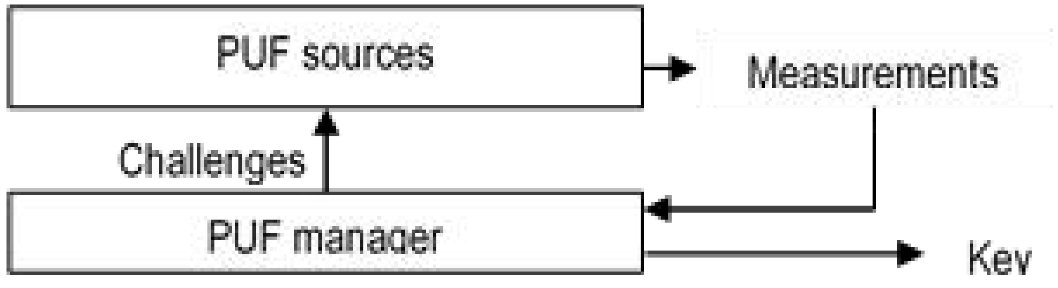
64-bits address



ARCHITECTURE



- **PUF Manager**
  - Controls the PUF entropy sources by giving various challenges. The measurements returned by the PUF entropy sources are processed by the manager to generate the key.



  - Ensures health-tests

4. THREATS AND COUNTERMEASURES

SECURE-iC
THE SECURITY SCIENCE COMPANY

OVERVIEW OF THE DIFFERENT THREATS ON PUF

- **Side-channel attack (SCA, Timing attacks).**
  - How does it work: side-channel measurement of loops frequencies.
- **Modeling attack (https://ieeexplore.ieee.org/document/6800562).**
  - How does it work: predict responses from never seen challenges.
- **Helper data manipulation (Replay of challenges).**
  - How does it work: divide-and-conquer where challenge set is narrowed down by duplicating challenges, ending by the repetition of only two challenges.
- **Challenge code splicing attack (Out-of-order hard-coded challenge lookup).**
  - How does it work: Find challenge equivalences by crafting challenge sequence. Reduce key domain bit-by-bit by looking for equivalent output of the PUF.
- **Invasive probing.**
  - How does it work: attacker probes the response bits.
- **Fault Injection Attacks (FIA).**
  - How does it work: Adversely change conditions to provoke changes in the PUF behavior (Clock glitch, Power glitch, EM or Laser injection, etc.)

PUF IS ATTACK-PROOF BY DESIGN!

Embedded health-tests

FIA, Invasive Probing

c and ¬c measurement order is random

SCA, FIA, Probing

Active Shield can protect digital parts after PUF output

FIA, Invasive Probing

Bit-Challenge order is random

SCA, FIA

Output passes through a crypto function, PUF output never gets out of the IP

Modeling, probing, SCA

Each Bit-Challenge runs only once

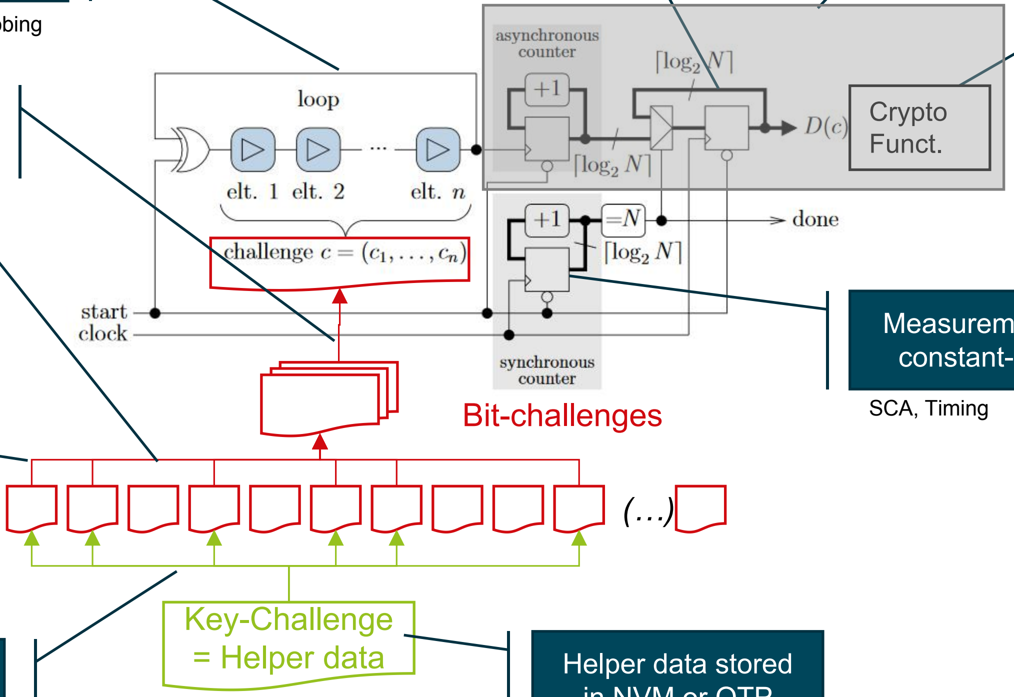
Replay (helper data manipulation)

Measurement is constant-time

SCA, Timing

Set of available Bit-Challenges are chosen orthogonal

Modeling



Key-Challenge is an address-type challenge

Modeling

Helper data stored in NVM or OTP

Replay (helper data manipulation)

5. STEADINESS AND PERFORMANCES

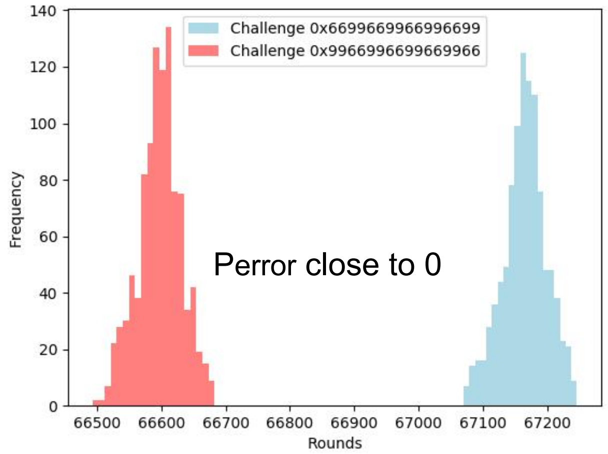
PRINCIPLE OF PUF STEADINESS

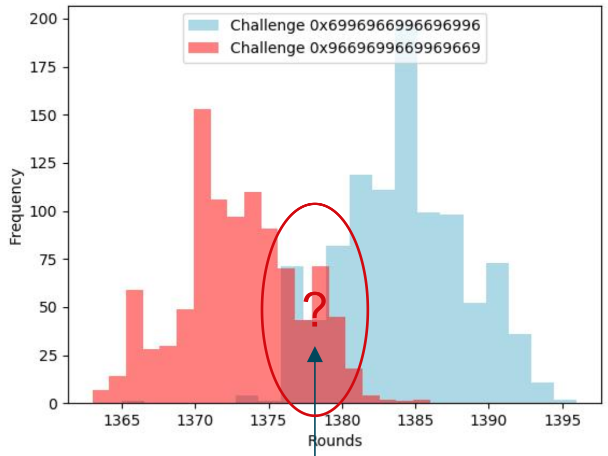
For a given Challenge set c and ¬c, entropy source output must **remain the same bit 0 or 1** whatever the environment conditions:

- Meaning loop number f(c) and f(¬c) must be diffferent enough

Measurement: Frequency distribution of a set of PUF responses (loop number) for 1000 iterations

Error probability is taken as an input of the PUF design process

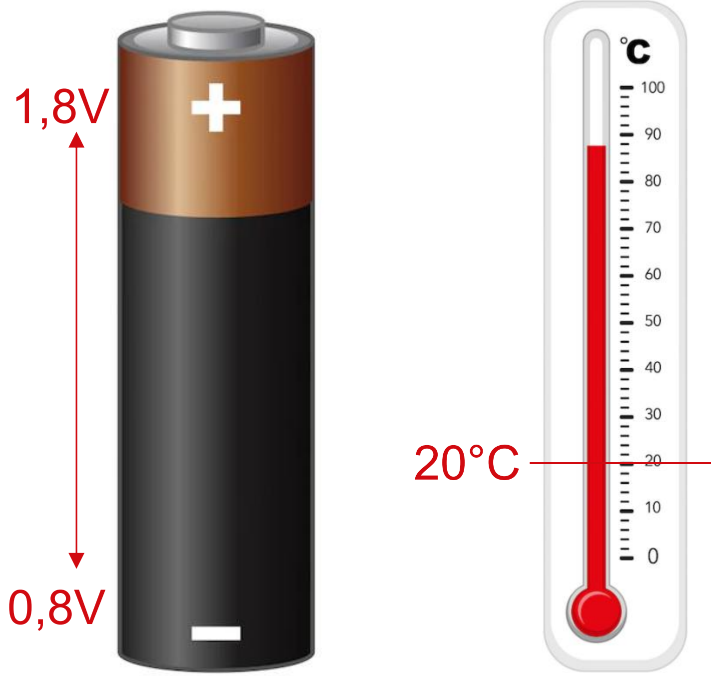


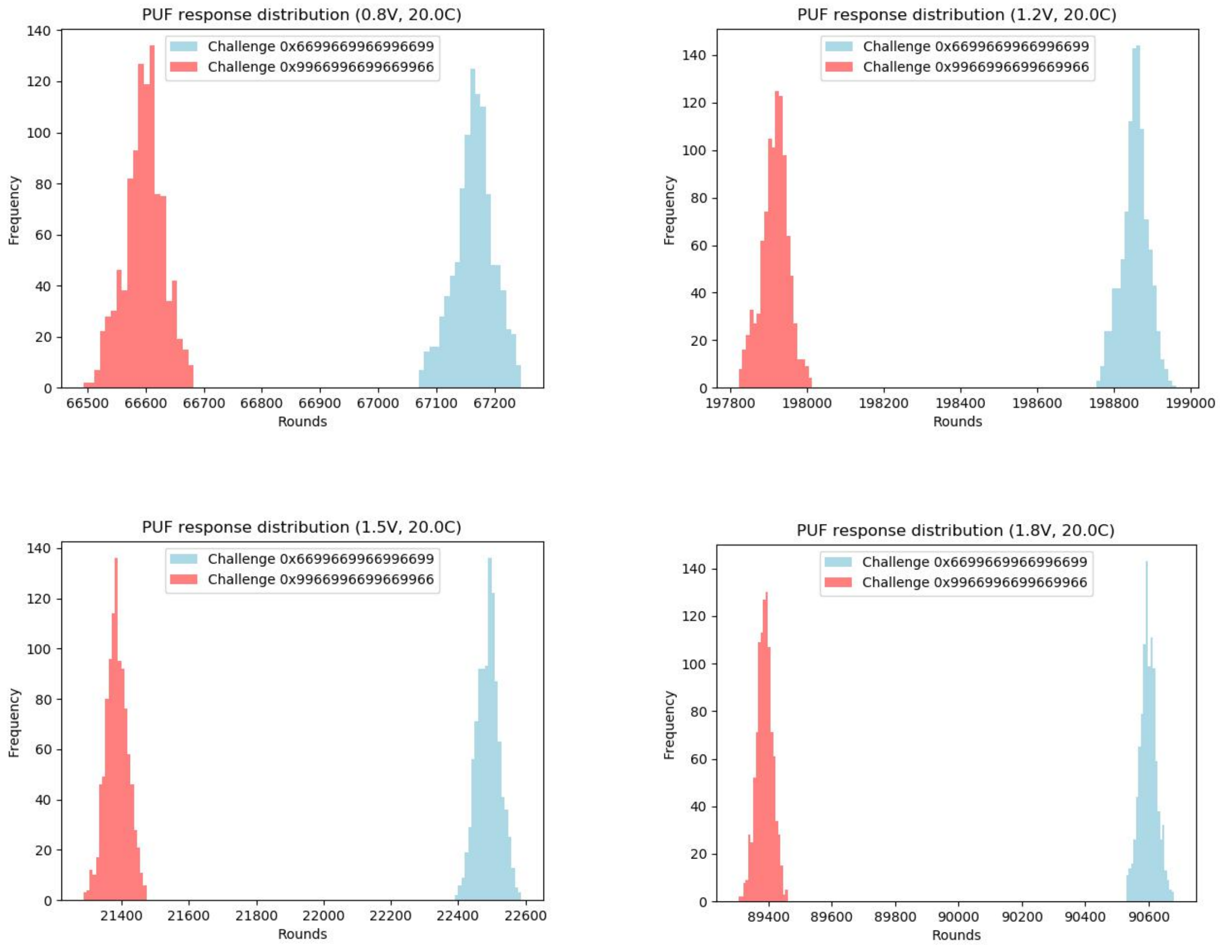


Sometimes $f_c > f_{\bar{c}}$, key bit is 1
Sometimes $f_c < f_{\bar{c}}$, key bit is 0

STEADINESS REGARDING VOLTAGE

Since the PUF unique ID can be used as SoC Master Key, it must output the same steady results whatever the **voltage** variation in the Process Design Kit Range



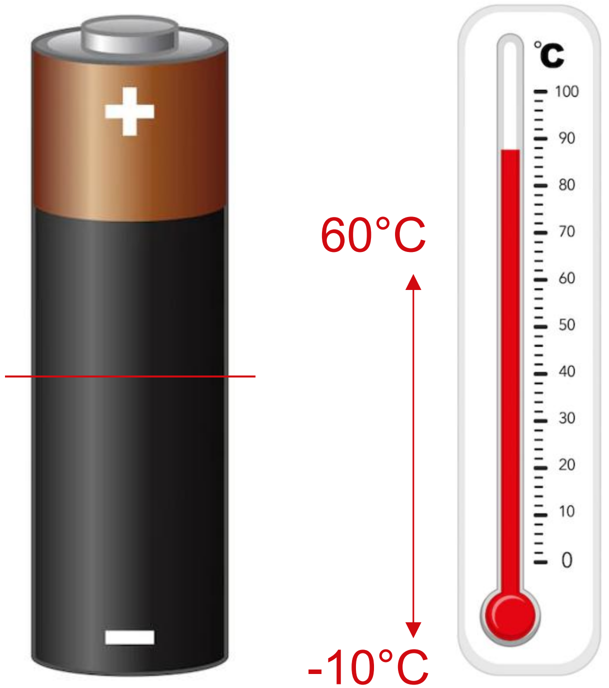


STEADINESS REGARDING TEMPERATURE

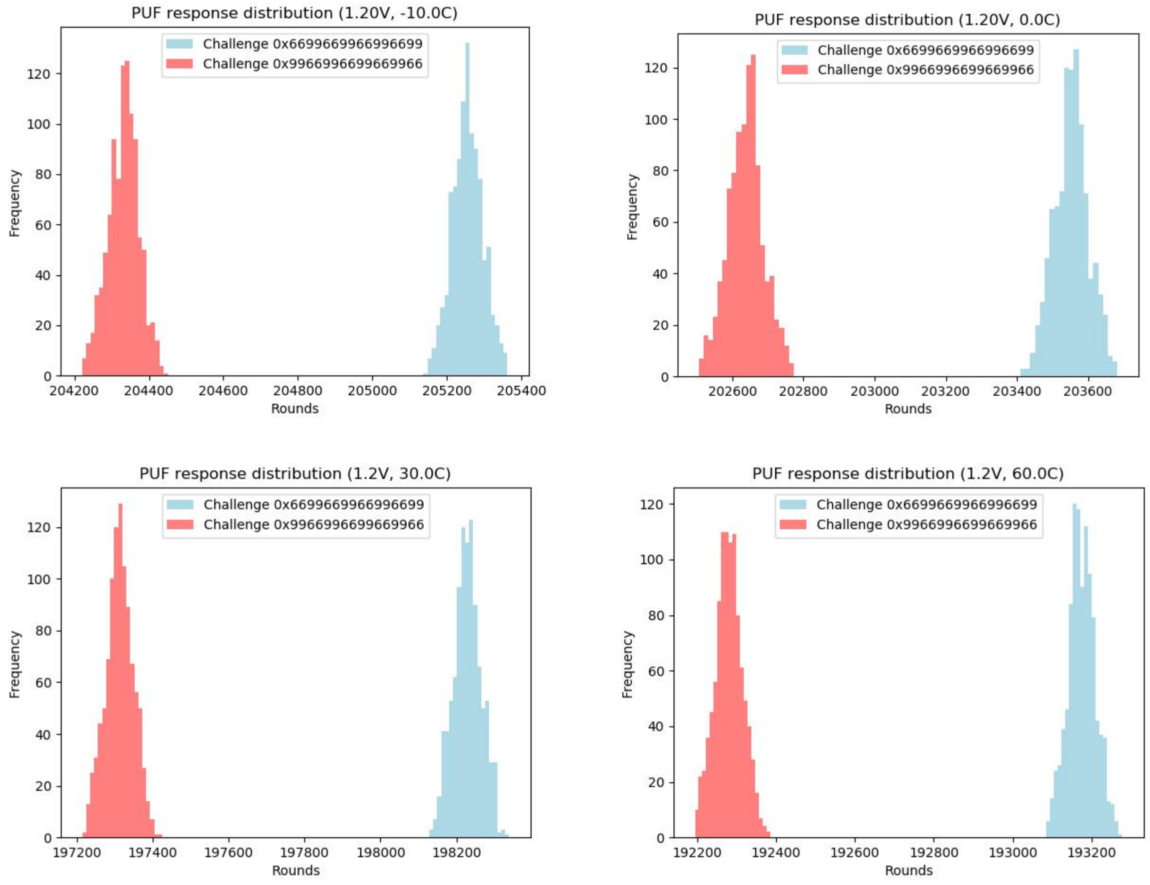
Since the PUF unique ID can be used as SoC Master Key, it must output the same steady results whatever the **temperature** variation in the Process Design Kit Range

1,2V

60°C

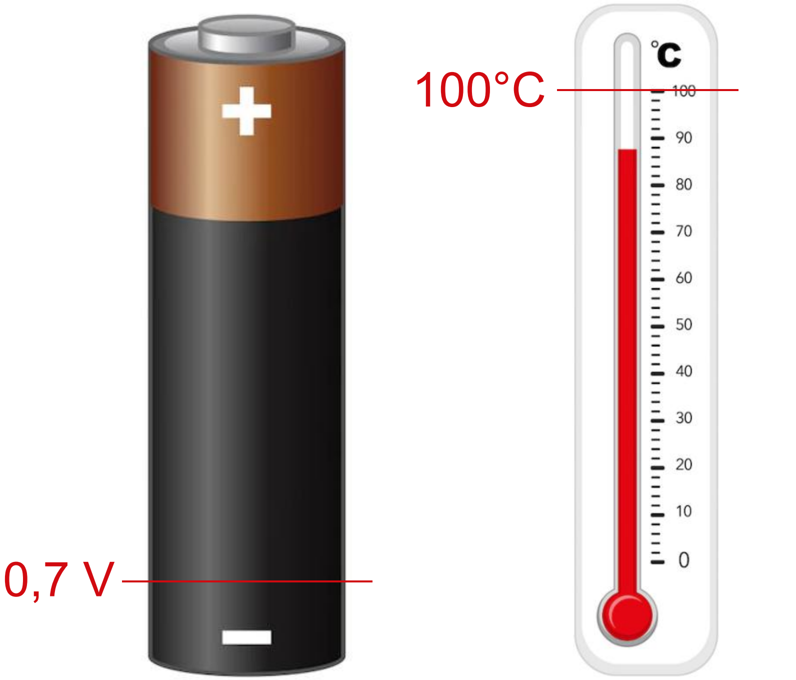


-10°C

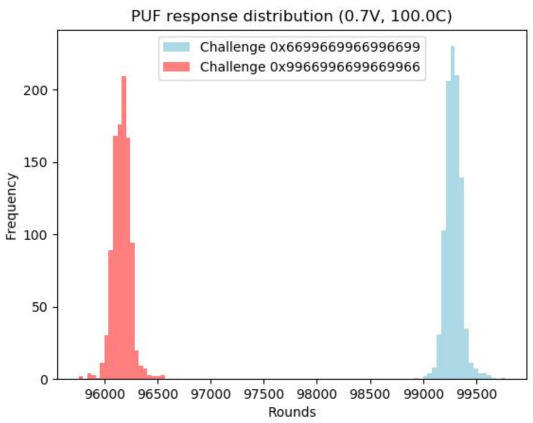


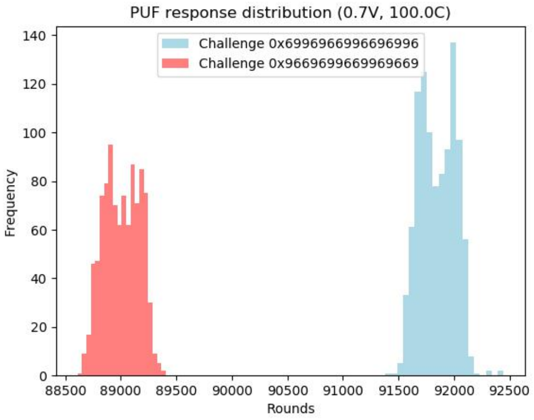
STEADINESS REGARDING AGING

Since the PUF unique ID can be used as SoC Master Key, it must output the same steady results **all along the Life cycle** of the device



Worst Case:
- Low Voltage (0.7V)
- High Temperature (100°C)





Oven accelerated aging*

Today

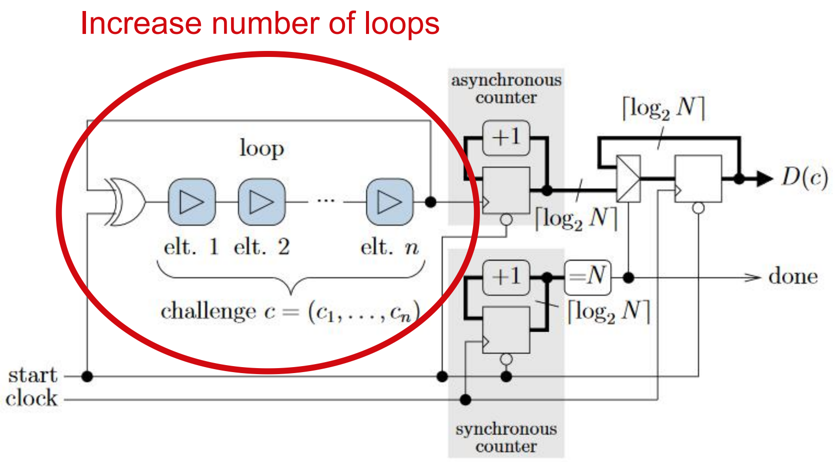
+30 years

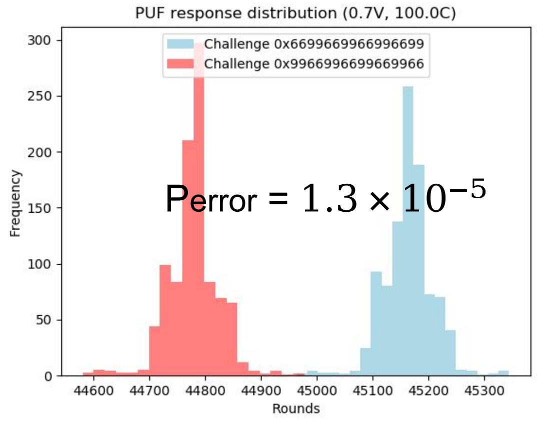
*oven aging allows to accelerate the component aging in order to discover in a short time how it will evolve over a long-time span

ON-FIELD ADJUSTMENTS: TIME FINE-TUNING TO COUNTER AGING

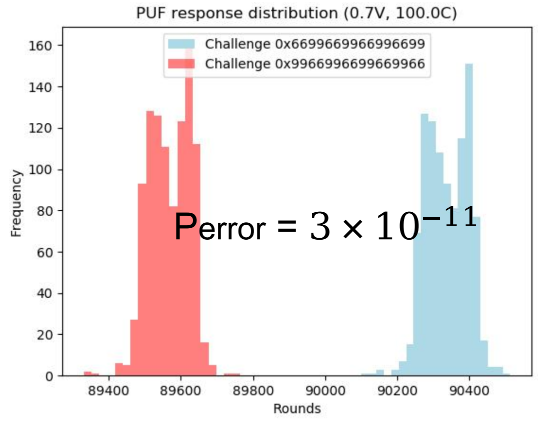
When in-field, the reliability may be adversely affected by aging or environmental conditions…

Usually, no action is required, but if needed, **key-rebuilding time increased by Software** remains an option to take advantage of averaging and regain reliability





Double the timing window



7. INTEGRATION AND POST-SILICON ADAPTATION

- Interaction flow and guidelines
- Adaptive Control
- PUF Lifecycle Details
- Strong PUF with Weak Implementation
- Helper Data – High Temperature and High Voltage

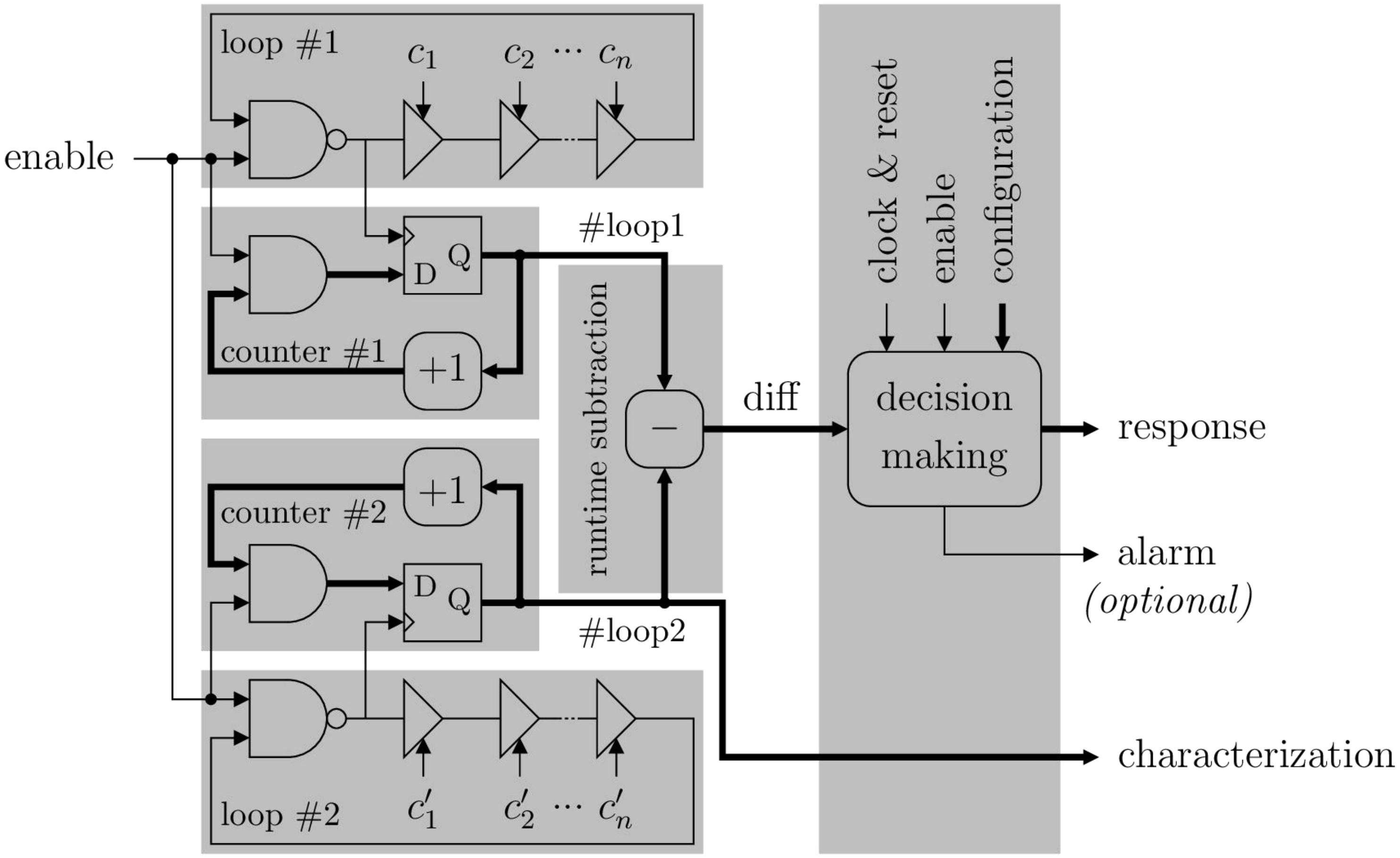
Differential Loop-PUF: specifications

Threats:

- Fault of one loop readout and not the other one: the difference is not consistent
- Leverage global signals to force the PUF values

To protect those against attacks, the loop PUF has been improved

- The two measurements (c and c’) are conducted at the same time
- As a byproduct, the common noise is eliminated

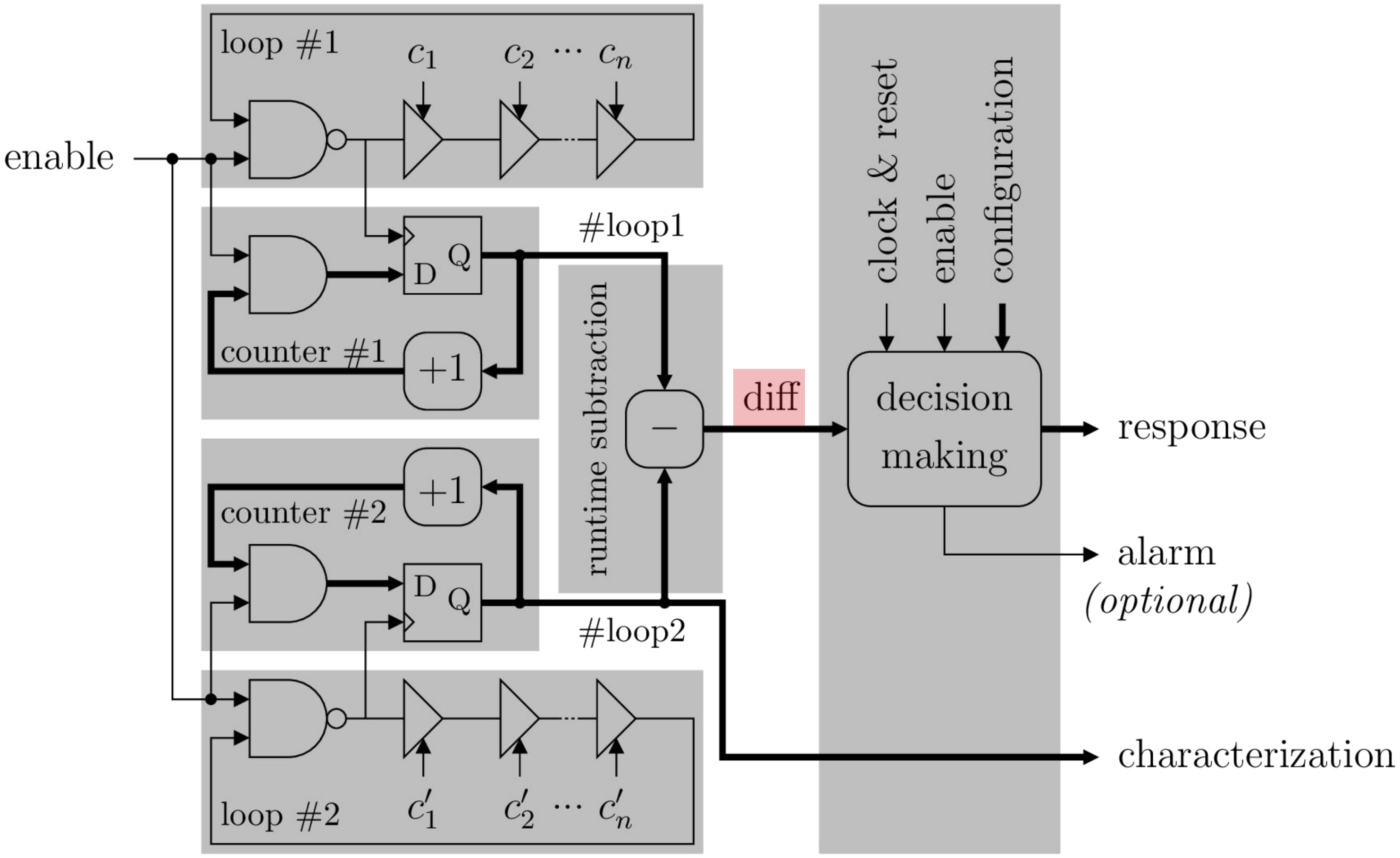


Differential Loop-PUF: differentiating feature

The difference «**diff**» signal:

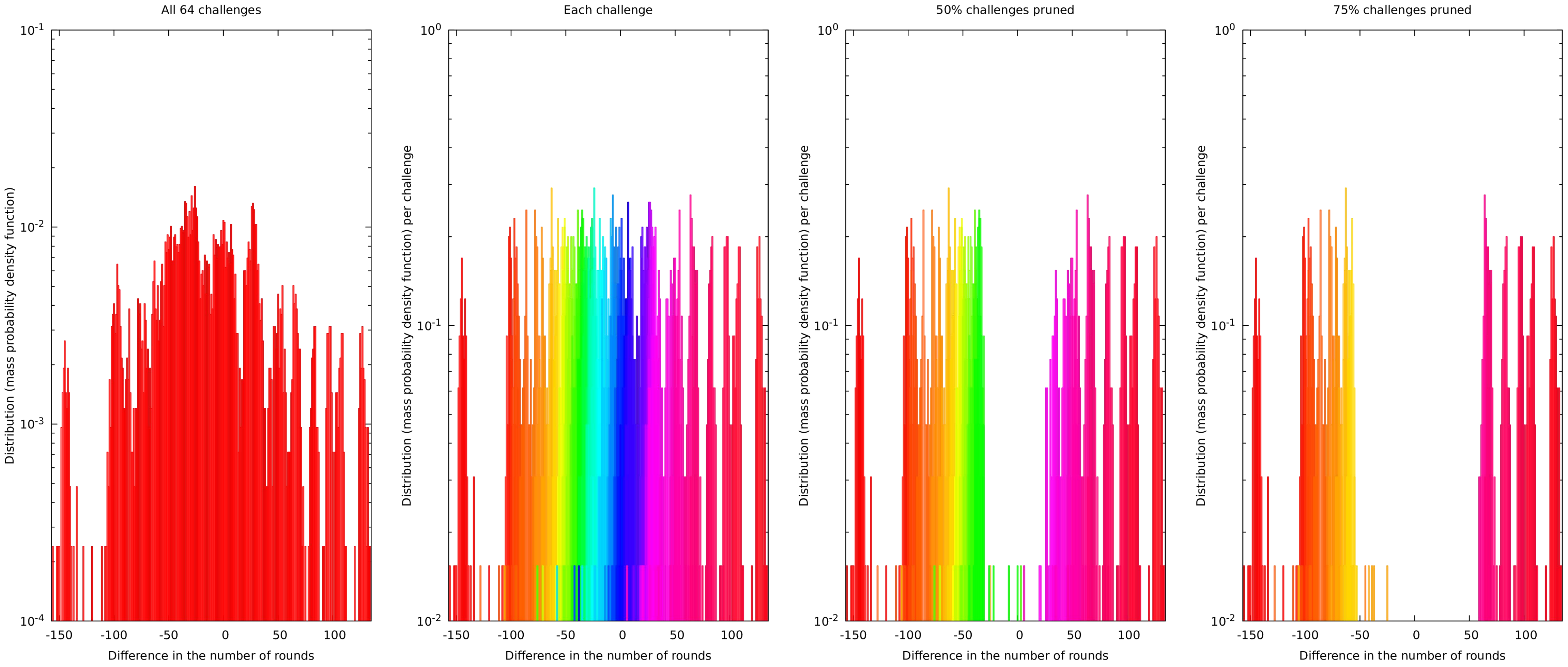
- Allows to monitor in a quantitative manner how the two loops frequency differ
- It becomes possible to use the value of «diff» as a reliability metric
  - for enrollment, and
  - for rebuild

This structure is still as easy to implement in ASIC or in FPGA.



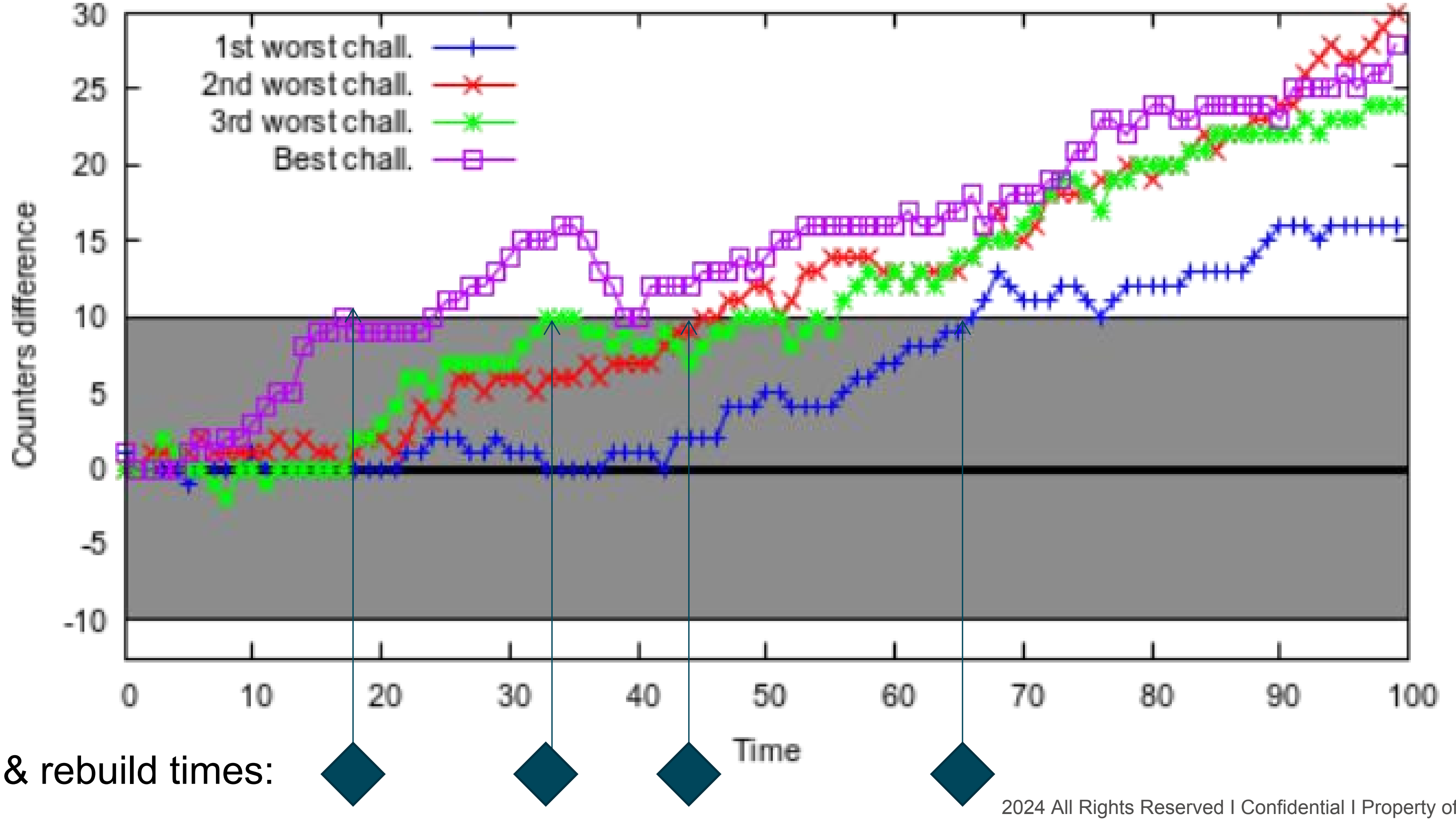
Differential Loop-PUF: measurements

All responses | Response per chall. | Pruning rate r=1/2 | Pruning rate r=1/4



Differential Loop-PUF: Brownian motion

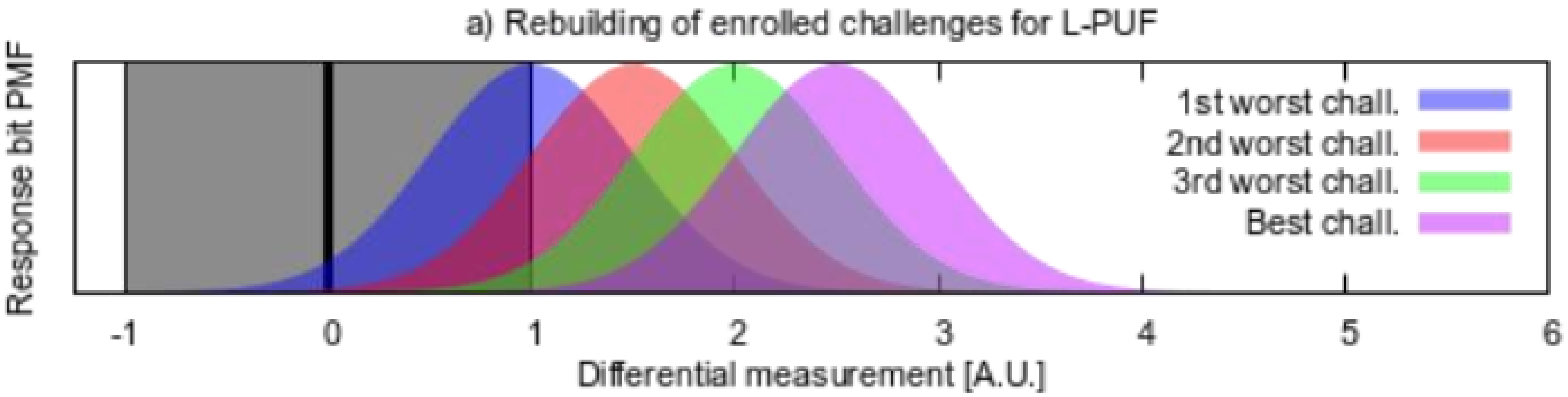
- Convergence speed, for selected (enrolled) challenges
  - Pruned challenges not represented. They would yield way slower responses (>> 65)



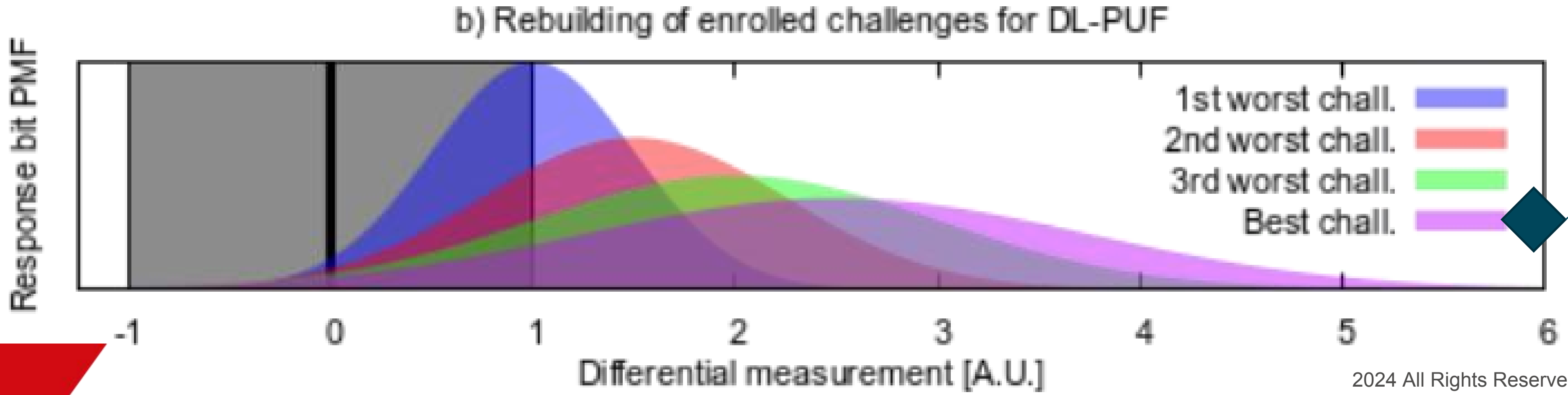
Enrollment & rebuild times:

Differential Loop-PUF: Allowed optimizations

- Optimization:
  - Better challenge can be rebuit faster, if the criteria is the time to get |diff|>threshold



In classical Loop-PUF, all challenges are rebuilt with same time, hence have different reliability



In Differential Loop-PUF, the best challenge can be rebuilt significantly faster if the metric is not the «worst case SNR», but the value of |diff|

Differential Loop-PUF advantages

In Differential Loop-PUF, the criteria selection for the decision that a response is acceptable (both in enrollment and rebuild phases) is not based on time, but on the value of |diff| (i.e., the absolute value of «diff»).

- This reduces both enrollment and rebuild times
- This also allows to get uniform reliability across rebuilt key bits
- The DL-PUF delivers its rebuilt key with the same reliability in all environmental conditions (even adversarial ones)
  - albeit at the expense of rebuild time

This opens unprecedented applications:

- Late enrollment, e.g., in adversarial or in uncontrolled environments (incl. already in field)
- Adaptation to challenging situations, not foreseen up chip specificiation
  - Allow for reaching higher certification levels, as per the CC quotation

7. INTEGRATION AND POST-SILICON ADAPTATION

- Interaction flow and guidelines
- Adaptive Control
- PUF Lifecycle Details
- Strong PUF with Weak Implementation
- Helper Data – High Temperature and High Voltage

LEVERAGING STRONG PUFS AS WEAK PUFS

- Working Principle:
  - Restrict PUF challenges to 64 from 2^64 options.
  - Optimizes entropy and enhances security.
- Reason for Restriction:
  - Maximizes entropy per bit.
  - Maintains high unpredictability.
  - Reduces risk of statistical analysis or reverse engineering.
- Benefits of Restricted Challenges:
- Mitigates ML Attacks:
  - Small dataset limits ML model accuracy.
  - Example: Reduces training data from millions to just 64.
- Prevents "SNAKE" Attack
  - SNAKE attack: A side-channel attack targeting cryptographic systems by analyzing physical properties
    - (e.g., power consumption, electromagnetic emissions) to extract secret information.
    - Vulnerabilities: Exploits hardware implementation weaknesses to reconstruct sensitive data.
  - Limits adaptive challenge techniques.
  - Example: Attackers have only 64 challenges to work with.

- Use Cases for Additional Challenges:
  - Working principle:
    - Its possible to rotate the 64 challenges
  - InField Reenrollment :
    - (Step2 is done once more with rotated challenge, enabling a fresh step 3 to be carried out (slide 8 ref)):
    - Secure updates and reprogramming.
    - Example: Devices can be securely reprogrammed in the field.
  - Service Challenges:
    - Onsite testing of PUF's integrity.
    - Example: Regular integrity checks ensure long-term reliability.

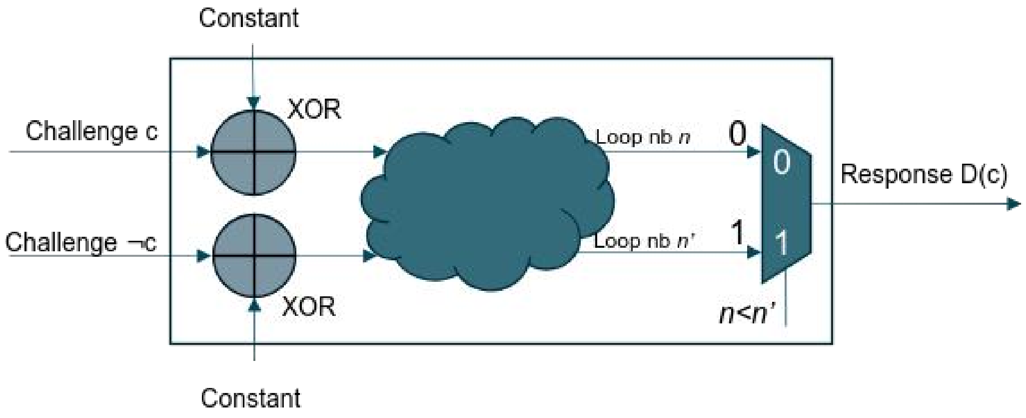


Fig: PUF Challenge Rotation

Attacks on "challenge bits" (helper data) manipulation: Snake I and II: "Attacking PUF-Based Pattern Matching Key Generators via Helper Data Manipulation", Jeroen Delvauxand Ingrid Verbauwhede, CT-RSA 2014: https://eprint.iacr.org/2013/566.pdf

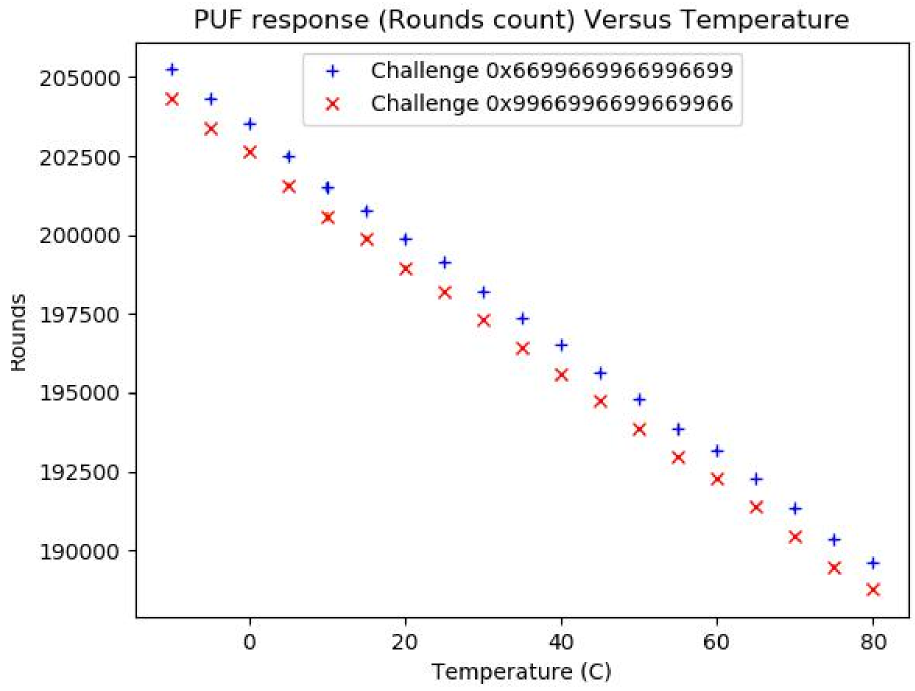
7. INTEGRATION AND POST-SILICON ADAPTATION

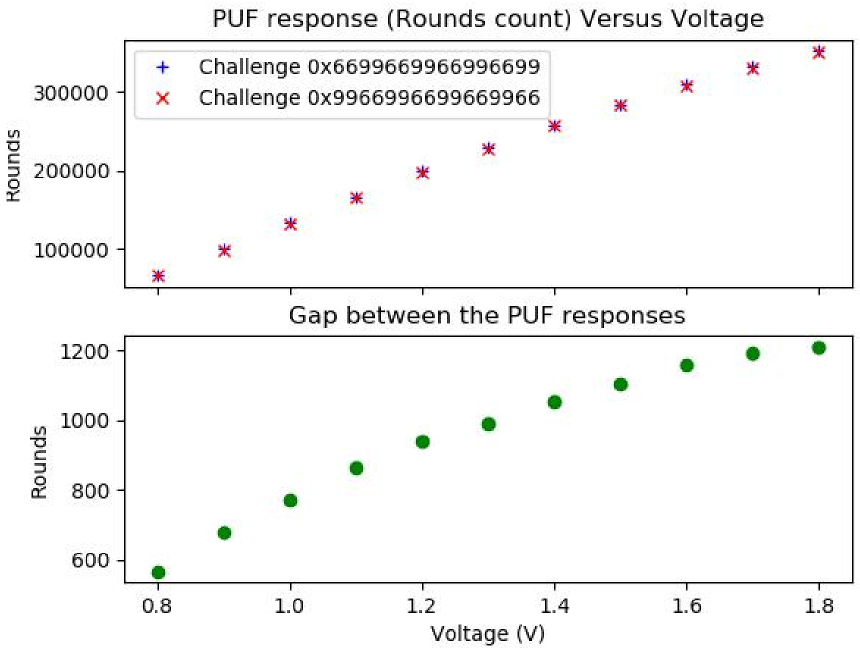
- Interaction flow and guidelines
- Adaptive Control
- PUF Lifecycle Details
- Strong PUF with Weak Implementation
- Helper Data – High Temperature and High Voltage

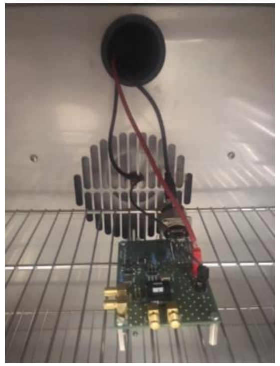
CHALLENGES RELIABILITY UNDER HIGH TEMPERATURE AND VOLTAGE

SECURE-IC
THE SECURITY SCIENCE COMPANY

Harsh conditions and aging tests







Note: The measurements are differential

Steadiness

vs temperature

Steadiness

vs Voltage

Note: During enrollment Challenge Response pairs are pruned to provide reliable helper data

Note: The order relationship #loop(c) ⩽ #loop(c') is also across enrollment & rebuild steps.

LATE ENROLLMENT POSSIBILITY

Thanks to the reliability of Challenges in any conditions:

§ Enrollment can be done in any PVT condition as the entropy source is differential. Enrollment is a process to optimize the challenges, but reliability is a feature of adaptive rebuilding. No key bit is deemed rebuilt until a sufficient distance between the two responses (from challenge & inversed challenge) is larger than the prescribed threshold)

§ Enrollment can be done by software (no need a "tester" to power on/off the chip)

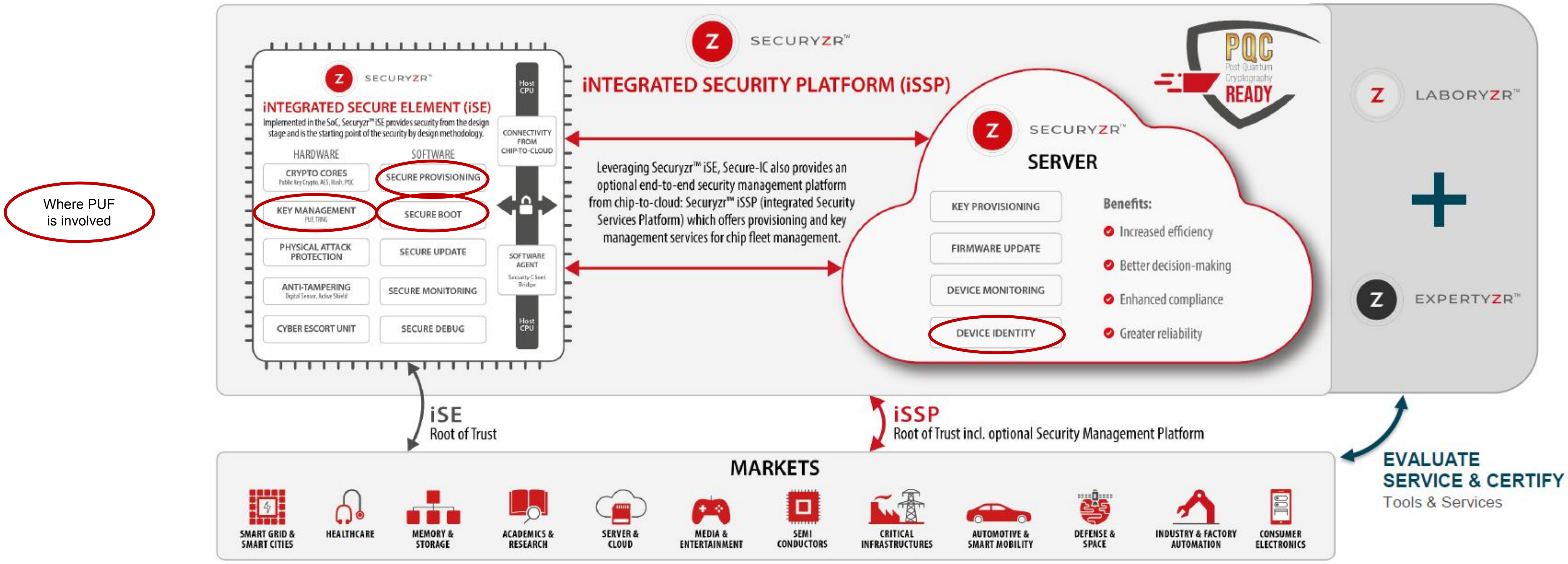
Possibility to enroll late

- after wafer testing
- even when the product is deployed already
- re-enroll capabilities (e.g., refurbishing, or mission retargeting, or for reliability improvement)
- revoke and re-enroll afresh with new challenges (leveraging our post-silicon challenge rotation feature)

9. KEY DIFFERENTIATORS

Secure-IC PUF – integration with other Secure-IC products

- Possibility to deliver the PUF integrated in Secure-IC's Root of Trust: Securyzr™ iSE series, for Master key generation
- Option to leverage the PUF from the Securyzr™ iSSP cloud platform to manage further security lifecycle services, such as Device Identity with ID extracted from the PUF



MAINTAIN TRUST THROUGHOUT THE WHOLE PRODUCT LIFE CYCLE

SECURE-IC
THE SECURITY SCIENCE COMPANY

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