Institut
Mines-Télécom

Some results about the Aging Impact on Delay PUFs

SPACE

Hyderabad, december 2016

Florent Lozac'h[2], Jean-Luc Danger[1,2], Naghmeh Karimi[3], Sylvain Guilley[1,2]

[1]Télécom ParisTech
[2]Secure-IC
[3]Rutgers University

Agenda

- Aging and delay PUFs
- Aging simulation
- Aging acceleration on real silicon
- Conclusions

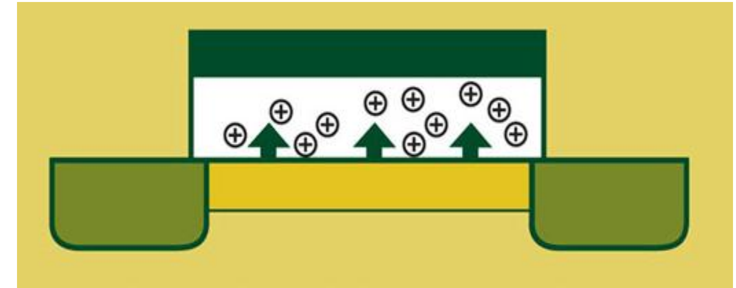
Agenda

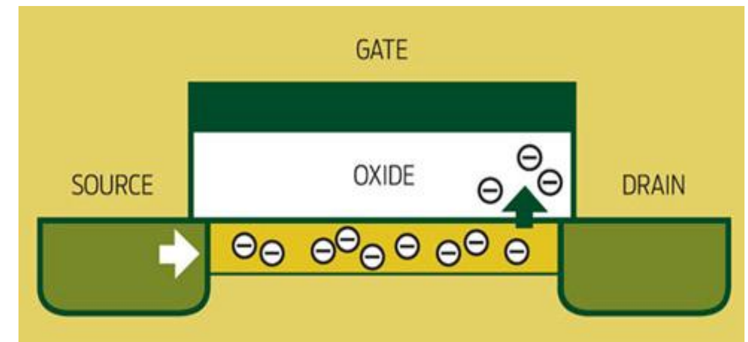
- **Aging and delay PUFs**
- Aging simulation
- Aging acceleration on real silicon
- Conclusions

TELECOM ParisTech

Aging in CMOS technology 1/2

- **Gate Oxide Wearout**
  - Negative Bias Temperature Instability (**NBTI**)
    - Cause: With gate voltage, Holes creating traps between Si-SiO2
    - Impact: Vth increase, especially for PMOS transistors
    - Acceleration: High temperature and high Vdd
  - Hot Carrier Injection (**HCI**)
    - Cause: Electrons colliding with the gate oxide (rather than going only to the condution channel between source and drain)
    - Impact: Vth increase
    - Acceleration: with high switching rate and high Vdd

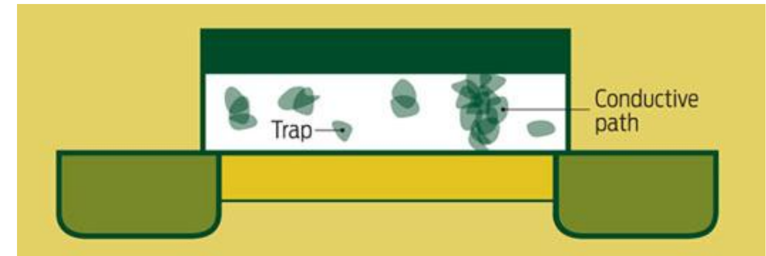




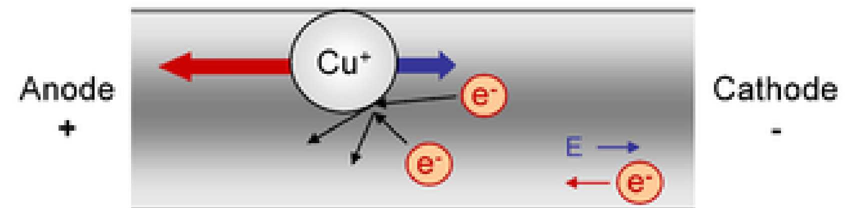
TELECOM ParisTech

Aging in CMOS technology 2/2

- **Gate Oxide Wearout (continue)**
  - Time dependent dielectric Breakdown (**TDDB**)
    - Cause: Conductive path creation in the gate oxide
    - Impact: Gate breakdown
    - Acceleration: with high switching rate and high Vdd



- **Interconnect**
  - Electromigration (EM)
    - Cause: High density current remove conductor atoms
    - Impact: short circuit, net breakdown



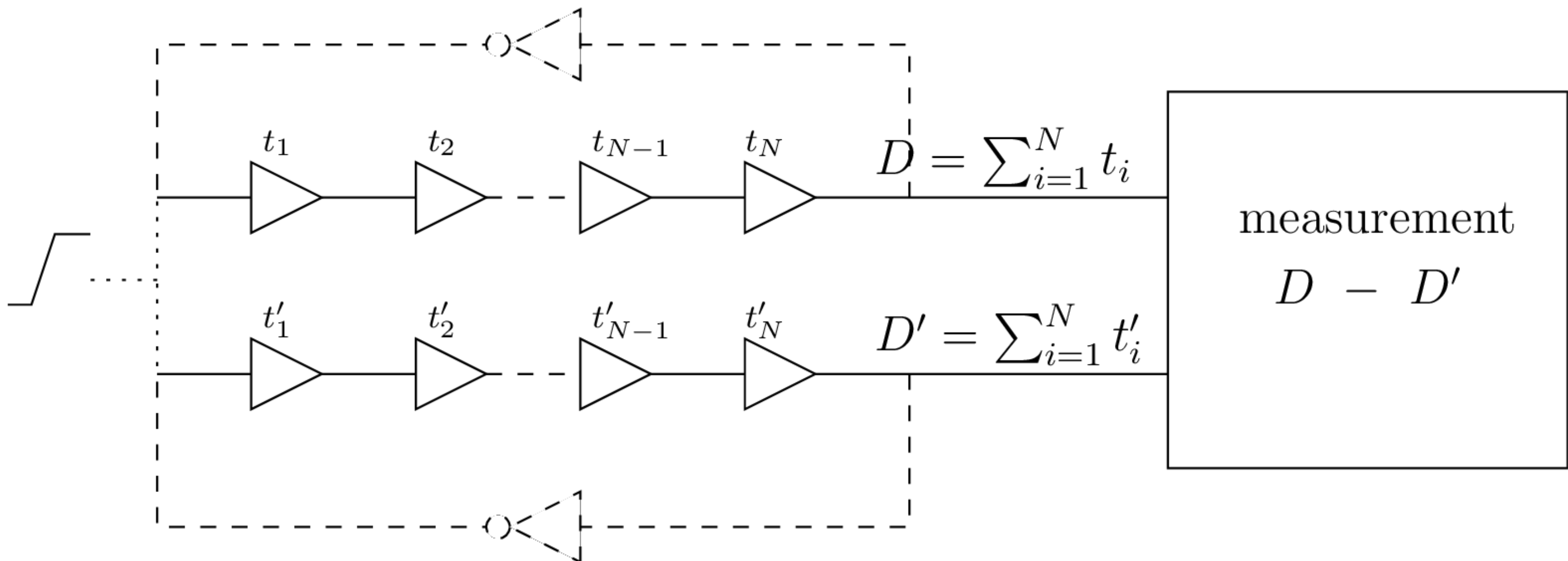
What is a PUF ?

- **Function returning an Identifier of the device**
  - **Physical** function,
  - which exploits **material** randomness,
  - and is unclonable: **same structure** for each device
- **The Identifier can be:**
  - A **unique** number
  - A list of **responses** for a given set of **challenges**
- **Pros**
  - No programmation (no human intervention)
  - Not clonable (no Reverse Engineering) as the structure is the same
  - Can be build in standard CMOS process (silicon PUF)

TELECOM ParisTech

Silicon PUF

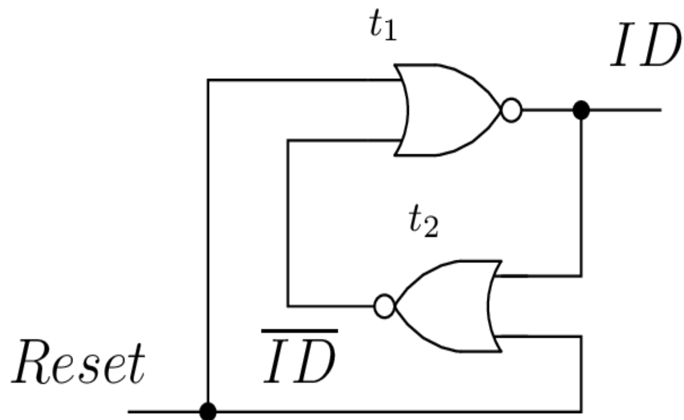
- **Delay PUF**
  - Based on differential measurement of time



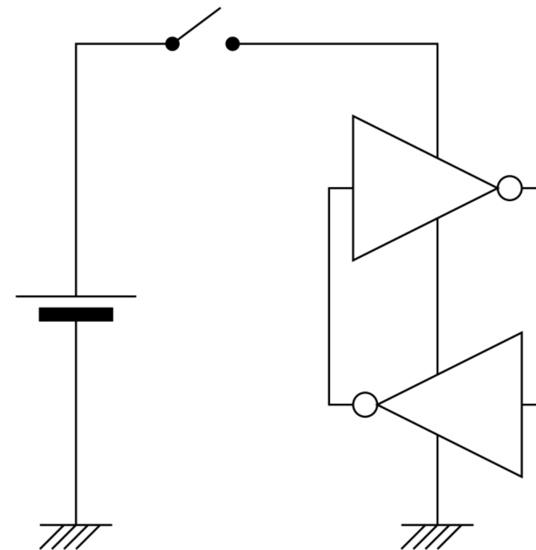
TELECOM ParisTech

Silicon PUF

- **Memory PUF**
  - Based on differential strength between two elements of a memory point



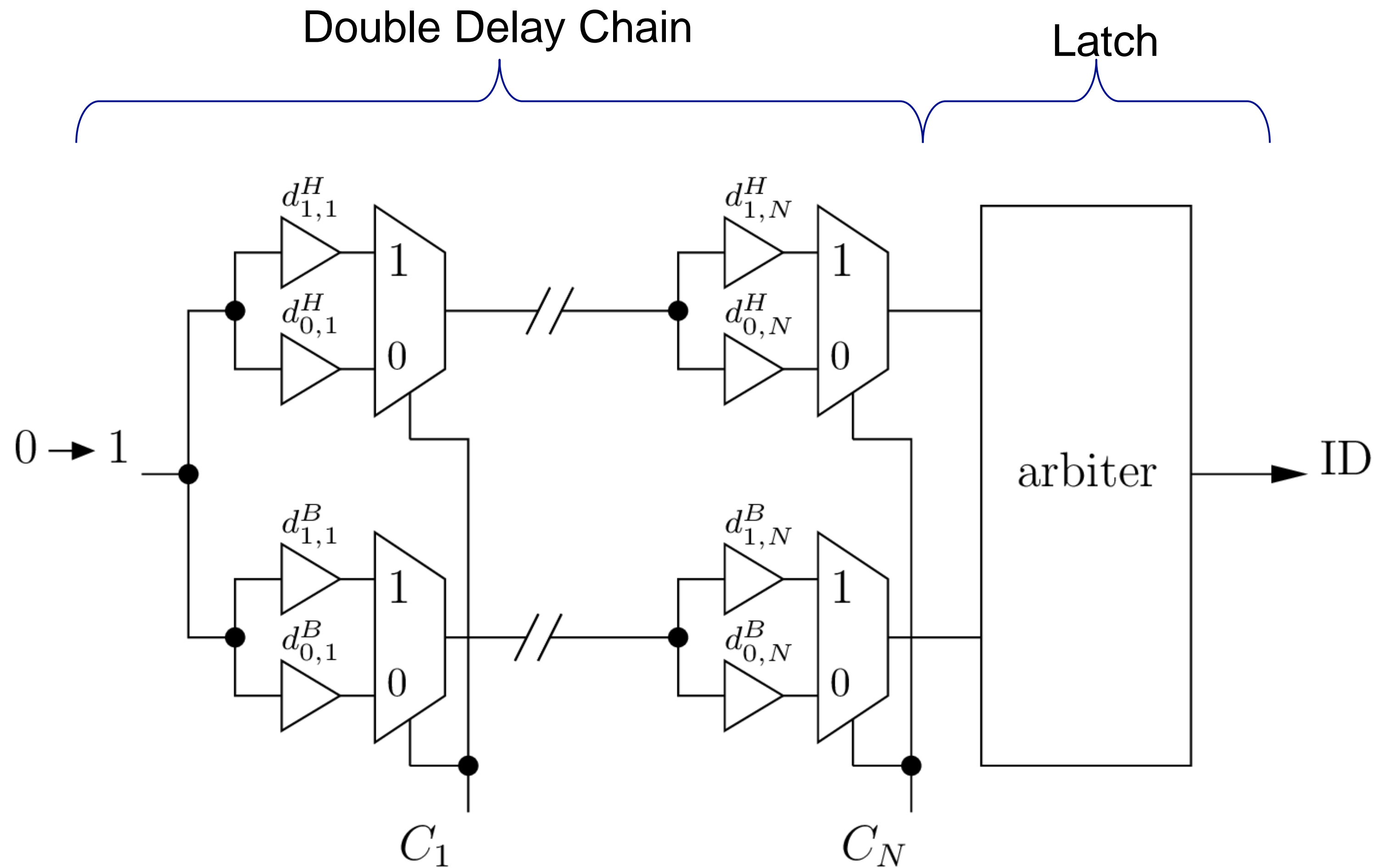
Stable state of a RS latch after Reset



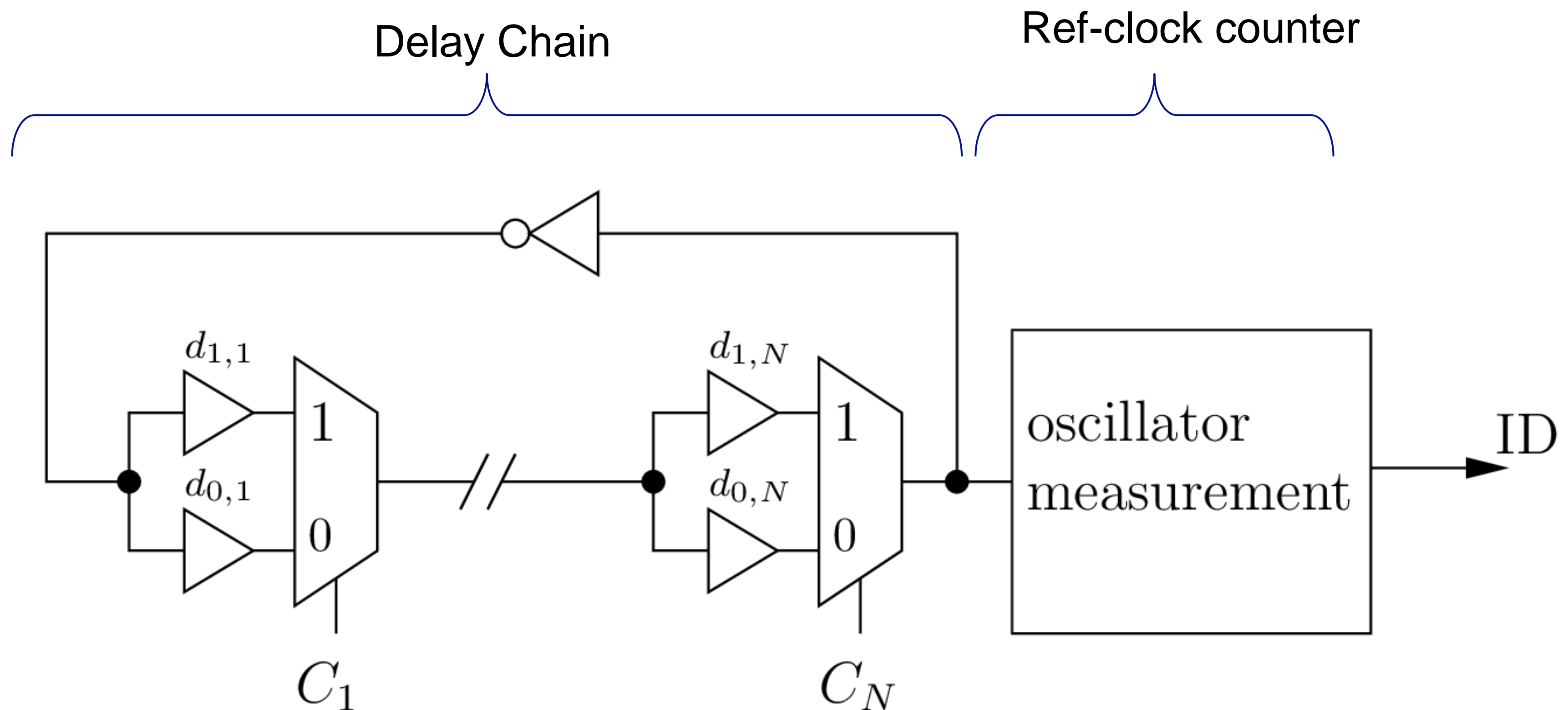
Stable state of a SRAM point at start-up

TELECOM ParisTech

Delay PUF: Arbiter PUF



Delay PUF: Loop PUF



Specific protocol: time measurement with challenge C then with challenge $\overline{C}$

APUF identifier extraction

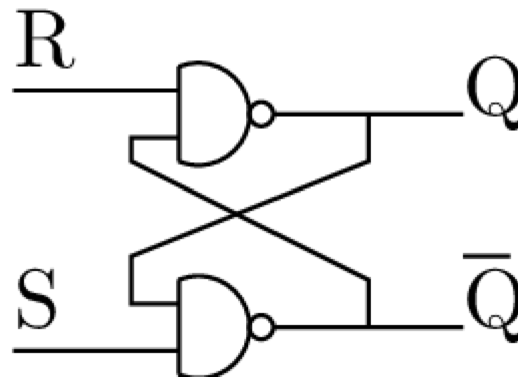
n delay elements

$$\text{APUF}: \quad \phi_a\left(\sum_{i=1}^{n} d(c_i), \sum_{i=1}^{n} d(-c_i)\right)$$

Delay line 1

Delay line 2

Arbiter based on balanced RS latch



TELECOM ParisTech

LPUF identifier extraction

n delay elements

$$\text{LPUF}: \quad \text{sign}(\lfloor N\sum_{i=1}^{n} d(c_i)\rfloor - \lfloor N\sum_{i=1}^{n} d(-c_i)\rfloor)$$

Subtractor

N loops

Delay line
with challenge C

Delay line
with challenge –C

Allows to know the accurately the delay difference

Soustractor, no latch

TELECOM ParisTech

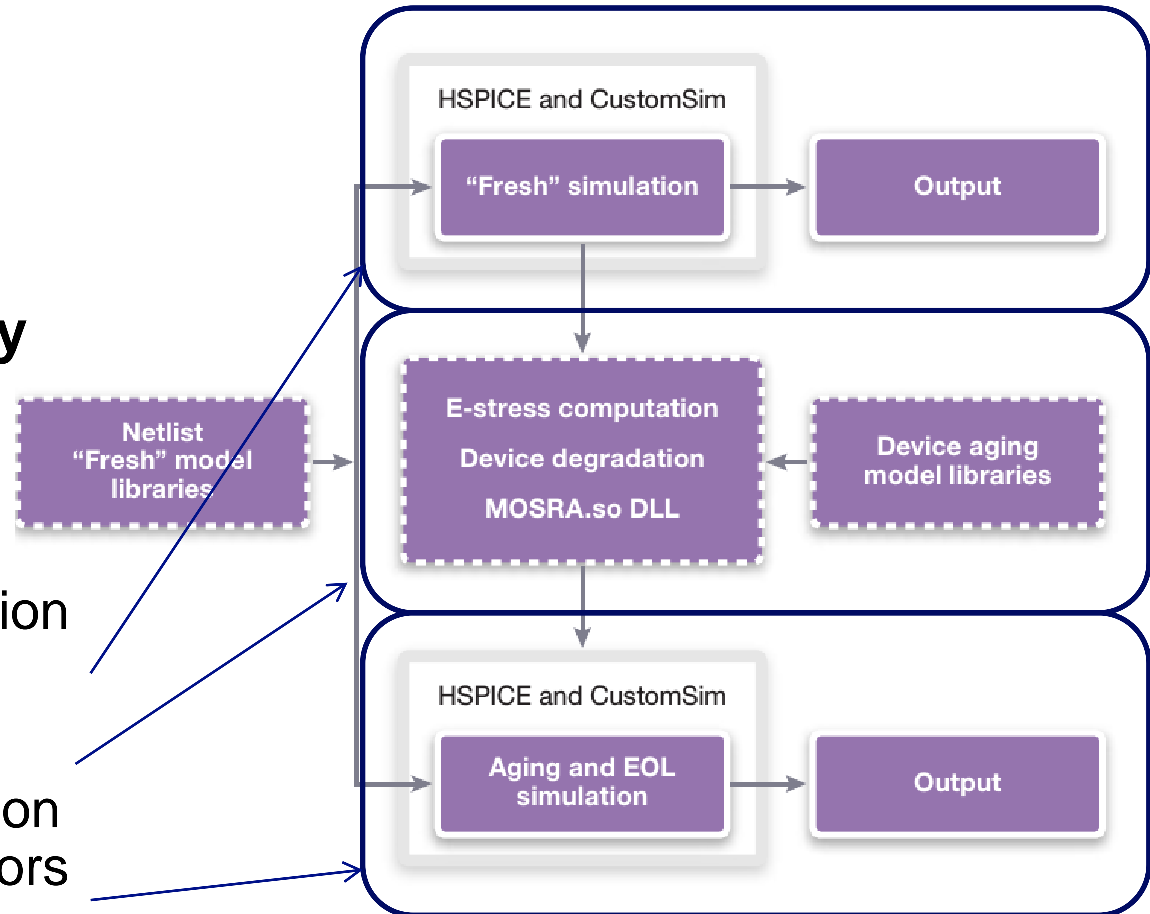
Agenda

- Aging and delay PUFs
- **Aging simulation**
- Aging acceleration on real silicon
- Conclusions

TELECOM ParisTech

Aging simulation

- **MOSRA from Sysnopsys**
  - NBTI and HCI models
- **NANGATE library**
  - 45nm open source library
- **3 steps**
  - Normal simulation
  - Stress factors extraction
  - Re-run simulation with stress factors



TELECOM ParisTech

Aging simulation of delay-chain PUF

Number of elements — Challenge bit — Complementary Challenge bit

Measurement of Delta = $$\left(\sum_{i=1}^{n} d(c_i) - \sum_{i=1}^{n} d(-c_i)\right)$$

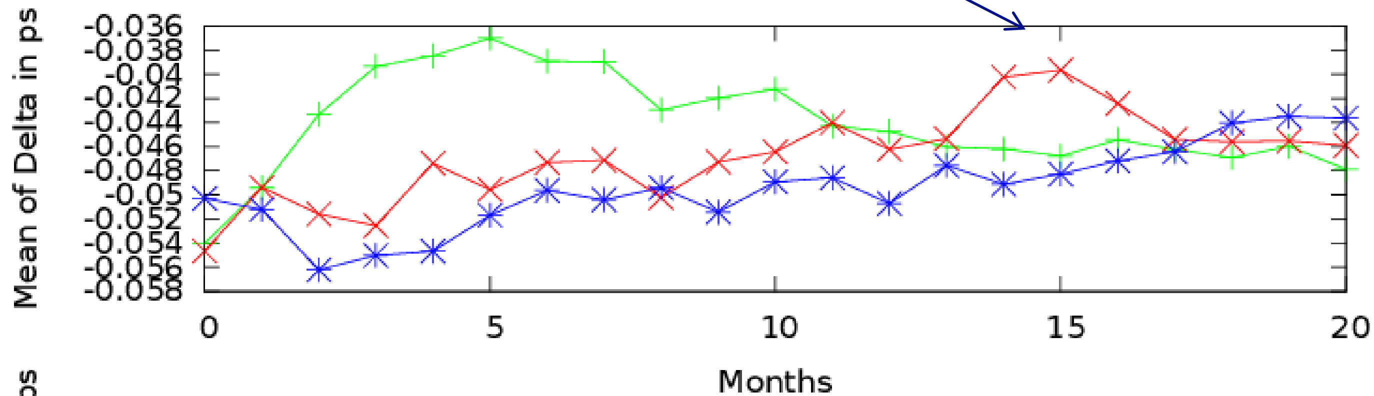
Aging simulation parameters:

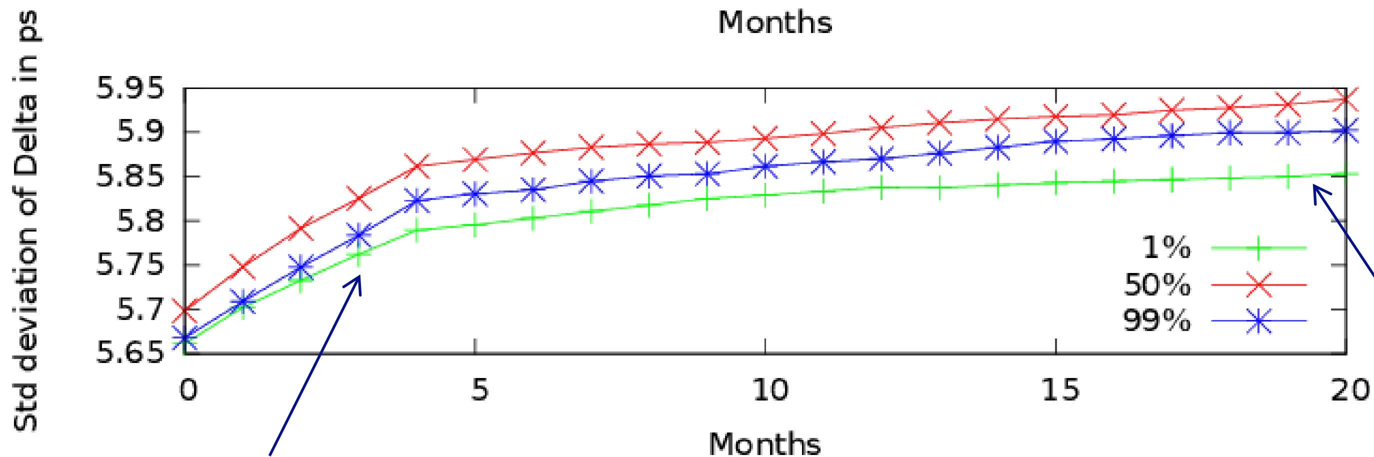
- 20 months of aging
- 8192 LPUF with n=1 element
- or 512 LPUF with n=16 elements
- 3 "duty cycle" of the signal, to check the NBTI impact
  - 1%, 50% and 99%
  - X% means that during X% of time the PMOS transistors are "off " (less NBTI aging)

TELECOM ParisTech

Aging simulation of Loop PUF of 16 elements challenge = 0x00FF

The aging has no monotonic impact on the mean: quantization error as the increase is too low





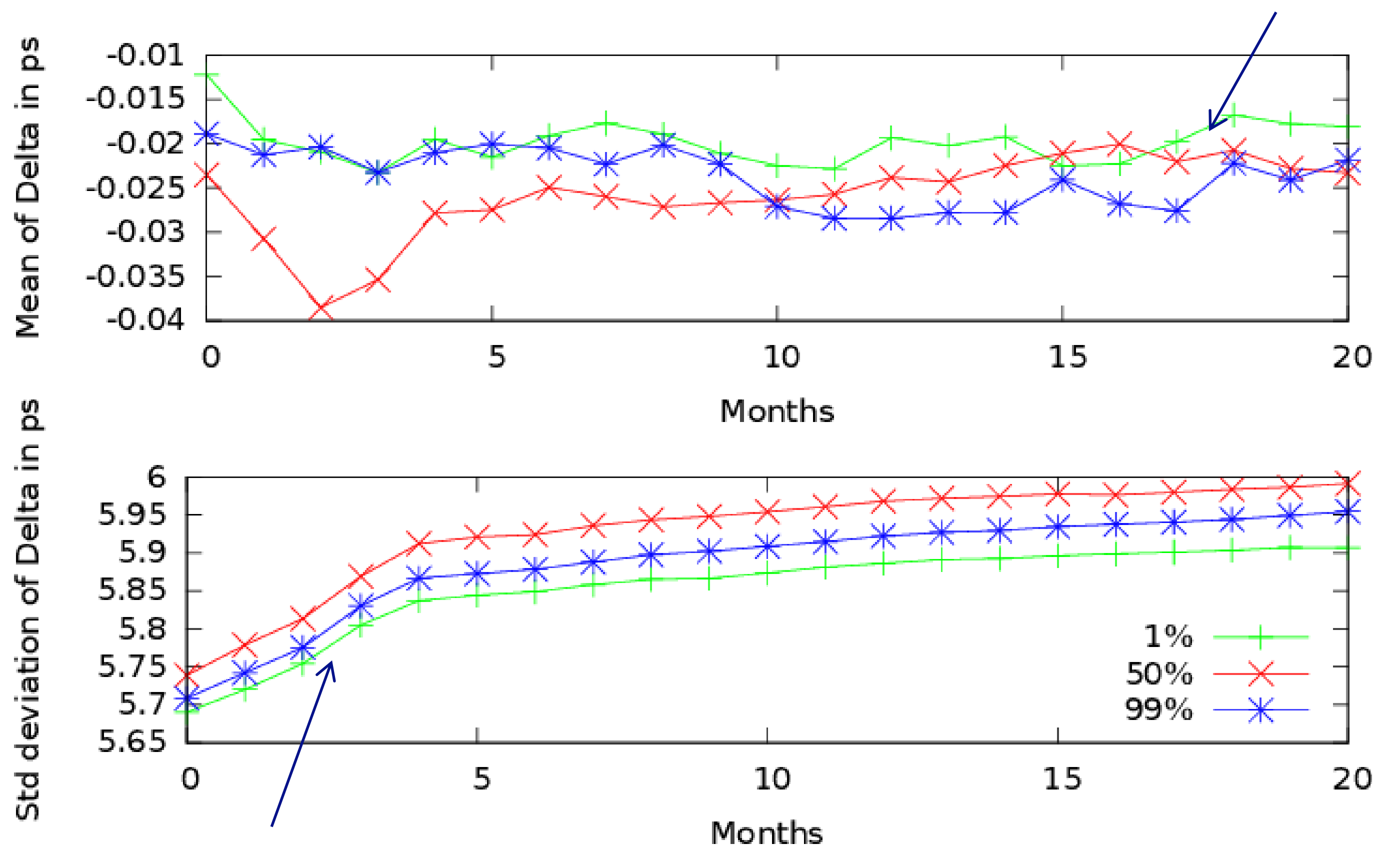
The std deviation always increases
Greater increase the first months

The slope with 1% duty cycle is slightly smaller

TELECOM ParisTech

Aging simulation of Loop PUF of 16 elements challenge = 0x5A5A

The aging has no monotonic impact on the mean: quantization error as the increase is too low



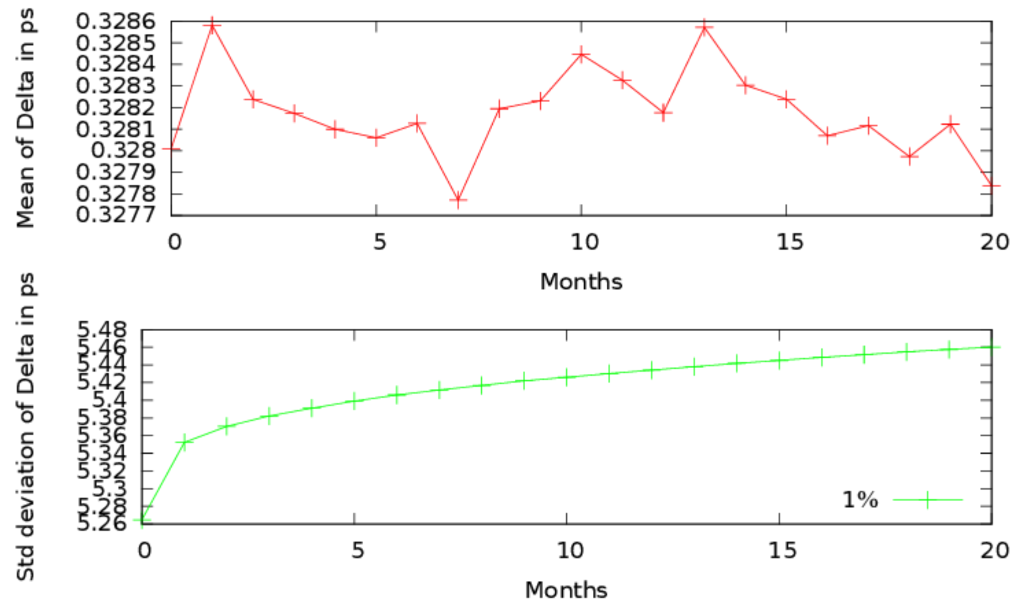
The std deviation always increases
Greater increase the first months

TELECOM ParisTech

Aging simulation of arbiter PUF

2 parts:

- **1. Delay chain**
  - Very similar to the Loop PUF



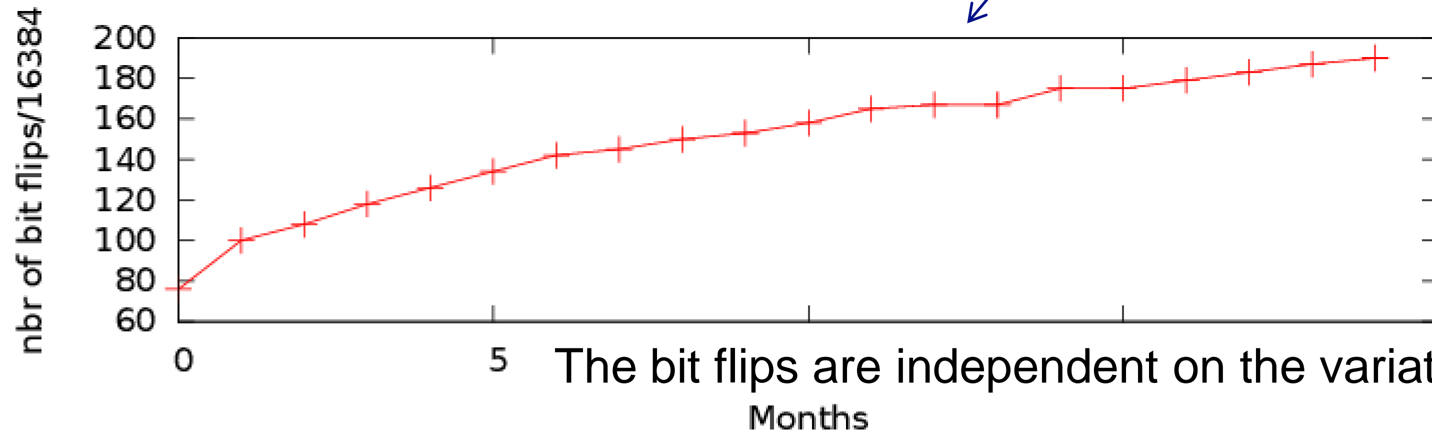
- **2. Arbiter**
  - Result =number of bit flips among 16384 arbiter latches

TELECOM ParisTech

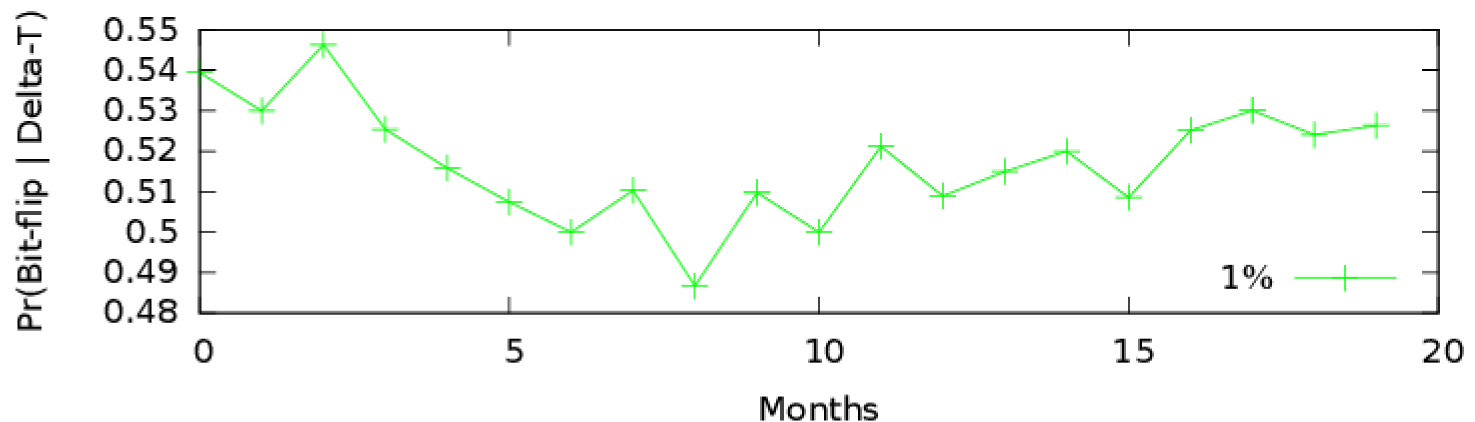
Aging simulation of the arbiter only

number of bit flips among 16384 arbiter latches

More than 1% of bit flips after 1 year



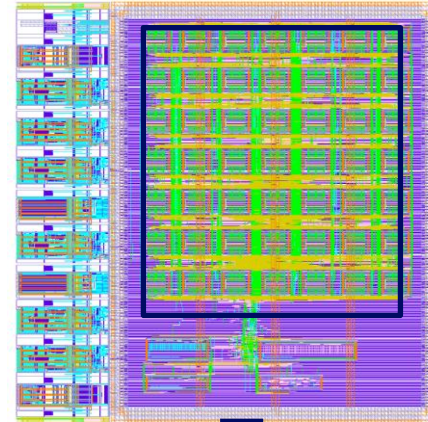
The bit flips are independent on the variation of delta



Agenda

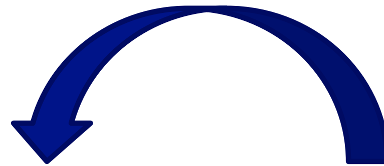
- Aging and delay PUFs
- Aging simulation
- **Aging acceleration on real silicon**
- Conclusions

Aging acceleration

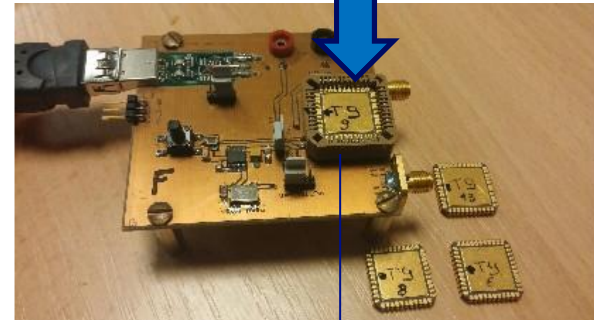


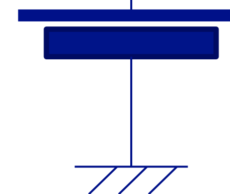
49 LPUFs

CMOS 65nm



85°C





2 V
Instead of 1.2 V

Aging acceleration of Loop PUF

Number of elements
Challenge bit
Complementary Challenge bit
N Loops

Measurement of Delta = $\lfloor N \sum_{i=1}^{n} d(c_i) \rfloor - \lfloor N \sum_{i=1}^{n} d(-c_i) \rfloor)$

Aging acceleration parameters:
- 100 days of acceleration
- 49 PUFs of 64 delay elements

TELECOM ParisTech

Aging acceleration procedure

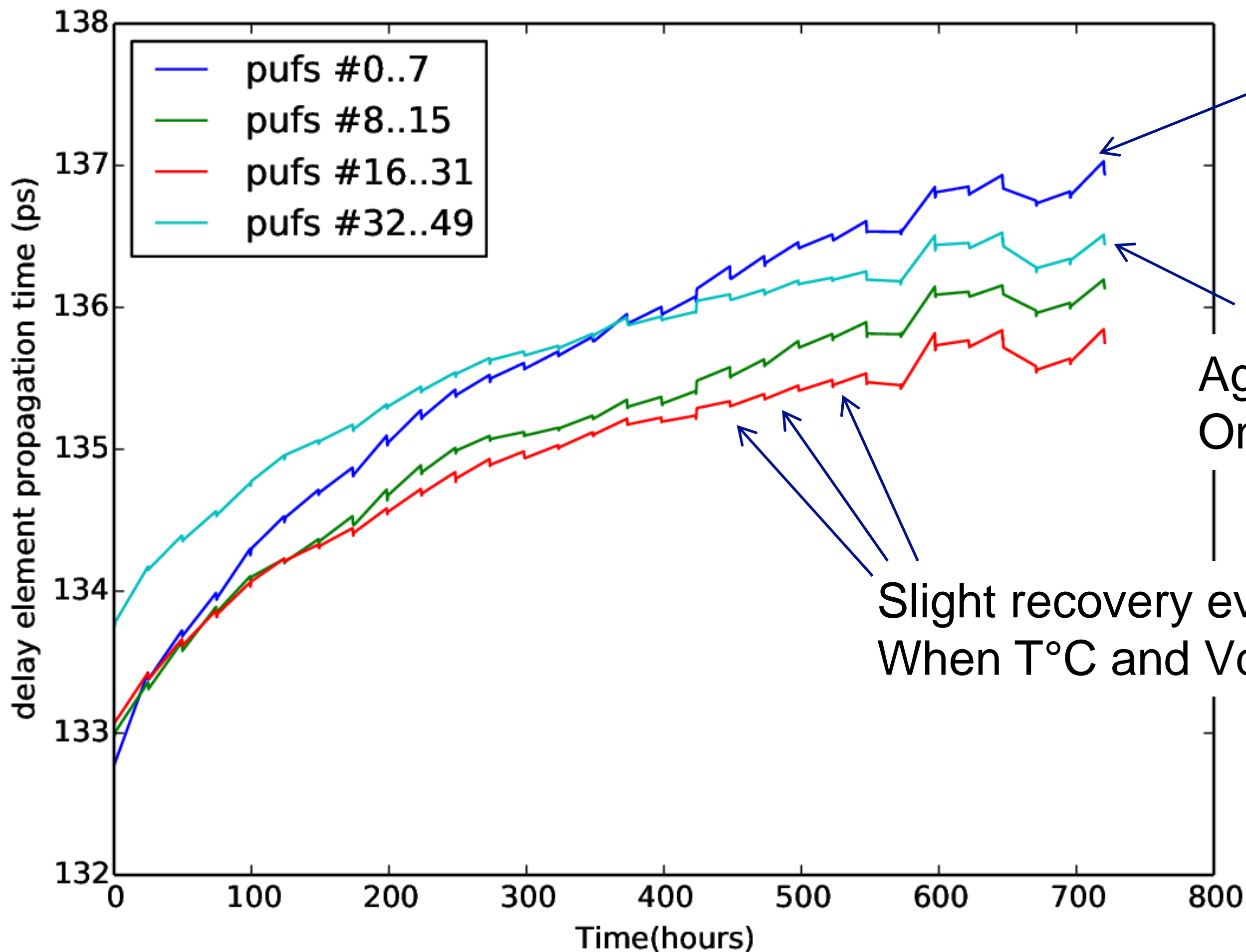
- **Step 1: STRESS phase, duration 23 hours**
  1. Power voltage is set at 2 V, Temperature is set at 85°C
  2. The challenge is set at 0x00000000ffffffff
  3. The PUFS are stressed in the following order:
     - pufs(1-8) always measured,
     - pufs(9-15) 1/8 time,
     - pufs(16- 31) 1 /64 time,
     - pufs(32-49) never measured

     Allows to test the impact of the switching activity
  4. Idem steps 2-3 with the challenge set to 0xffffffff00000000

- **Step 2: MEASUREMENT phase, duration 1 hour**
  - The chip is back at normal conditions (1.2V, 20°C) , and PUF measurements are taken periodically.
- **GOTO Step 1**

TELECOM ParisTech

Aging impact on the absolute value $\sum_{i=1}^{n} d(c_i)$



The first 8 PUFs are more sensitive to HCI (more switching)

Aging even if no activity On PUFs 32-49

Slight recovery every 24 hours When T°C and Vdd decrease

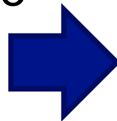
TELECOM ParisTech

Aging impact on the mean of the differential value

$$\lfloor N \sum_{i=1}^{n} d(c_i) \rfloor - \lfloor N \sum_{i=1}^{n} d(-c_i) \rfloor)$$

Mean on 49 PUFs
Challenge = 0x00000000FFFFFFFF

Mean of the delay for one element



Non monotonic, Close to noise !

delay element propagation time (ps)

Time(hours)

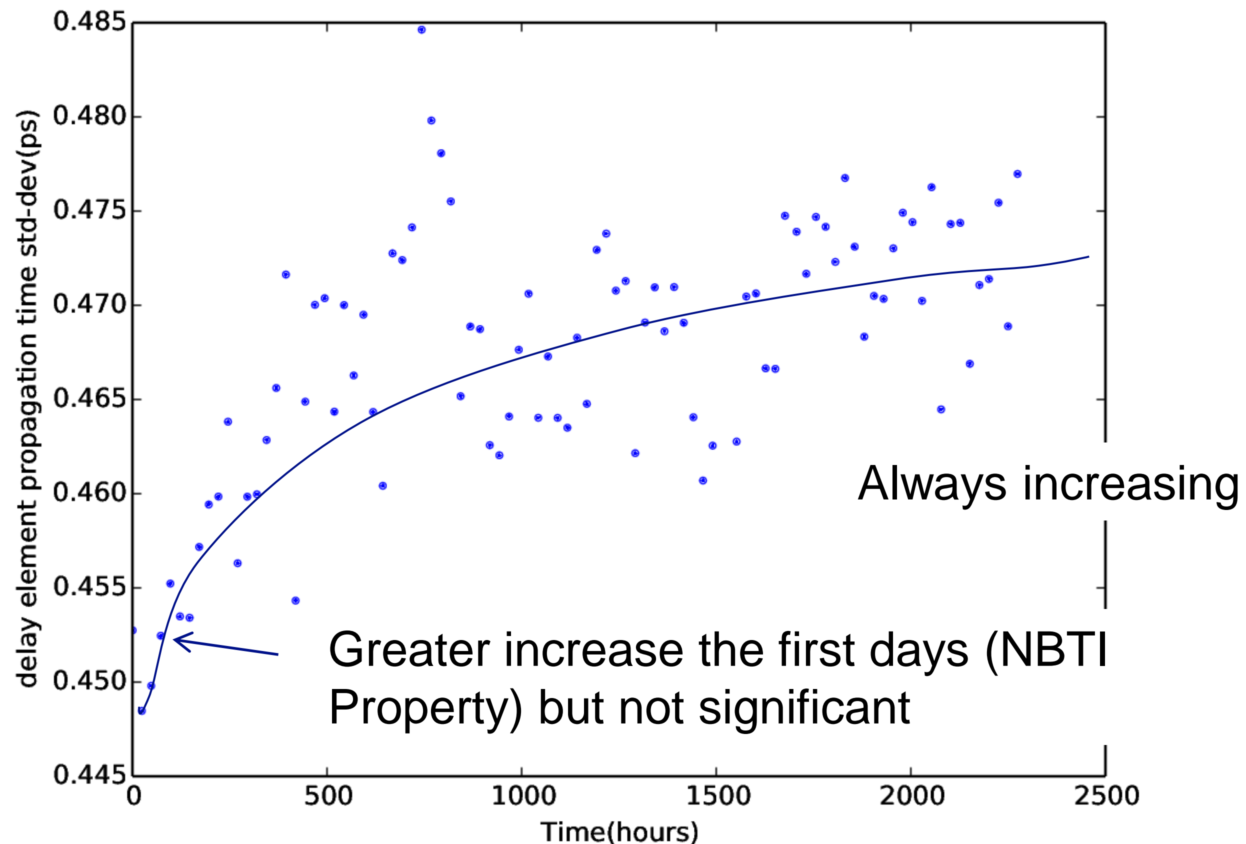
TELECOM ParisTech

Aging impact on the std deviation of the differential value

$$\lfloor N\sum_{i=1}^{n} d(c_i)\rfloor - \lfloor N\sum_{i=1}^{n} d(-c_i)\rfloor)$$

Mean on 49 PUFs
Challenge = 0x00000000FFFFFFFF

Std deviation of the delay for one element



TELECOM ParisTech

Agenda

- Aging and delay PUFs
- Aging simulation
- Aging acceleration on real silicon
- **Conclusions**

Conclusions 1/2

- **The aging has a very small impact on delay chains**
  - The std deviation increases of 0.02 ps / element after 1000 hours
  - The aging impact on the mean is small, not extractable from noise
  - The results of the aging acceleration on real silicon of the combinational path confirms the simulation
- **The aging has a significant impact on the arbiter**
  - More than 1% BER after one year

TELECOM ParisTech

Conclusions 2/2

- **The NBTI effect is dominant**
  - Aging even if no activity
  - The memory points (as RS latch of the arbiter) are very impacted by NBTI aging due to the imbalance.
- **The HCI appears with intense switching activity**
- **Loop PUF and RO-PUF natively less impacted than Arbiter PUF and SRAM PUF**