Some results about the Aging Impact on Delay PUFs

Cryptarchi

June 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

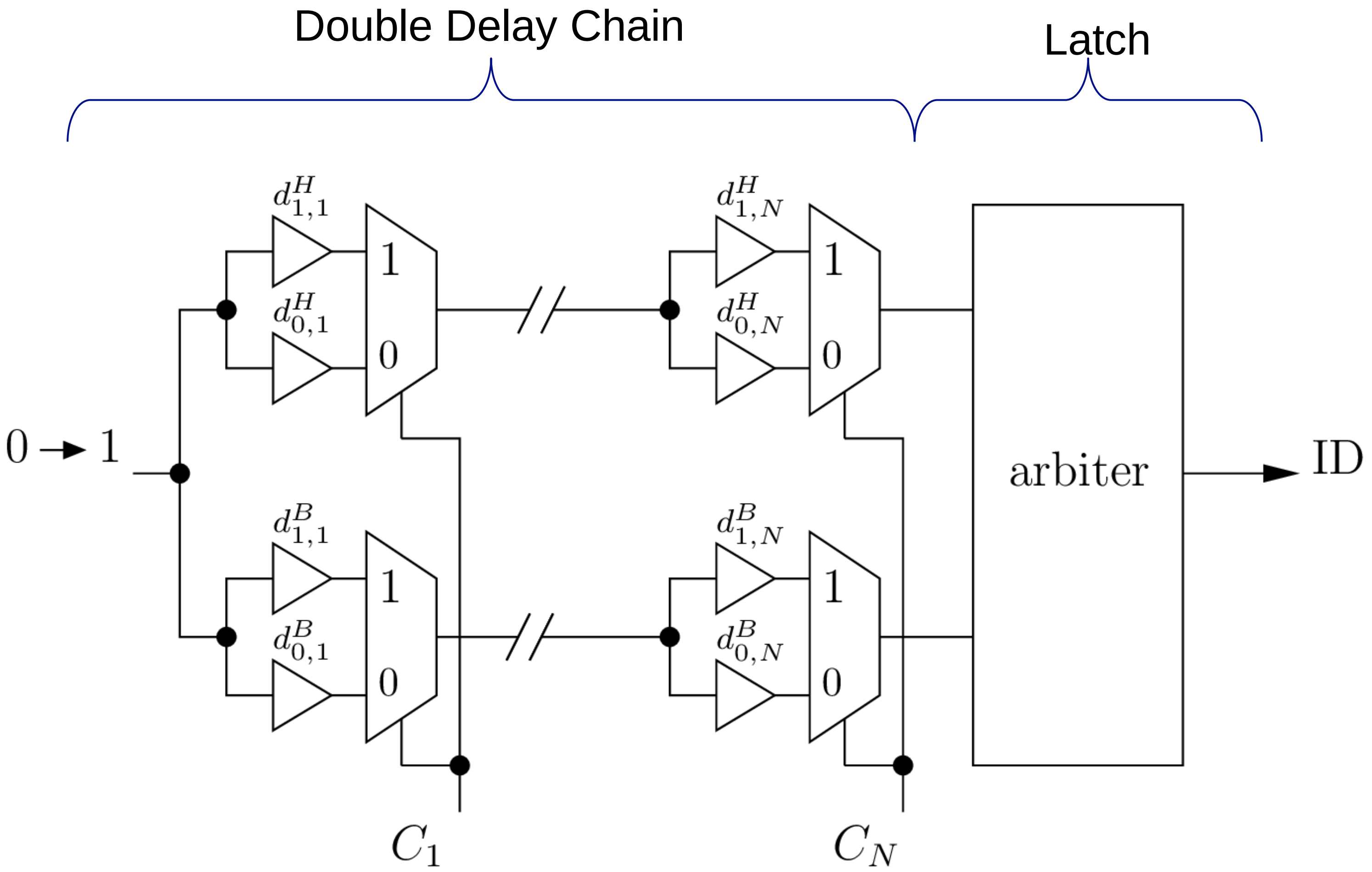
Agenda

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

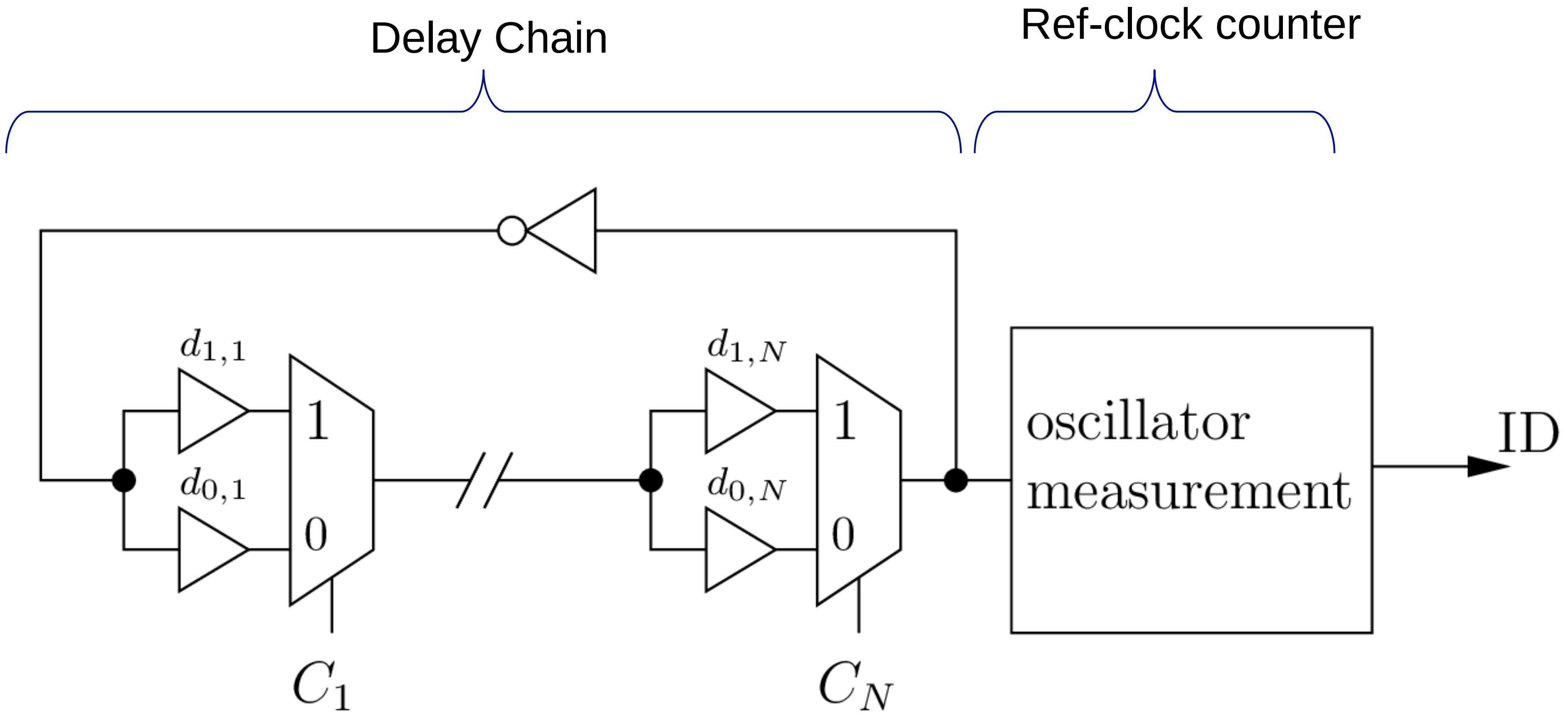
Aging

- **Gate Oxide**
  - Negative Bias Temperature Instability (**NBTI**)
    - Cause: Holes creating traps between Si-O2 and substrate
    - 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
  - 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: net breakdown

Delay PUF: Arbiter PUF



Delay PUF: Loop PUF



APUF vs LPUF differences

n delay elements

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

Latch Arbiter race comparator

Delay line 1

Delay line 2

n delay elements

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

Subtractor

N loops

Delay line
with challenge C

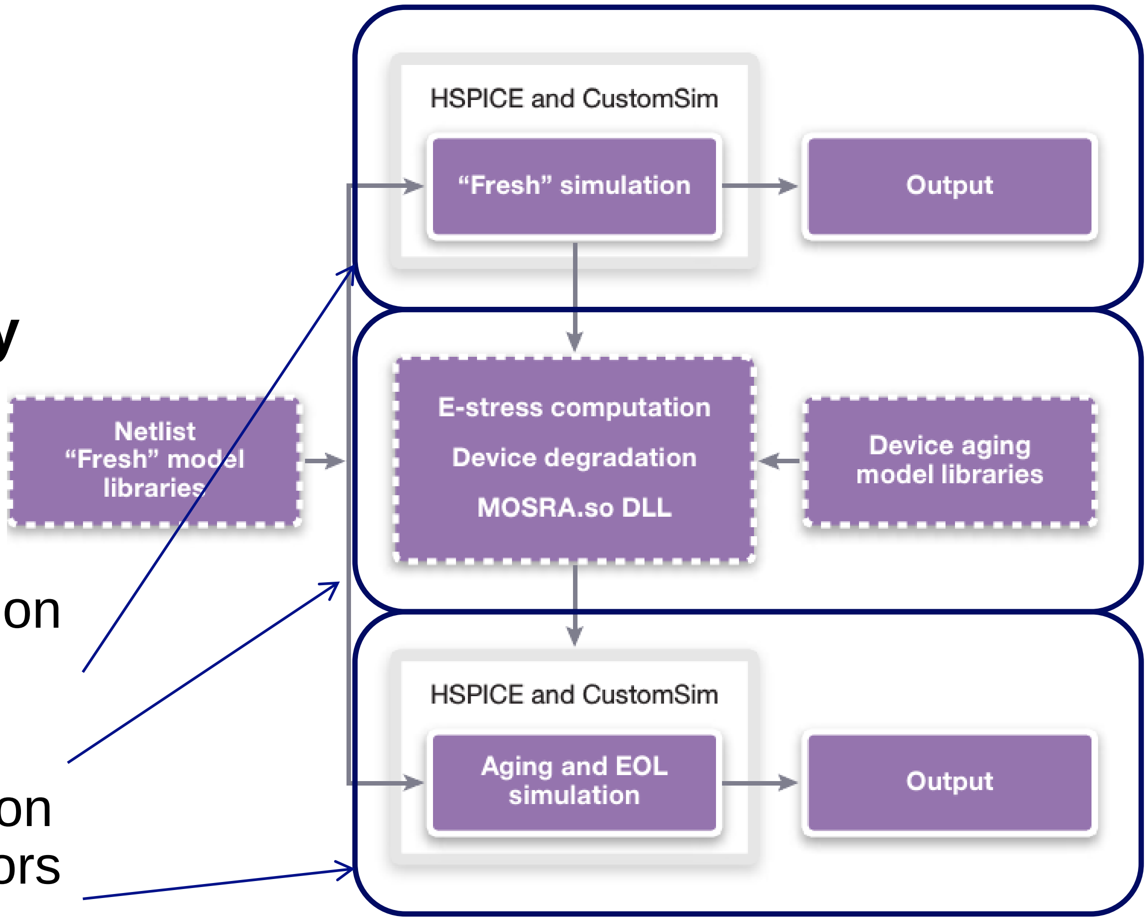
Delay line
with challenge –C

Agenda

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

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



Aging simulation of delay-chain PUF

Number of elements — Challenge bit — Complementary Challenge bit

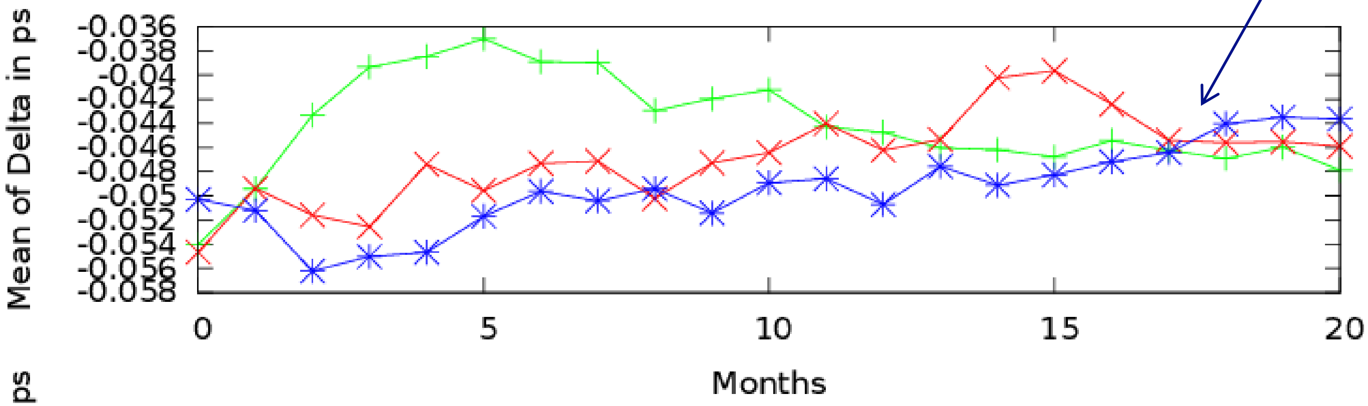
Measurement of Delta = $$\left(\sum_{i=1}^{n} d(c_i) - \sum_{i=1}^{n} d(-c_i)\right)$$

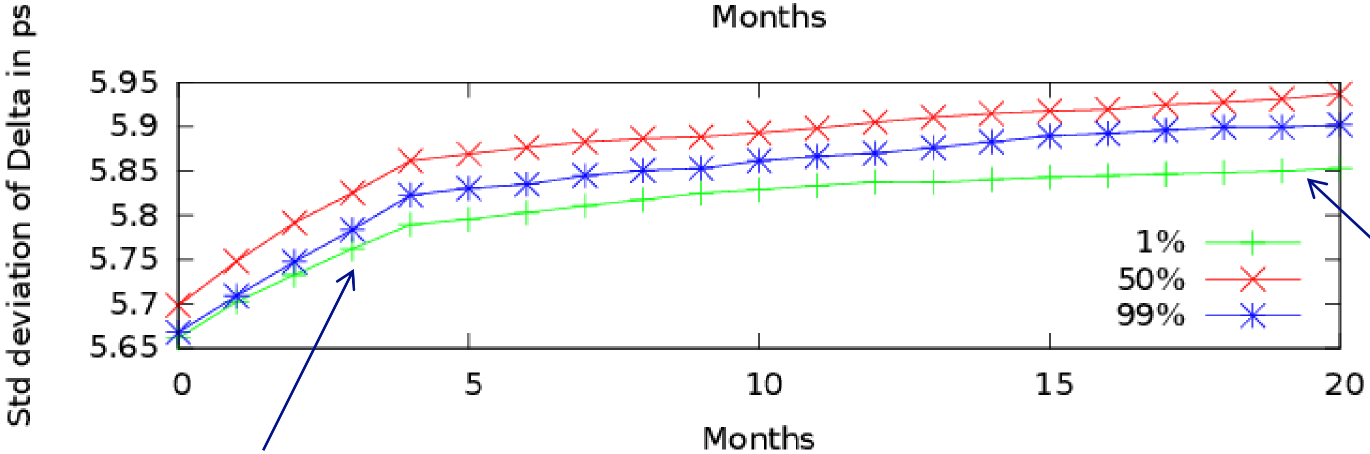
Aging simulation parameters:

- 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 " (no NBTI aging)

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

The aging has no monotonous impact on the mean



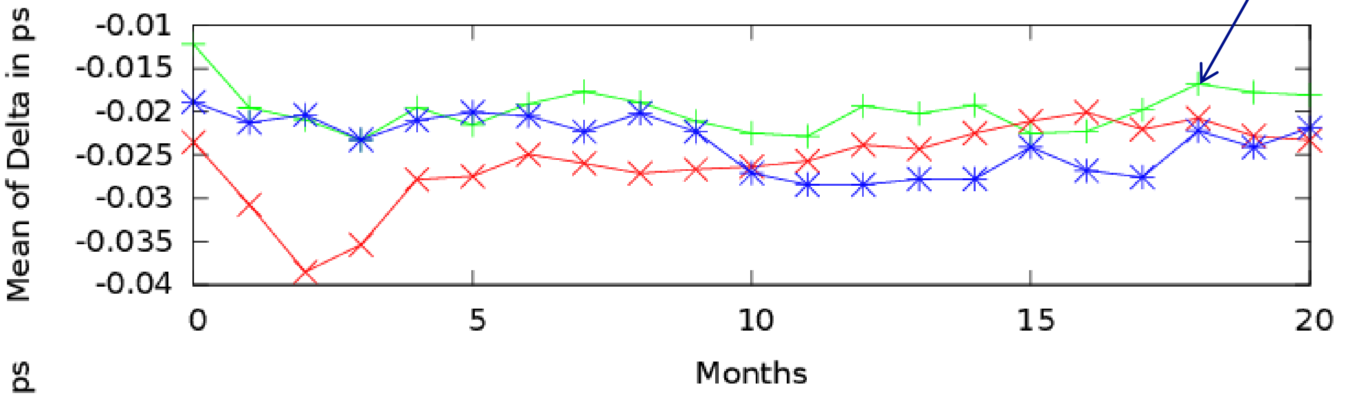


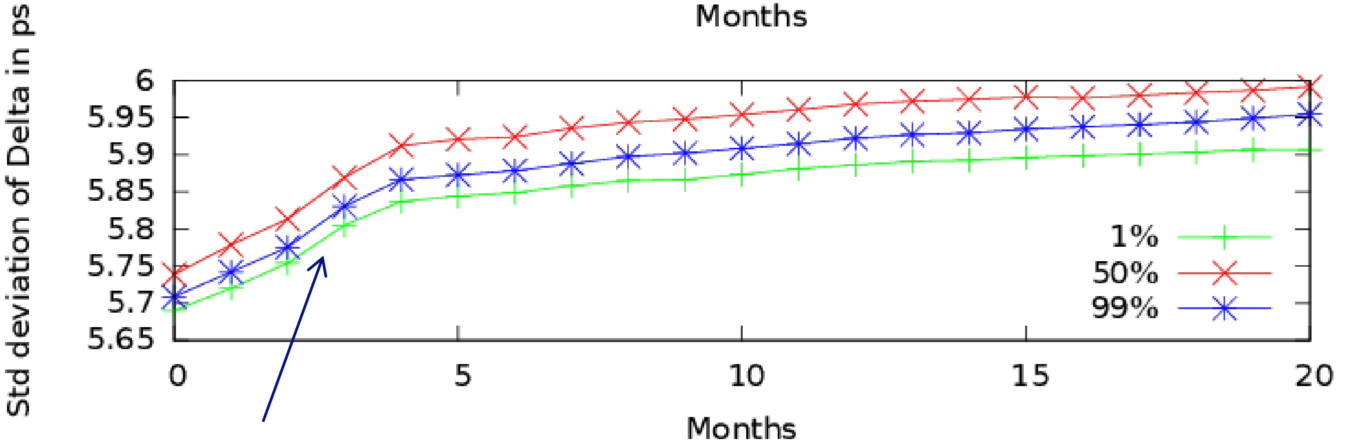
The std deviation always increases
Greater increase the first months

The slope with 1% duty cycle is slightly smaller

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

The aging has no monotonous impact on the mean



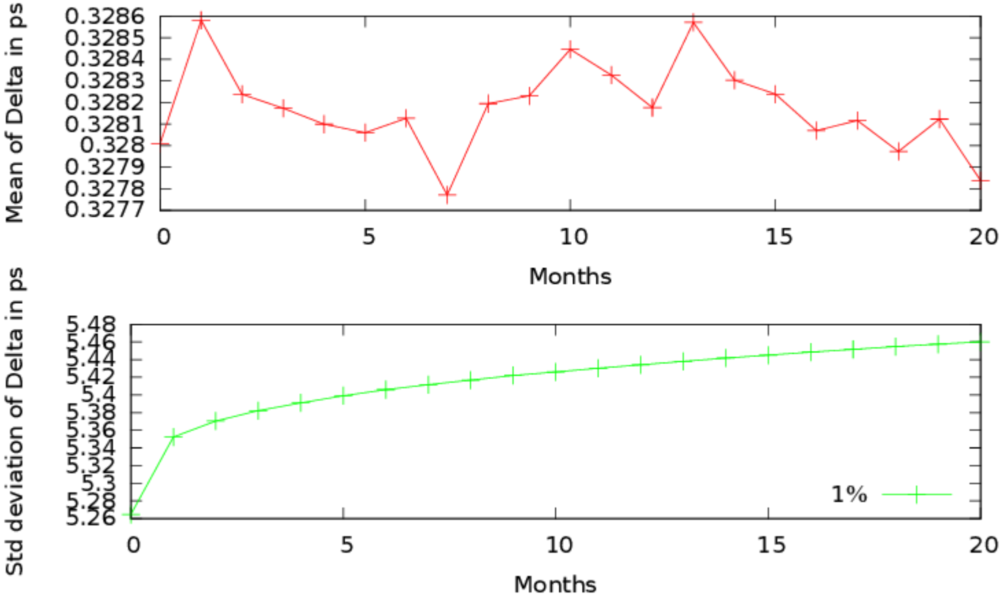


The std deviation always increases
Greater increase the first months

Aging simulation of arbiter PUF

2 parts:

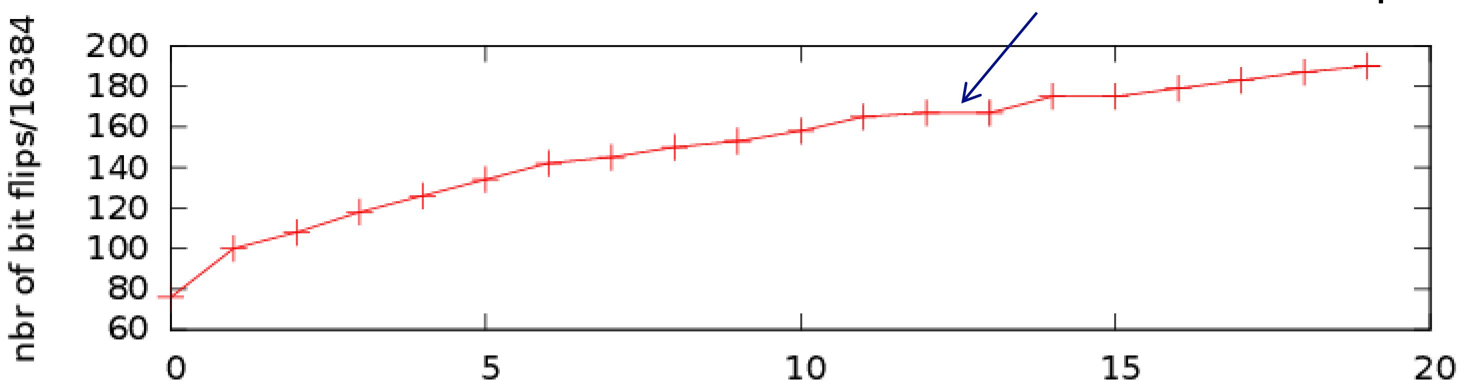
- **1. Delay chain**
  - Very similar to the Loop PUF



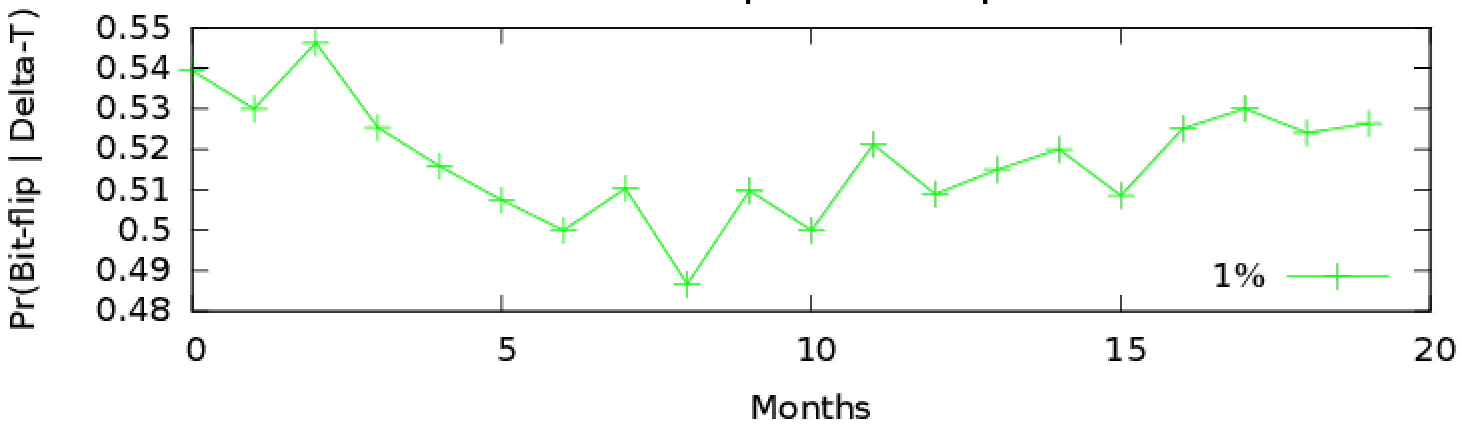
- **2. Arbiter**
  - Result =number of bit flips among 16384 arbiter latches

Aging simulation of the arbiter only

More than 1% of bit flips after 1 year



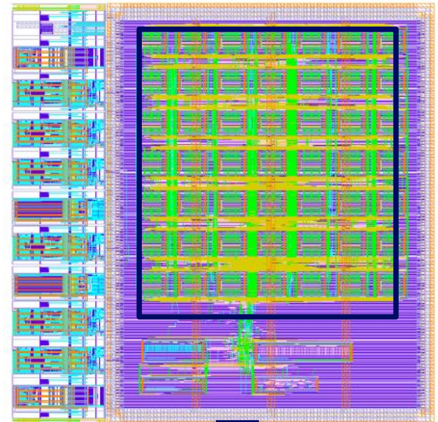
The bit flips are independent on the variation of delta



Agenda

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

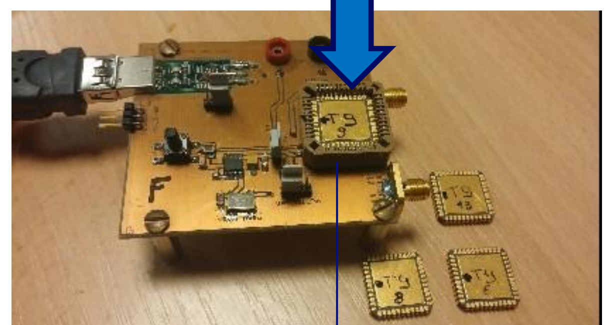
Aging acceleration

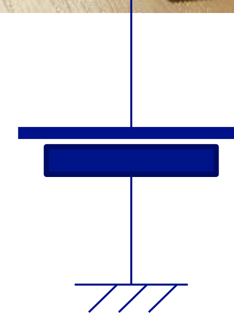


49 LPUFs

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

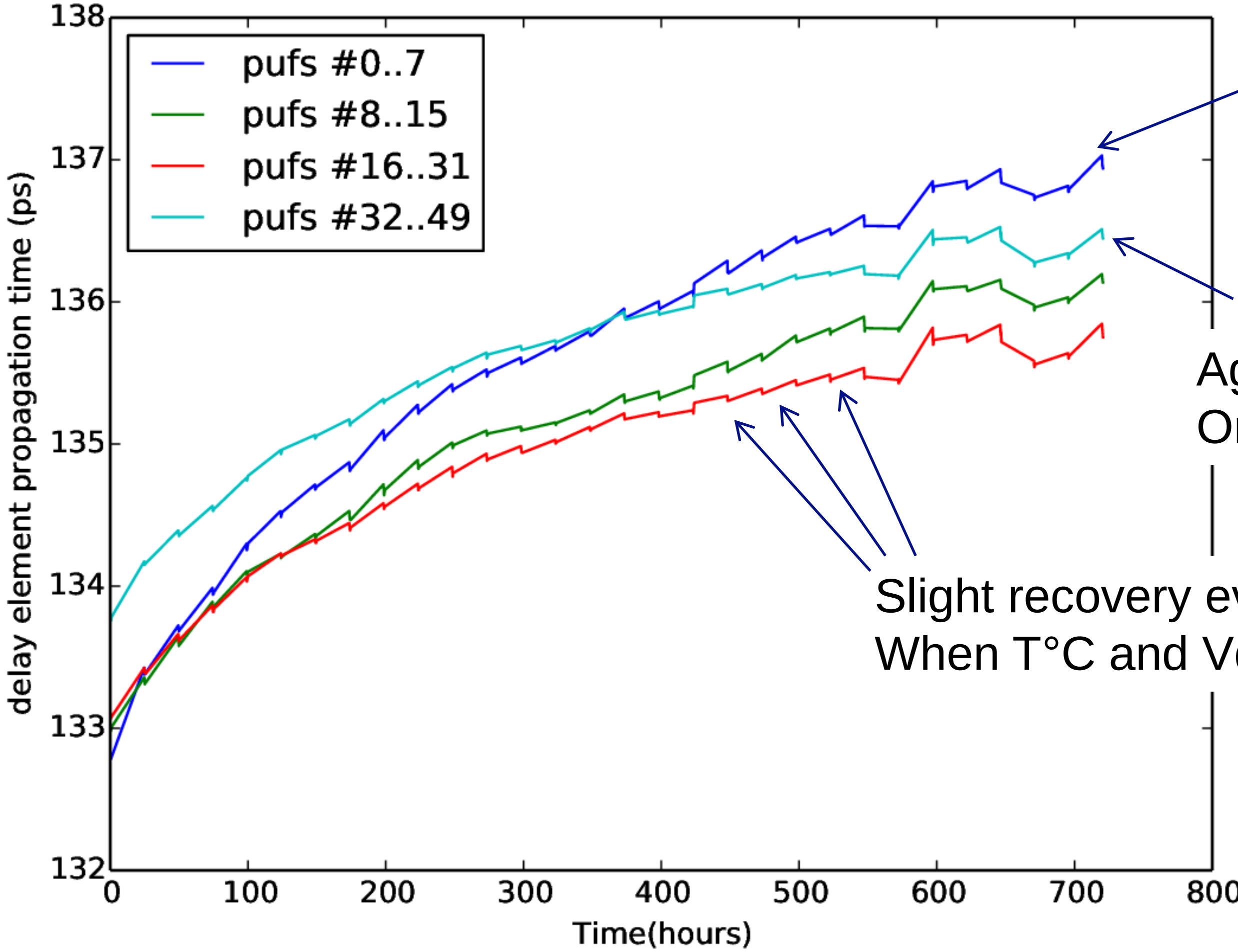
Aging acceleration procedure

- **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**

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

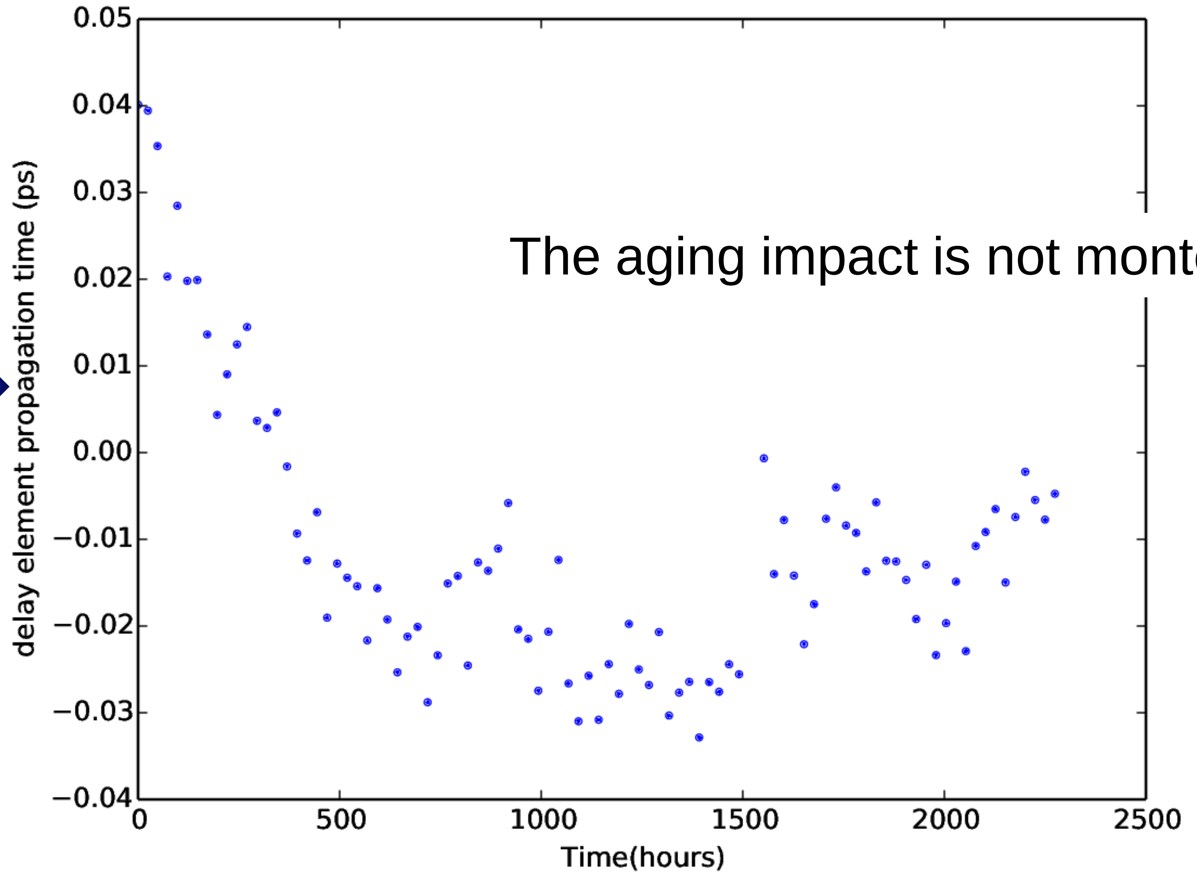
TELECOM ParisTech

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



The aging impact is not montonous

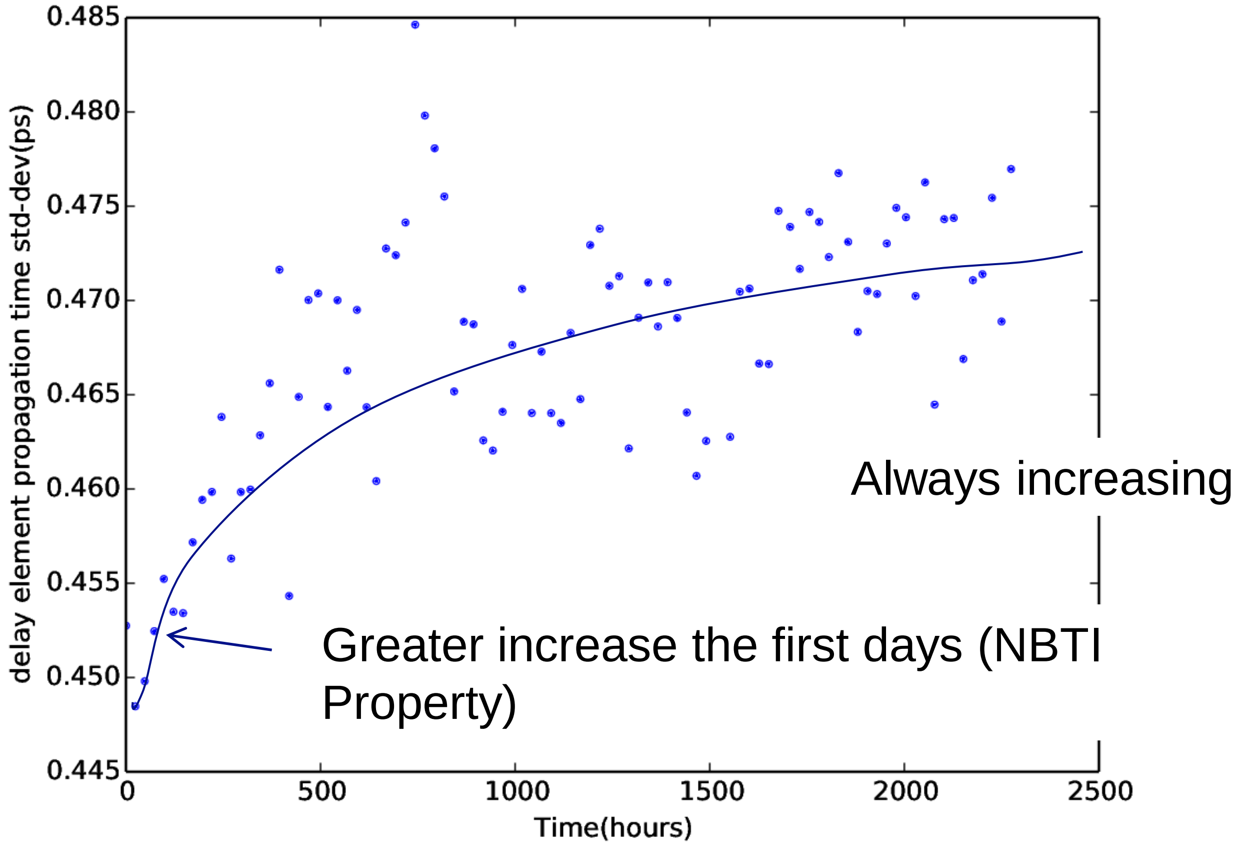
TELECOM ParisTech

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



Agenda

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

Conclusions

- **The results of the aging acceleration confirms the simulation**
- **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 not a monotonous function
- **The aging has a significant impact on the arbiter**
  - More than 1% bit flip after one year (simulation)
- **The NBTI effect is dominant**
  - Aging even if no activity
- **The HCI appears with intense switching activity**
- **Perspectives**
  - Validate the Arbiter bit flips results on a real circuit
  - Simulate with the 65nm technology