Impact of Process Mismatch and Device Aging on SR-Latch Based True Random Number Generators

Javad Bahrami
Mohammad Ebrahimabadi
Naghmeh Karimi

University of Maryland Baltimore County

Jean-Luc Danger *
Sylvain Guilley *°

*** Télécom Paris**
° Secure-IC S.A.S

UMBC
AN HONORS UNIVERSITY IN MARYLAND

SECURE-IC
THE SECURITY SCIENCE COMPANY

TELECOM Paris

IP PARIS

Outline

Motivation

Principles of SR-latch TRNG

Stochastic Model

Device Aging

Experimental Setup and Results

Conclusion and Future Work

Motivation

- True Random Number Generators (TRNGs) are critical for security provision through cryptographic modules
- The ring oscillator-based TRNG introduced in 2007 to fulfill this requirement
- Current security assurance requires at least two sources of randomness (to prevent SPOFs)
- Requirement for Hi-Speed TRNG (>1Gb/s)

- **Attentions toward SR-latch based TRNGs**

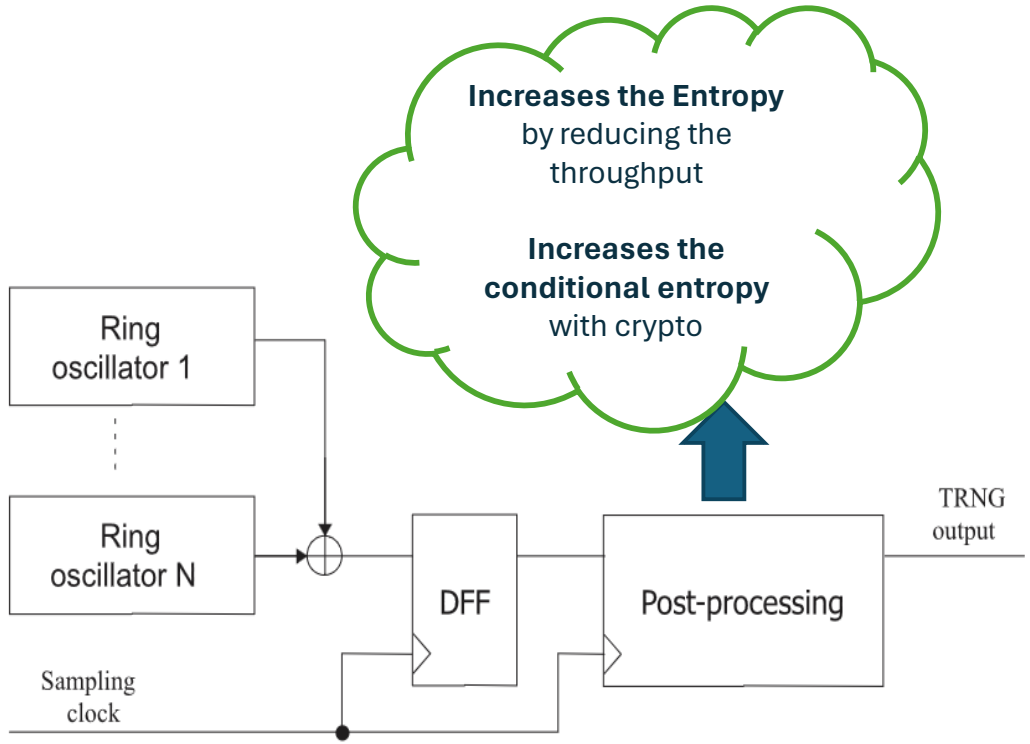
- Are these SR-latch based TRNGs remain efficient over time?
  - How is the uniformity affected over time?
  - Does it make the TRNG biased?

True Random Number Generators

❑ Applications

- Initialization vectors (AES-CBC)
- HMAC Keys (key generation)
- Authentication challenges
- Side-channel protection random numbers
- ECDSA Nonces
- Crystals Kyber Noise

❑ RO-based TRNGs



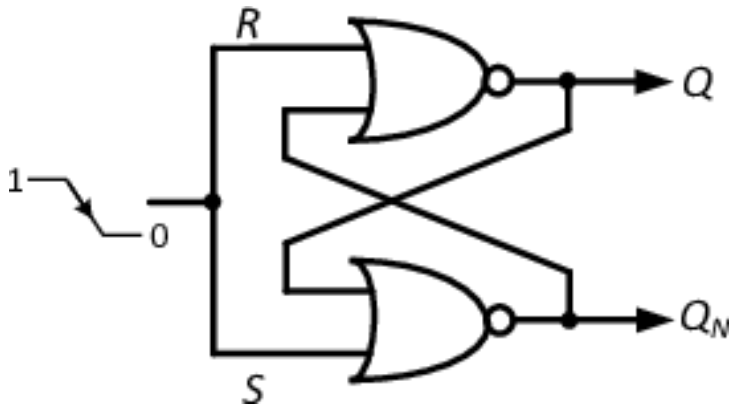
Very common, but medium throughput, power hungry, sensitive to PVT variations

Outline

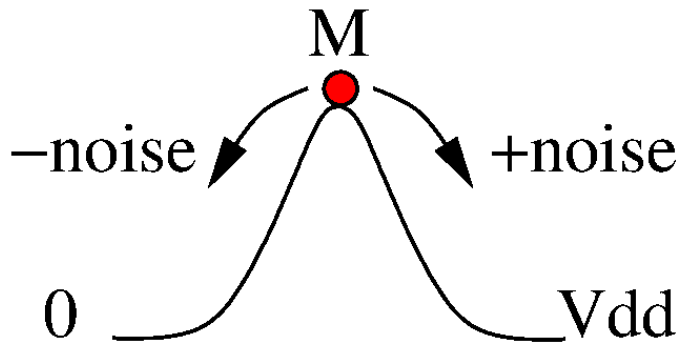
SR-latch based TRNGs

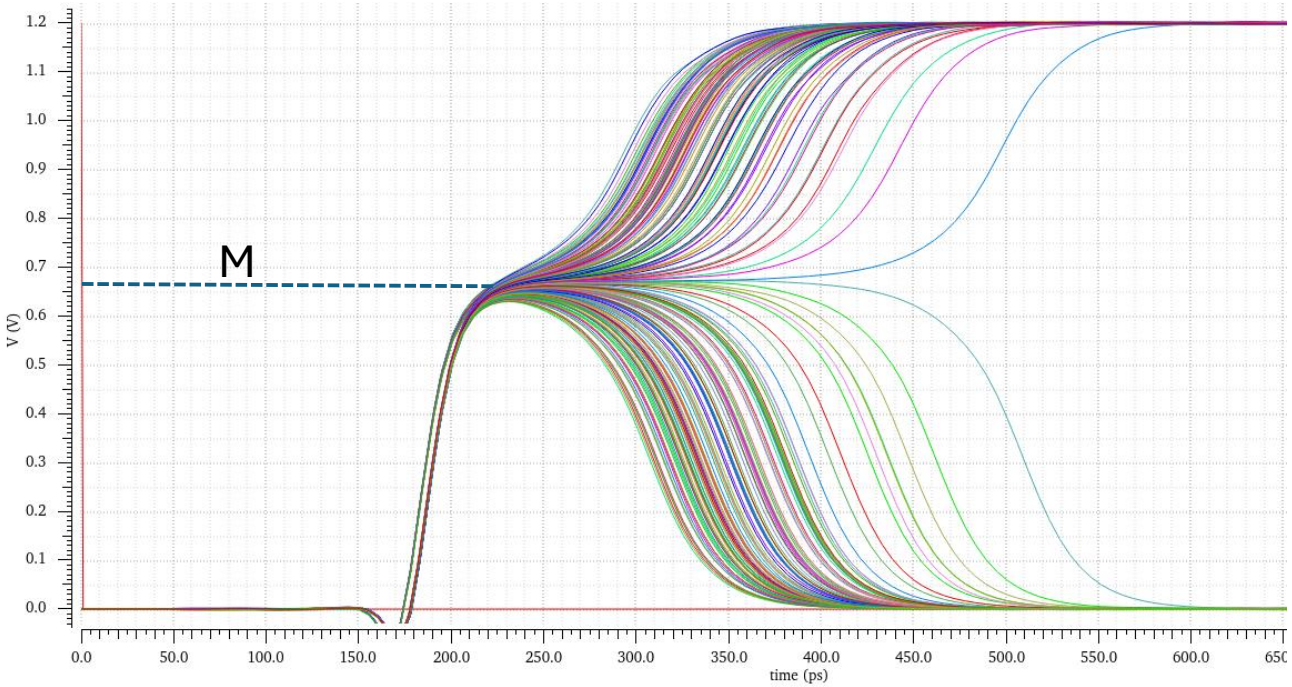
With a small **noise** around M, Q will converge to a stable state randomly ⇨**TRNG**

SPICE simulation



M=Metastable state

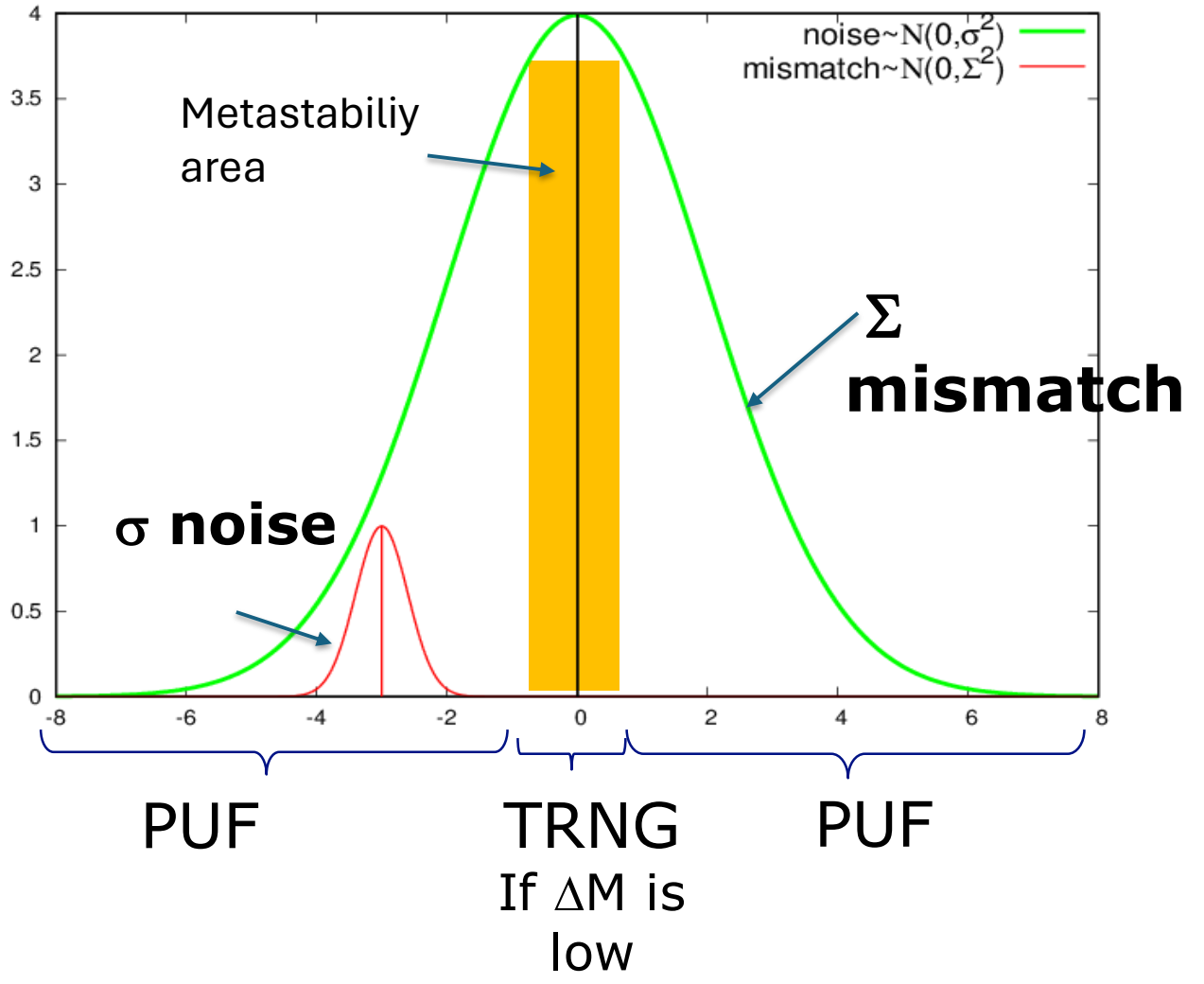




PUF Vs. TRNG

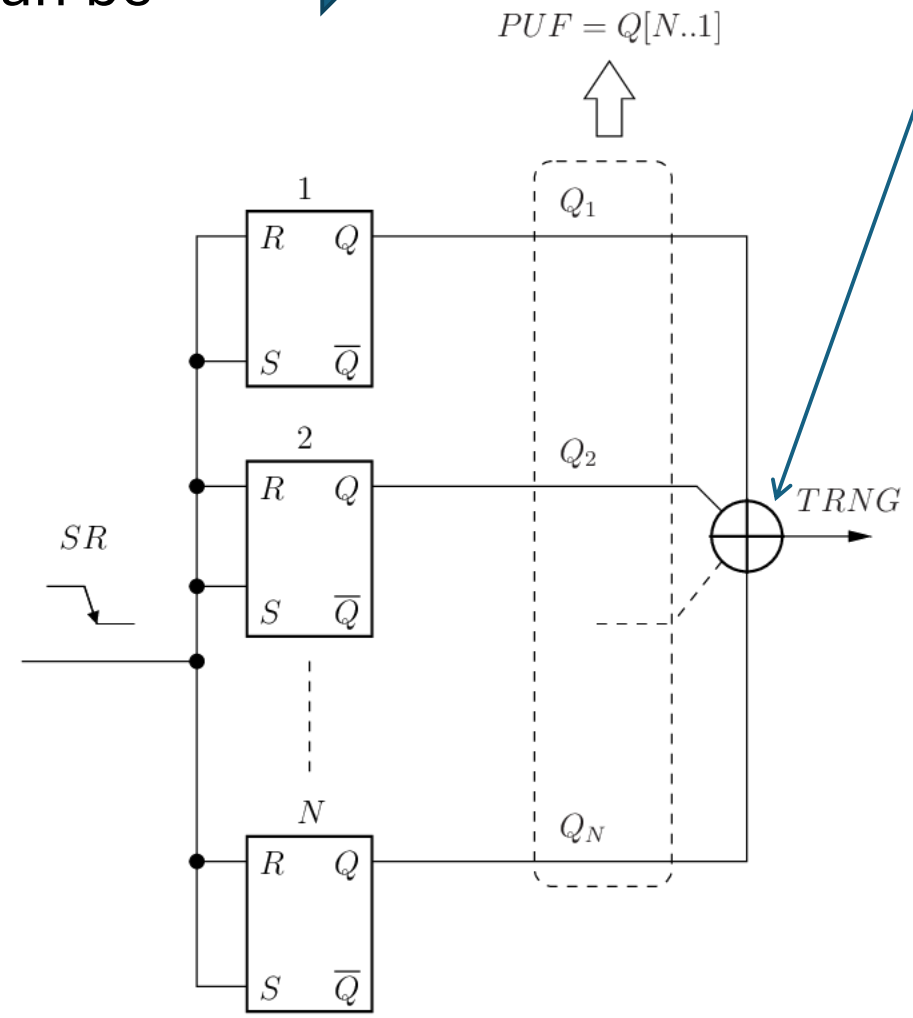
- An imbalance due to the **mismatch** between the two NOR gates makes the SR-latch behave like a PUF
- This mismatch is equivalent to a **delay offset** ΔM between the S and R input.

pdf of the delay offset ΔM to characterize the mismatch between two 2 NOR gates



Among a set of *N* SR-latches, some of them are statistically near the metastable state. The others can be used as PUF

TRNG = XOR(*N* SR-latches)



Set of SR-latches

Important Question:

What is the value of *N* to get a good entropy ?

Outline

Stochastic Model

Probability of the TRNG

If *pi* is the probability that latch *i* is at '1' then *pi* of the ideal latch should be *pi = ½*

We define the bias $\varepsilon_i = p_i - 1/2$

By applying the piling-up lemma, The probability $P_0 = \mathbb{P}[TRNG = 0]$ ORing N latches is:

$$P_0 = 1/2 + 2^{N-1} \prod_{i=1}^{N} \varepsilon_i,$$

The mismatch is characterized by a **delay offset** ΔM between the S and R inputs:

$$\Delta_M \sim \mathcal{N}(0, \Sigma^2)$$

The noise *Z* is considered gaussian: $Z \sim \mathcal{N}(0, \sigma^2)$

We define the Mismatch to Noise ratio as:

$$\mathrm{MNR} = \frac{\Sigma}{\sigma}$$

This MNR ratio has to be as low as possible for the TRNG

Stochastic Model

Mean Entropy

We demonstrated that the closed form of the mean bias according to MNR is:

$$\widehat{|\varepsilon_i|} = \frac{1}{\pi}\arctan\left(\mathrm{MNR}\right)$$

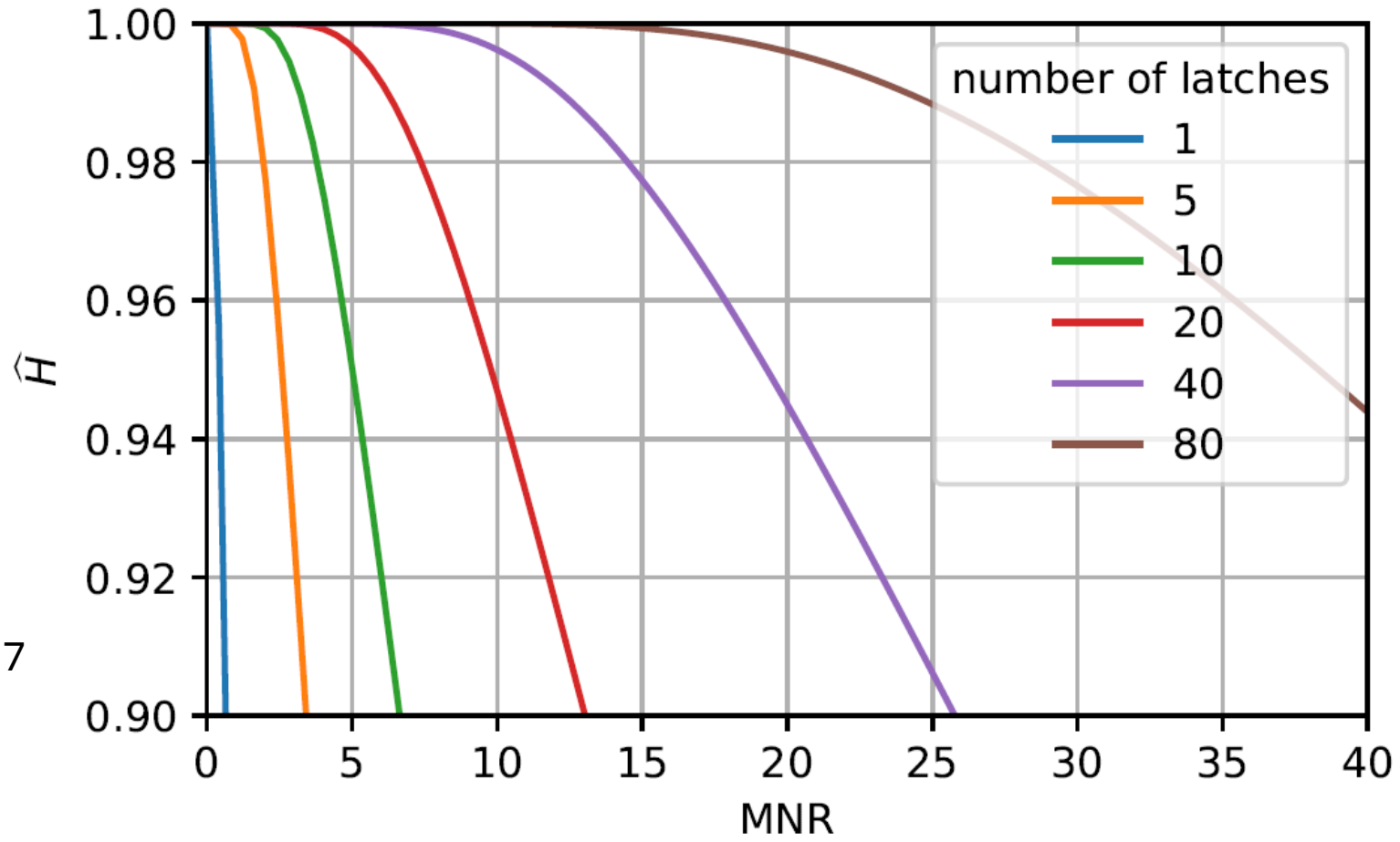
By considering that the pi are independent, the mean probability of the TRNG is:

$$\widehat{P_0} = 1/2 + (-1)^s \cdot 2^{N-1}\left(\frac{1}{\pi}\arctan\left(\mathrm{MNR}\right)\right)^N \qquad s = sign(\textstyle\prod_{i=1}^{N}\varepsilon_i)$$

The mean Shannon Entropy can be computed with $\widehat{P_0}$ $\widehat{P_1} = 1 - \widehat{P_0}$

$$\widehat{H} = -\sum_{i\in\{0,1\}} \widehat{P_i}\log(\widehat{P_i})$$

Mean Entropy of the TRNG according to MNR

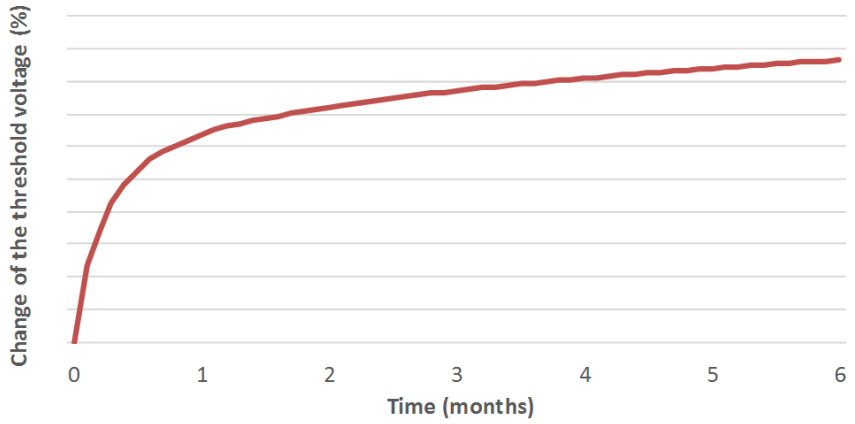


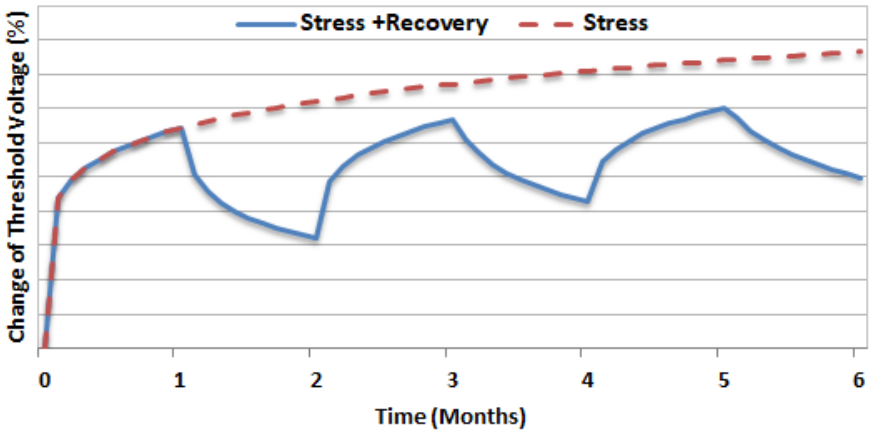
MNR has been estimated at 7 in FD-SOI 28nm [1]

[1] Danger, J. L., Yashiro, R., Graba, T., Mathieu, Y., Si-Merabet, A., Sakiyama, K., ... & Nagata, M. (2018, August). Analysis of mixed PUF-TRNG circuit based on SR-latches in FD-SOI technology. In *2018 21st Euromicro Conference on Digital System Design (DSD)* (pp. 508-515). IEEE.

Outline

Device Aging





- **Hot Carrier Injection (HCI)**
  - Cause: Electrons colliding with the gate oxide (rather than going only to the conduction channel between source and drain)
  - Impact: V_{th} increase

- **Negative Bias Temperature Instability (NBTI)**
  - Cause: Holes creating traps between Si-SiO2 and substrate
  - Impact: V_{th} increase, (stress & recovery modes)

- **We are to investigate how the SR-Latch Based TRNG Works during the course of usage (when aged)**

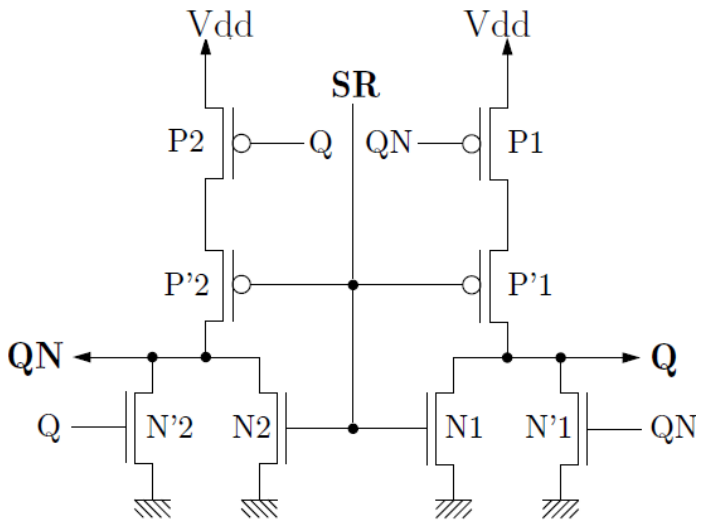
Outline

First order analysis

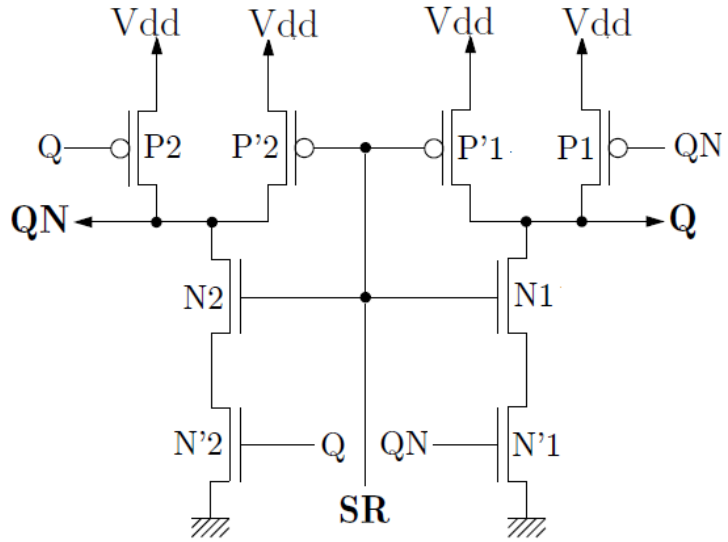
Impact of Aging on V_{th} of TRNG's Transistors

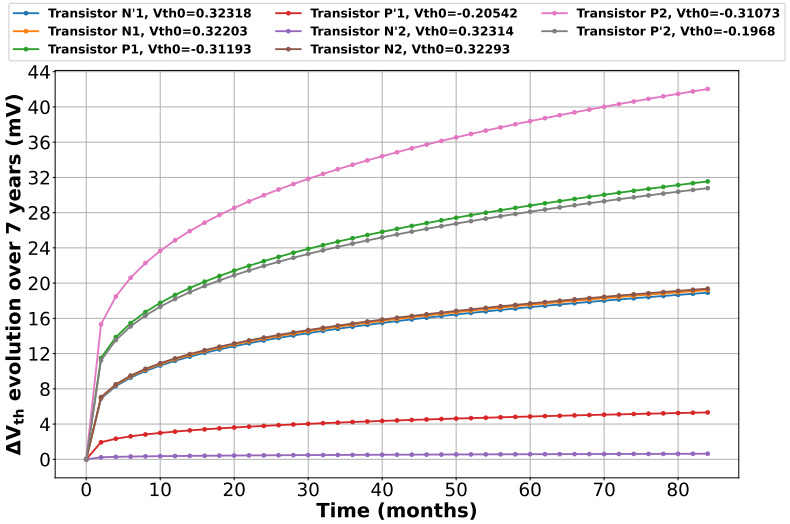
NBTI an PBTI Aging makes the latch to go toward metastability

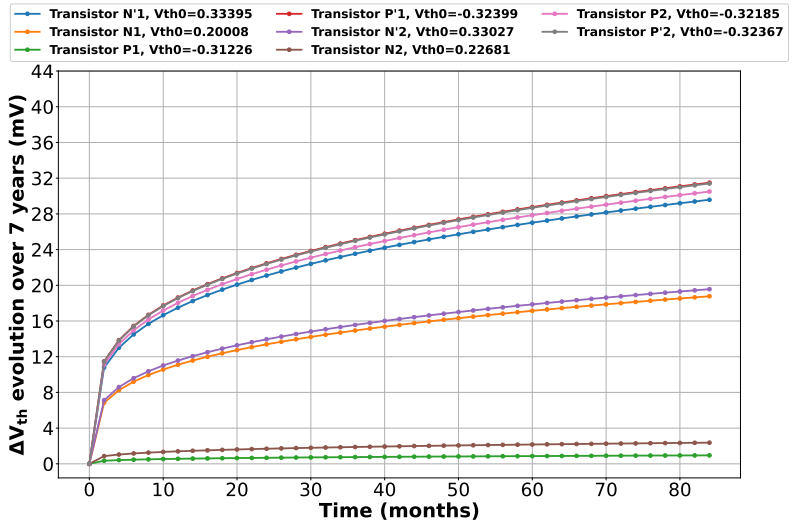
NOR-based TRNG



NAND-based TRNG



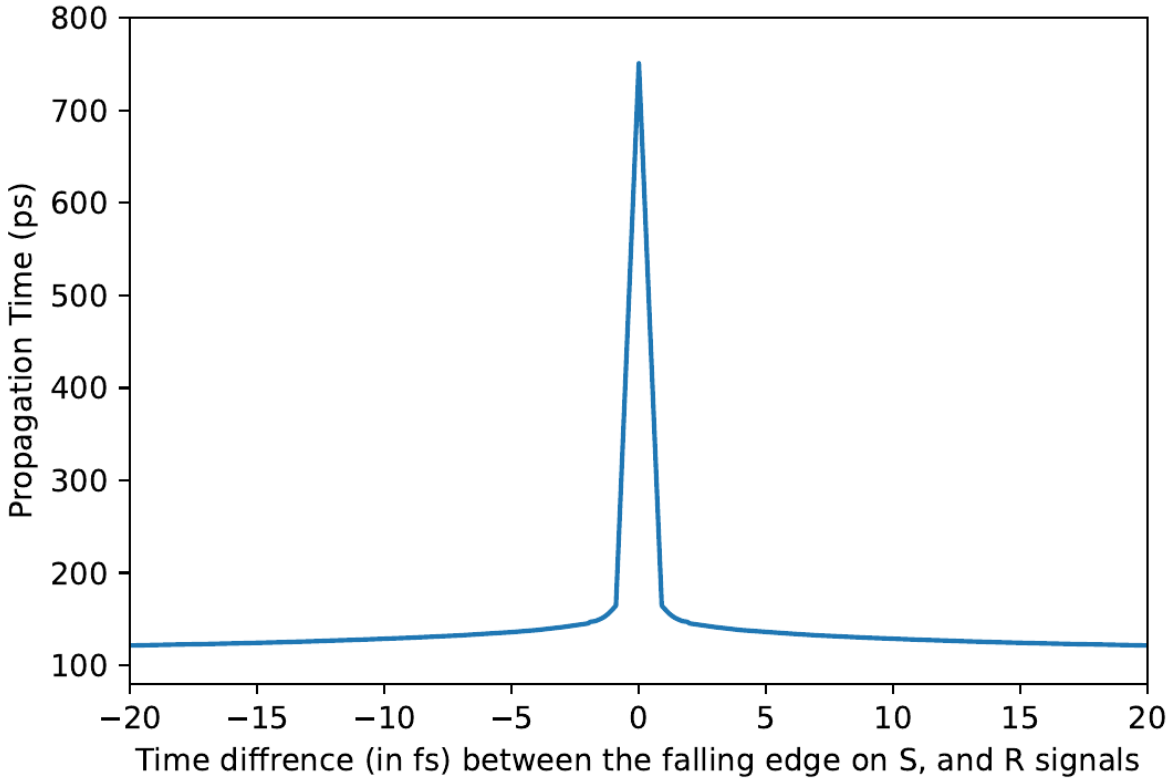




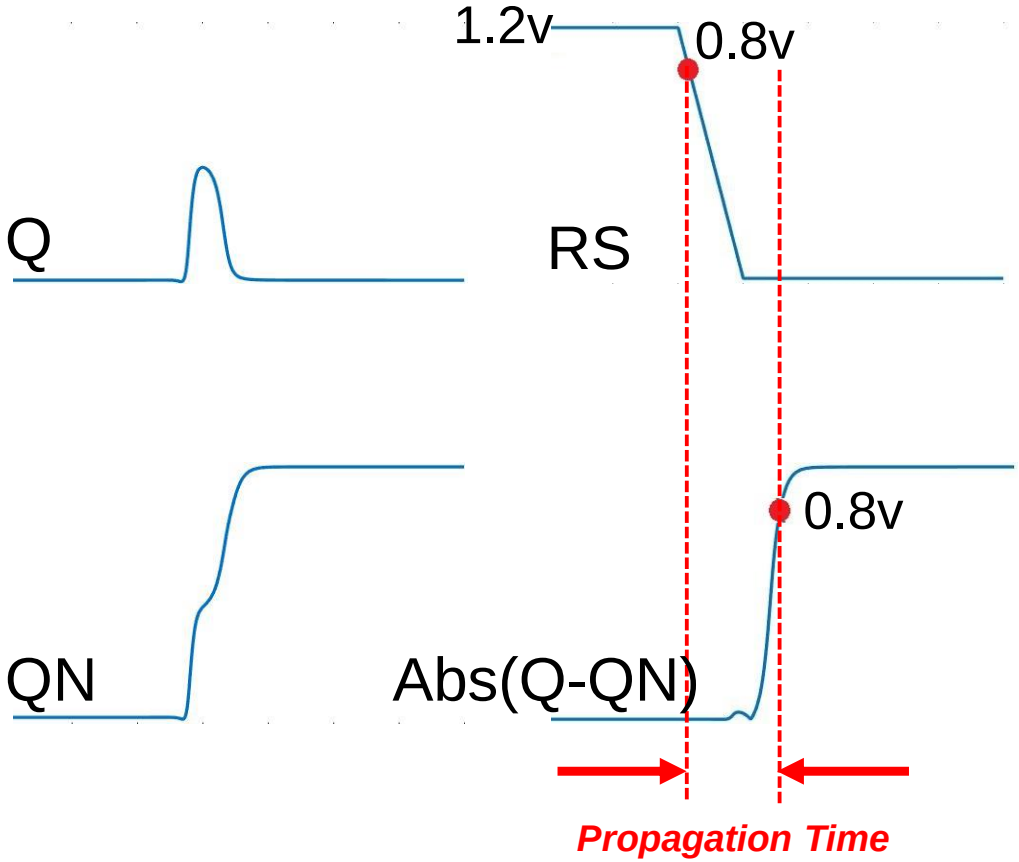
Timing Analysis

- Our circuit includes 1024 latches
- 45nm open-source NANGATE technology
- Hspice Monte-Carlo simulation
  - Transistor gate length → $L: 3\sigma = 10\%$
  - Threshold voltage (V_{th}) → $V_{th}: 3\sigma = 30\%$
  - Gate oxide thickness → $t_{ox}: 3\sigma = 3\%$
- $Temp = 85^{o}, V_{dd} = 1.2V, Freq. = 500\ MHz$
- Impact of 7 years of aging

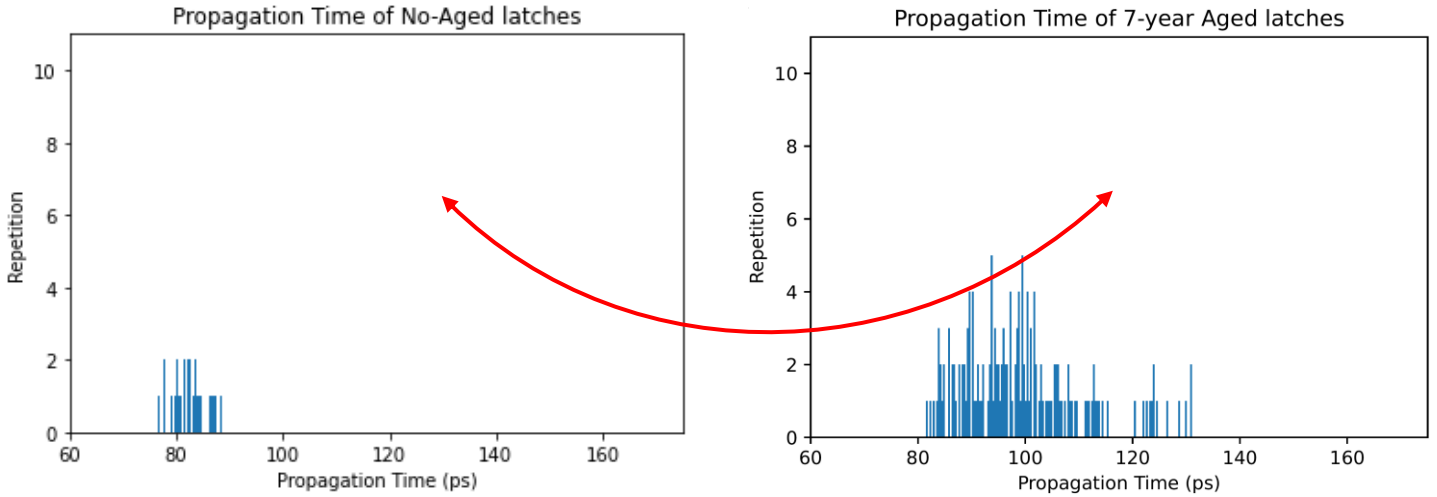
The propagation time drastically increases when approaching metastabilty



Impact of Aging on Propagation Time of SR-Latches that keep the same state (cont'd)



- The propagation time is defined as the time difference from when the SR signal crosses 0.8 V until the absolute value of (Q – QN) exceeds 0.8 V.



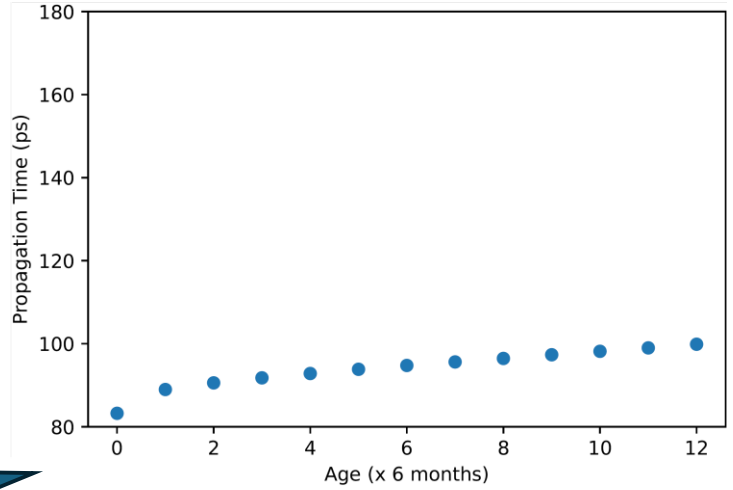
The propagation time of SR-Latches that the toggling state in new and 7-years aged devices are observed on *QN:*

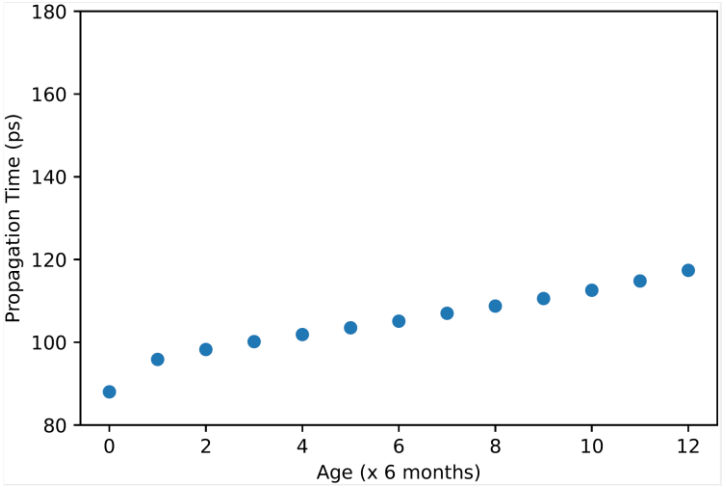
Propagation Time is increased by aging
(**82.4**ps to **99.35**ps)

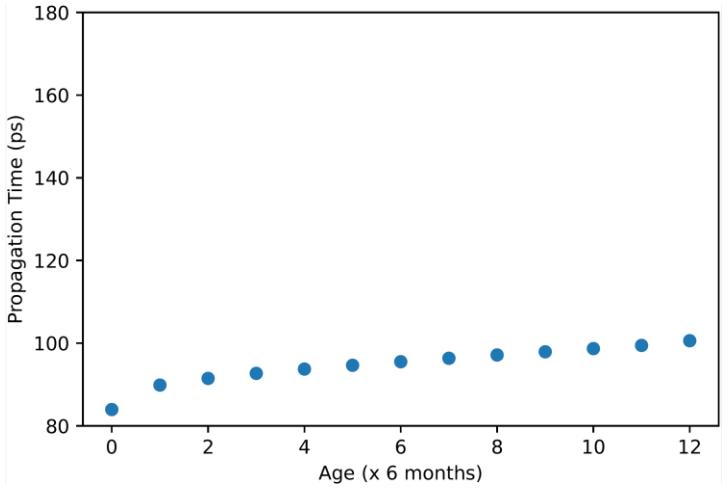
Impact of Aging on Propagation Time of SR-Latches that keep the same state (cont'd)

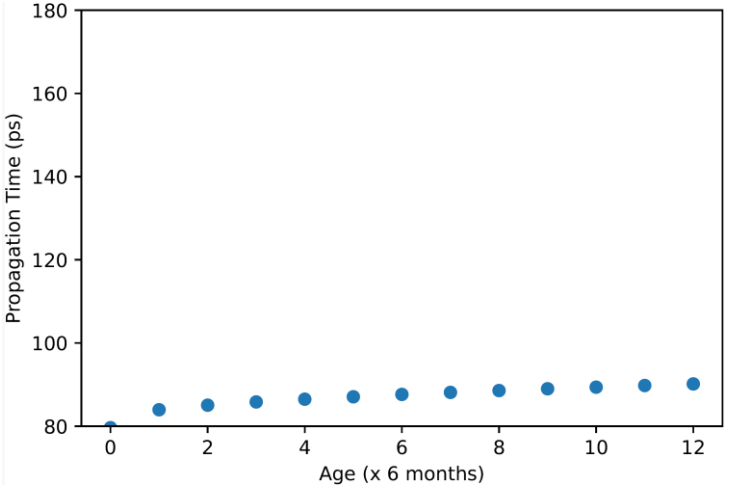
- Evolution of propagation time with aging for 4 sample latches keeping the state Q=1 (top row) and QN = 1 (bottom row):

Aging moves SR-Latches toward metastable state, and improves entropy





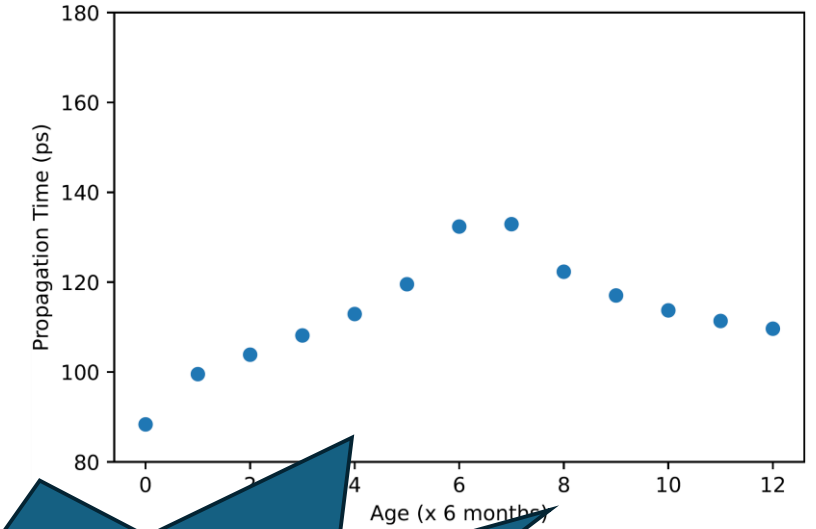




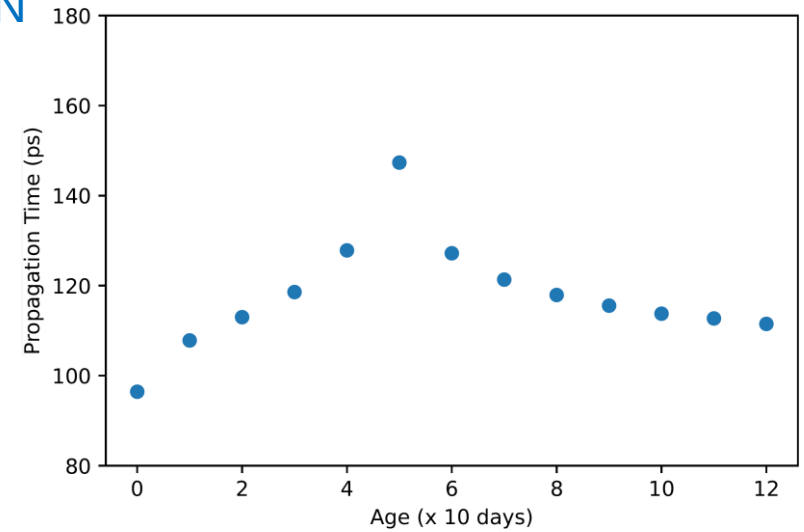
Impact of Aging on Propagation Time of SR-Latches with state toggling

- Evolution of propagation time with aging for 2 sample latches
- Propagation time is increased, then after specific ages the PG monotonically is decreased

New Device Toggle in QN, Aged Device Toggle in Q



New Device Toggle in Q, Aged Device Toggle in QN



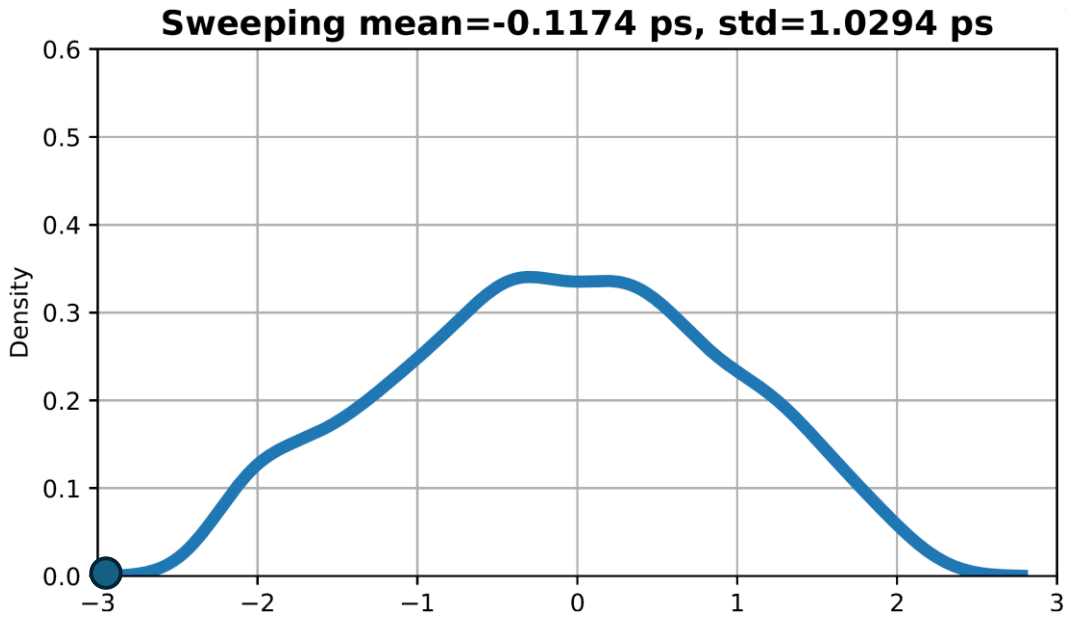
In Latches near metastable, aging moves away from metastable state.

Process mismatch characterization (ΔM_i distribution)

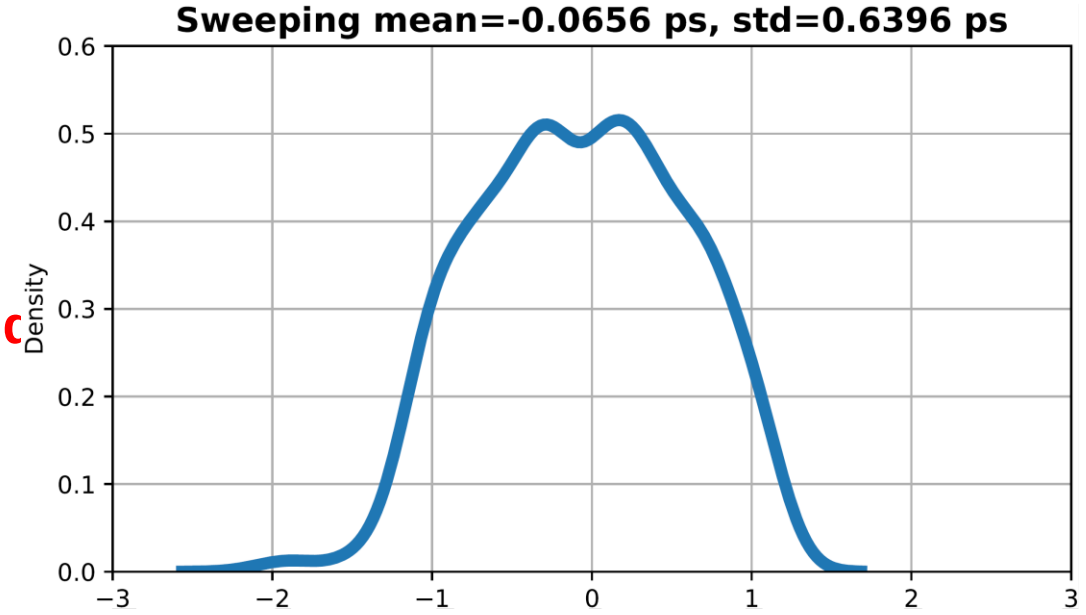
- Sweeping ΔM until we observe a transition in output.

SR-Latch based TRNG becomes more metastable over time

Age 0



7-year old



Mean Entropy Evaluation Example

$$H = -P_0 \log(P_0) - P_1 \log(P_1)$$

- Entropy is increased with the number of latches
- Aging slightly improves the entropy

MNR = 10, $\sigma_{noise} = 100\ fs$

year \ #latches	20	40	80
0	0.833	0.985	0.997
2	0.927	0.995	0.999
4	0.960	0.999	1
6	0.940	0.995	1

MNR = 20, $\sigma_{noise} = 50\ fs$

year \ #latches	20	40	80
0	0.580	0.876	0.943
2	0.700	0.918	0.995
4	0.731	0.923	0.994
6	0.721	0.913	0.999

Outline

Conclusion and Future works

- Building of the Stochastic model of the SR-latch TRNG to size the number of latches of the architecture
- We shown that Aging has globally a positive impact on the entropy of the SR latch.
- Future works are to confirm our results on real devices with different process mismatch and noise levels.