WRAC'H 2019

Analysis of Mixed PUF-TRNG Circuit Based on SR-Latches in FD-SOI Technology

Jean-Luc DANGER, **Télécom ParisTech**

In collaboration with:

Risa Yashiro, Kazuo Sakiyama (UEC)

Noriyuki Miura, Makoto Nagata (Kobe University)

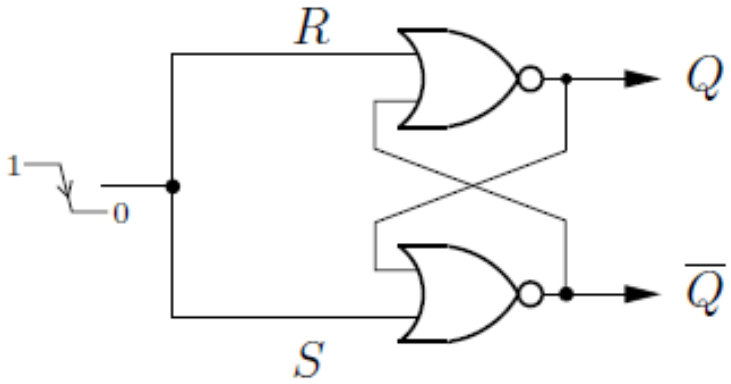
Yves Mathieu, Tarik Graba, Abdelmalek Si-Merabet (TPT)

Sylvain Guilley (Secure-IC)

Outline

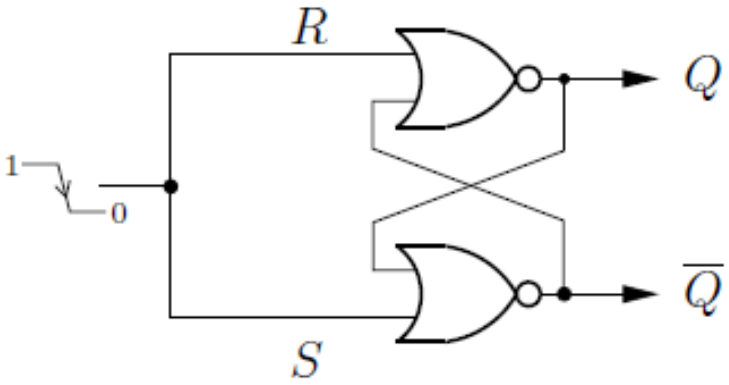
- Principle
- Analysis
- Conclusions

SR-latch as PUF -TRNG



What is the state of Q when S/R goes from 1 to 0 ?

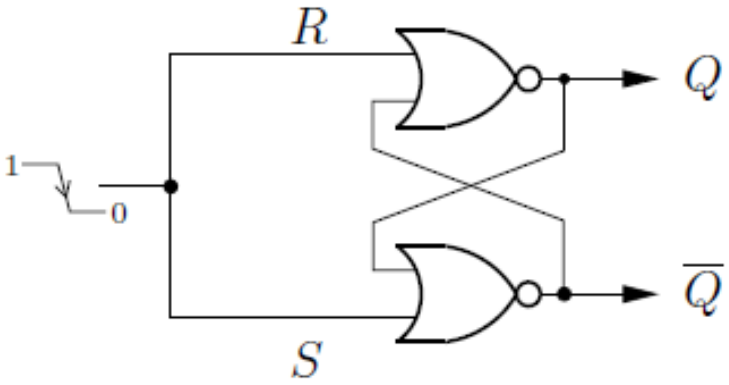
SR-latch as PUF -TRNG



What is the state of Q when S/R goes from 1 to 0 ?

- If Gates perfectly balanced => **metastability** (~Vdd/2Q will converge to a stable state randomly, thanks to the noise) => **TRNG**

SR-latch as PUF -TRNG

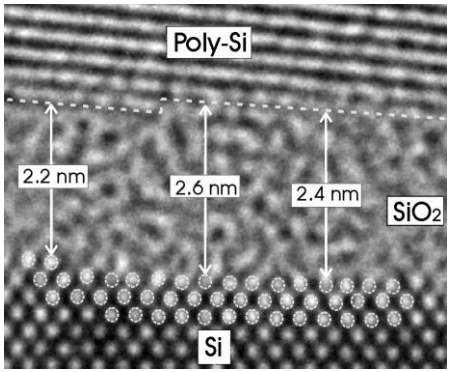


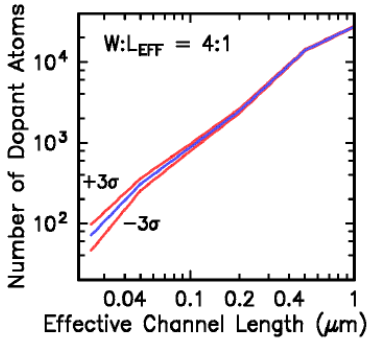
What is the state of Q when S/R goes from 1 to 0 ?

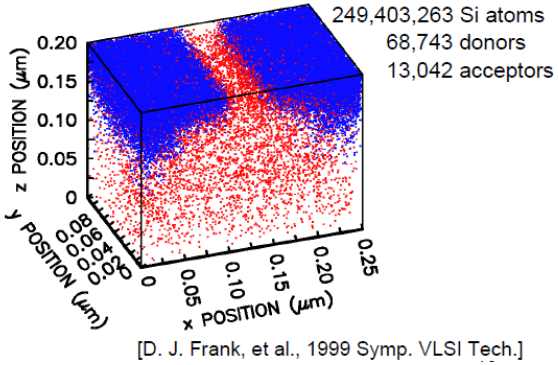
- If Gates perfectly balanced => **metastability** (~Vdd/2Q will converge to a stable state randomly, thanks to the noise)
=> **TRNG**
- If imbalance => goes to the same stable state
=> **PUF** (as SRAM-PUF)

What is the cause of imbalance ?

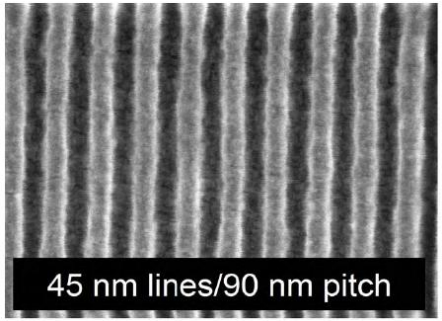
- **CMOS process mismatch**
  - Oxide thickness
  - Metal line edge roughness
  - Random dopant fluctuation





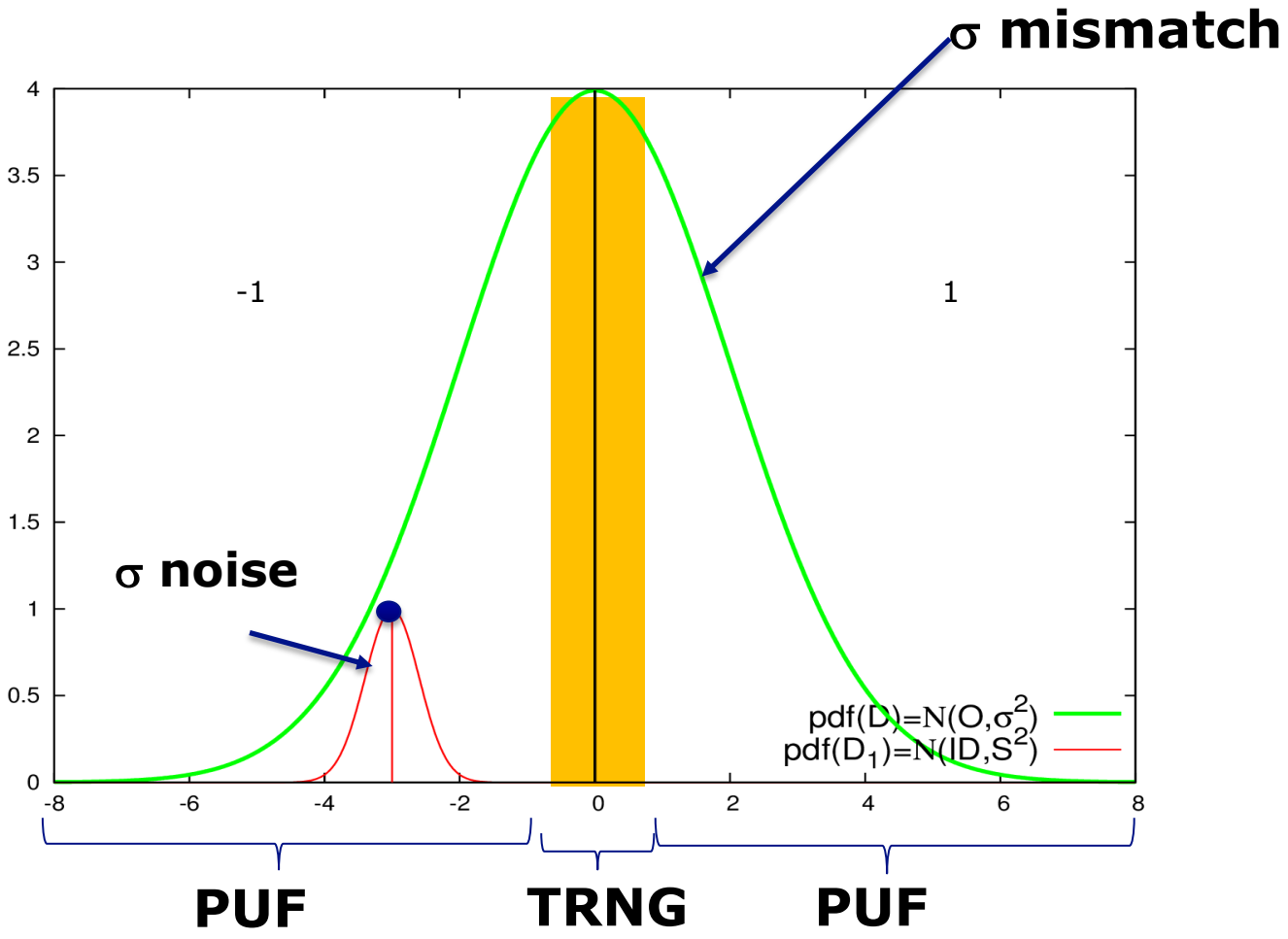


[D. J. Frank, et al., 1999 Symp. VLSI Tech.]

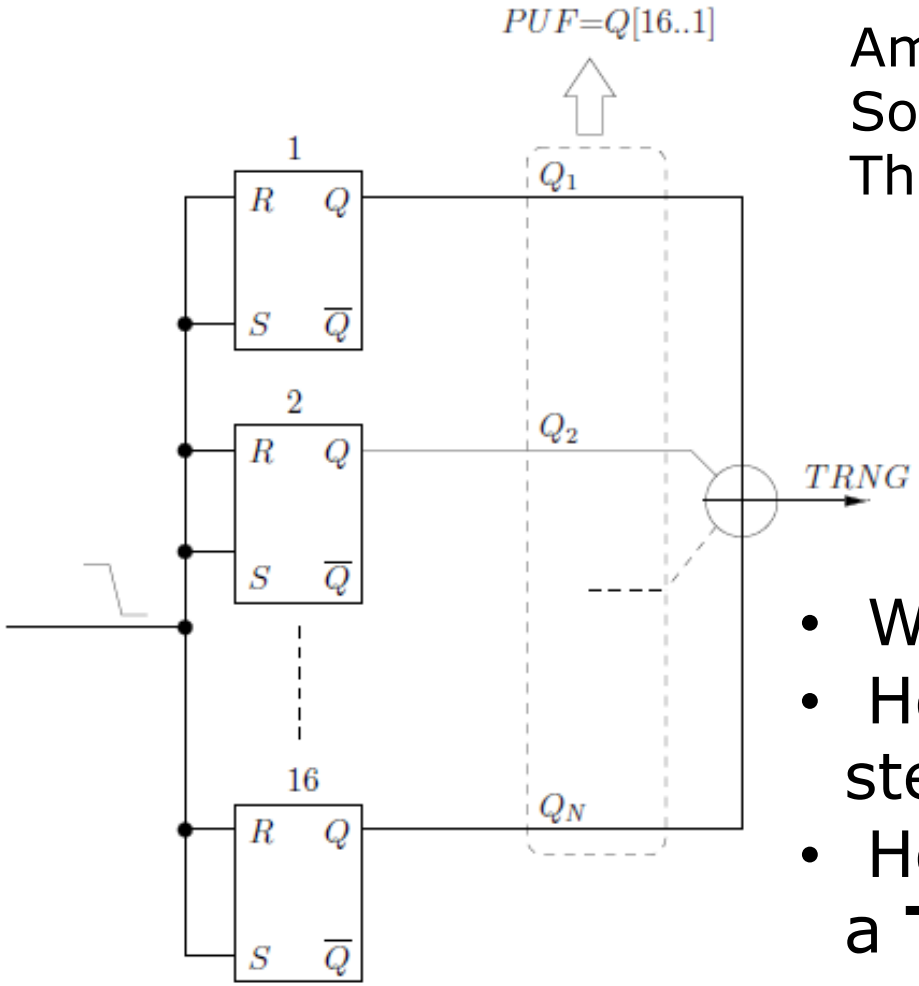


- Can be characterized by a time difference **T_su** for an SR latch
- Has a Gaussian distribution

SR latch as PUF or TRNG according to T_su



Set of SR-latch as PUF -TRNG

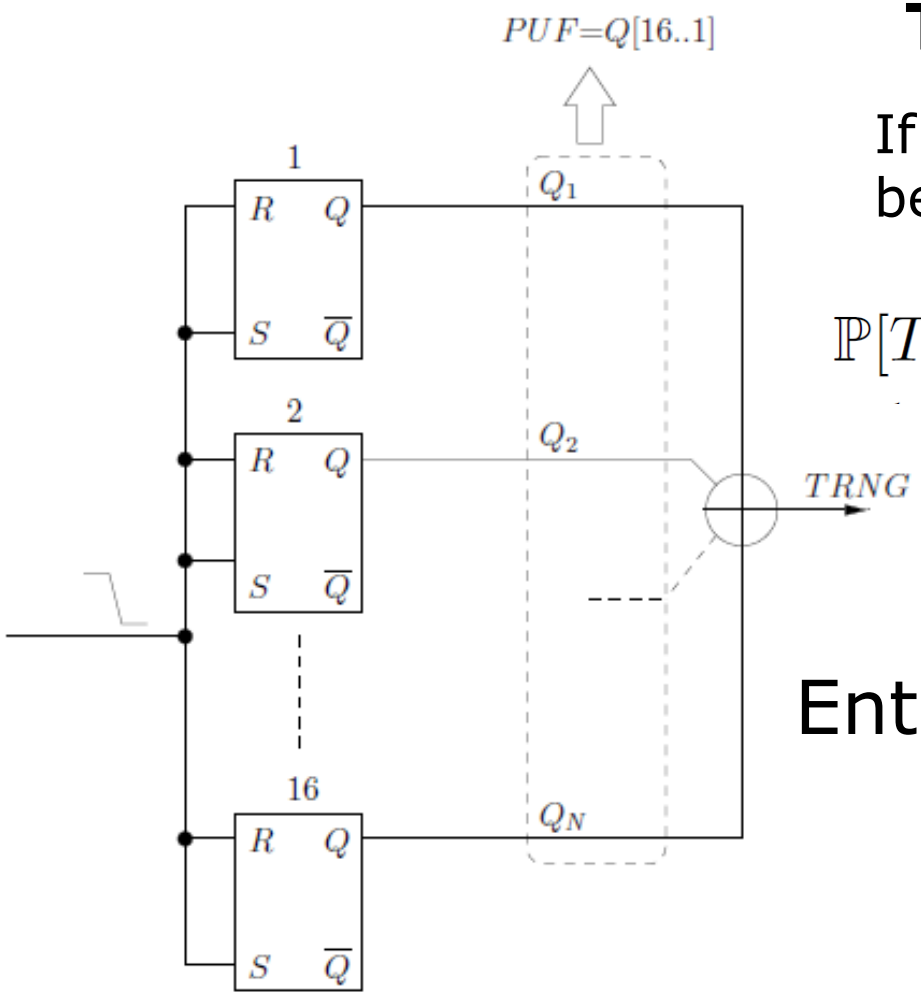


Among the set of N elements ,
Some of them will be used as **PUF**
The others as FAST **TRNG**

Challenges:

- What is the value of N ?
- How many can be used as steady **PUFs** ?
- How many can be used for a **TRNG** with good entropy ?

Set of SR-latch as TRNG



TRNG Requirements :

If noise is independent between latches:

$$\mathbb{P}[TRNG = 0] = \frac{1 + (2p_i - 1)^N}{2}$$

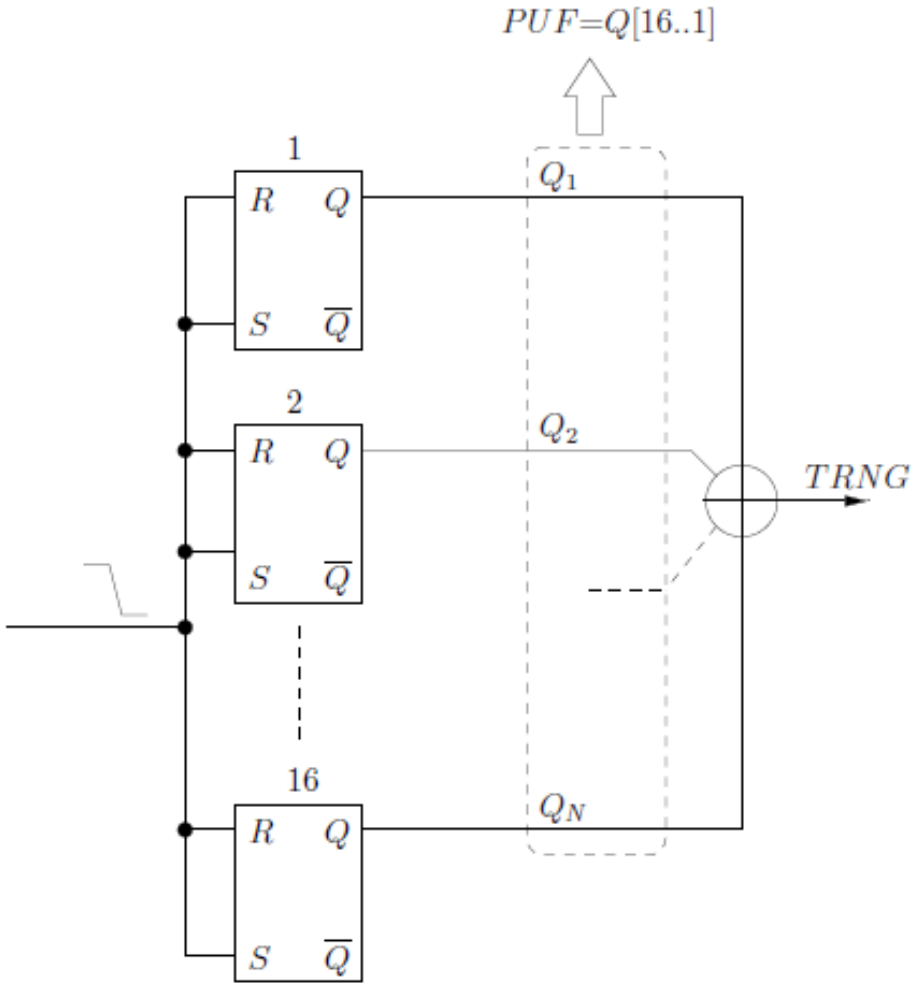
$$\mathbb{P}[Q_i == 1] = p_i$$

Entropy=0.997 ➡ N=12

AIS31

With pi ∈ [0.1,0.9]

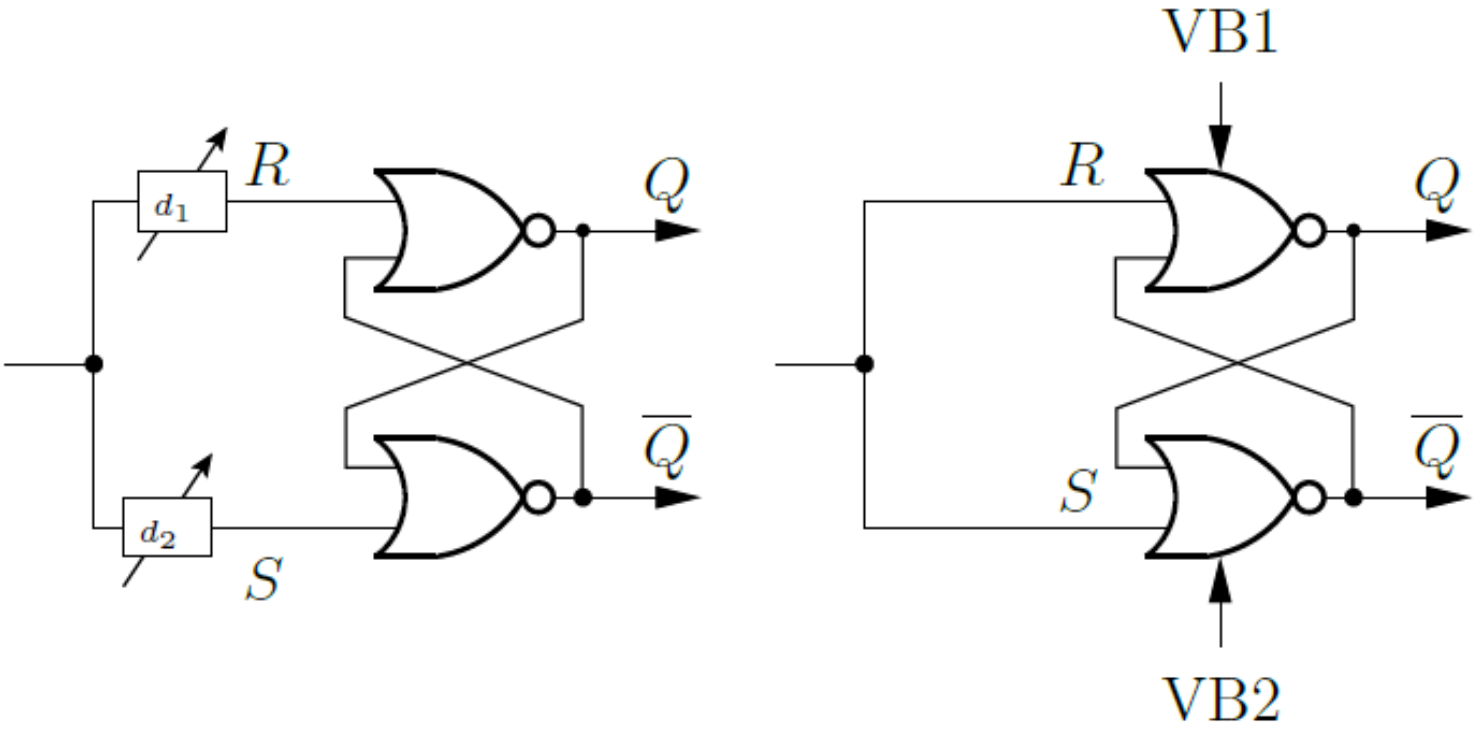
Set of SR-latch as PUF



PUF Requirements :
The Imbalance (T_su) has to be controlled in order to:

- Select the most reliable latches during the enrollment phase
- Obtain as many latches at '0' as '1'

How to analyze/control the SR latch Imbalance ?



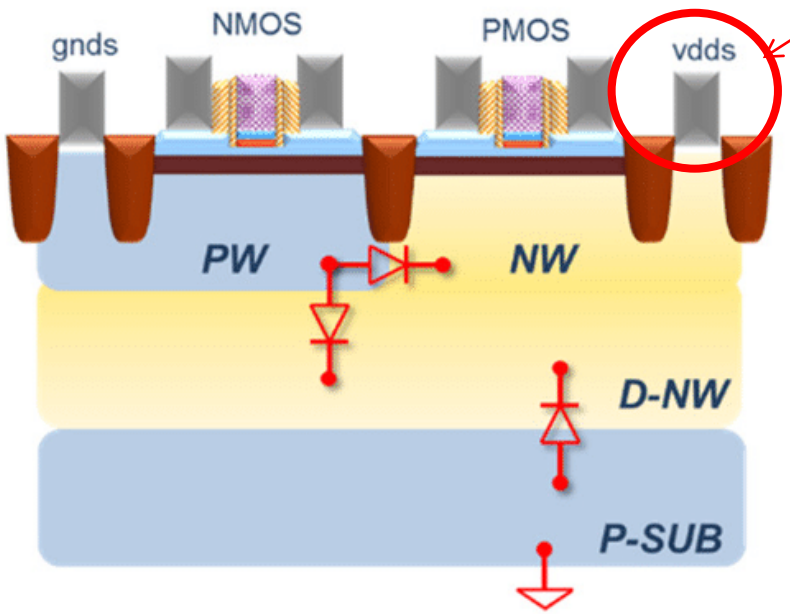
T_su adjustment

Not so easy to design in ASIC

FD-SOI Body biasing

FD-SOI Body bias

$V_{BB} = V_{DD} - V_{DDS}$

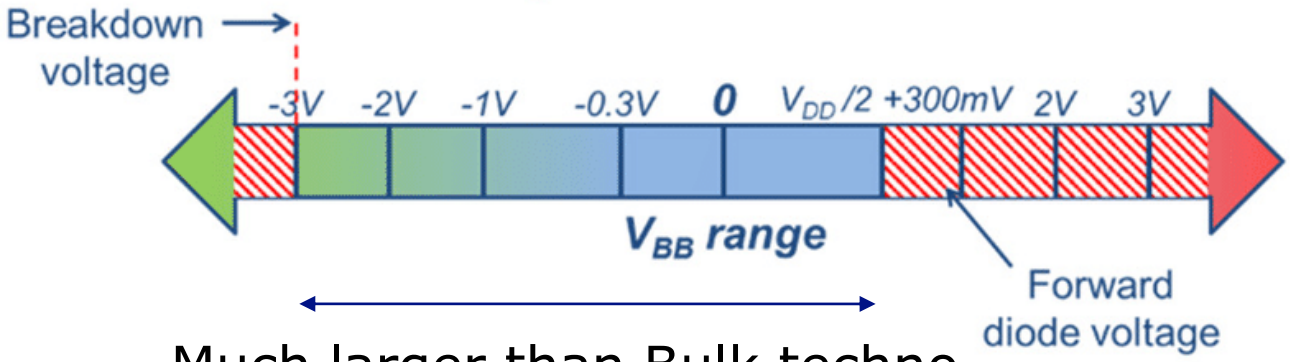


Well voltages

$V_{DDS} = V_{DD} - V_{BB}$
$GNDs = V_{BB}$

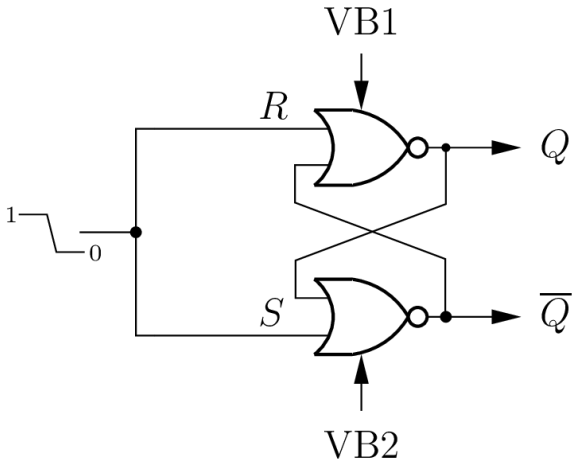
Back-Bias Range

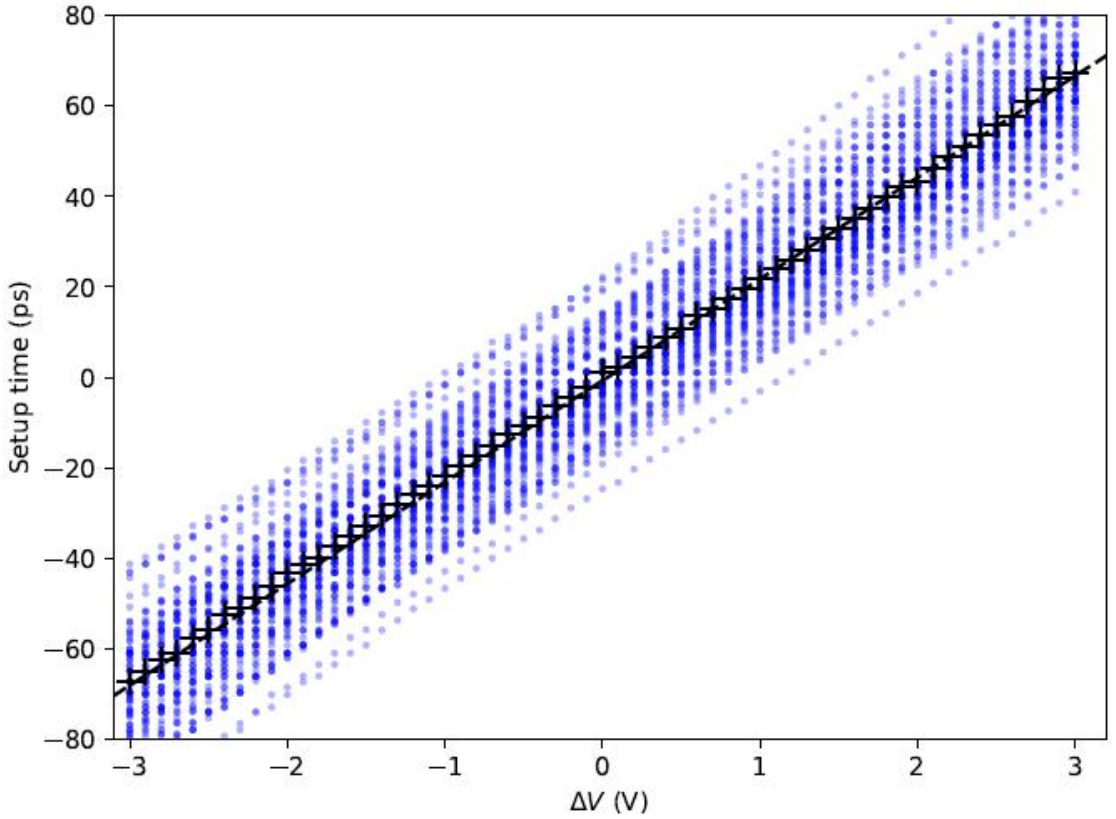
$-3V < V_{BB} < \frac{V_{DD}}{2} + 300mV$



Much larger than Bulk techno

Set-up time T_su vs Body Bias





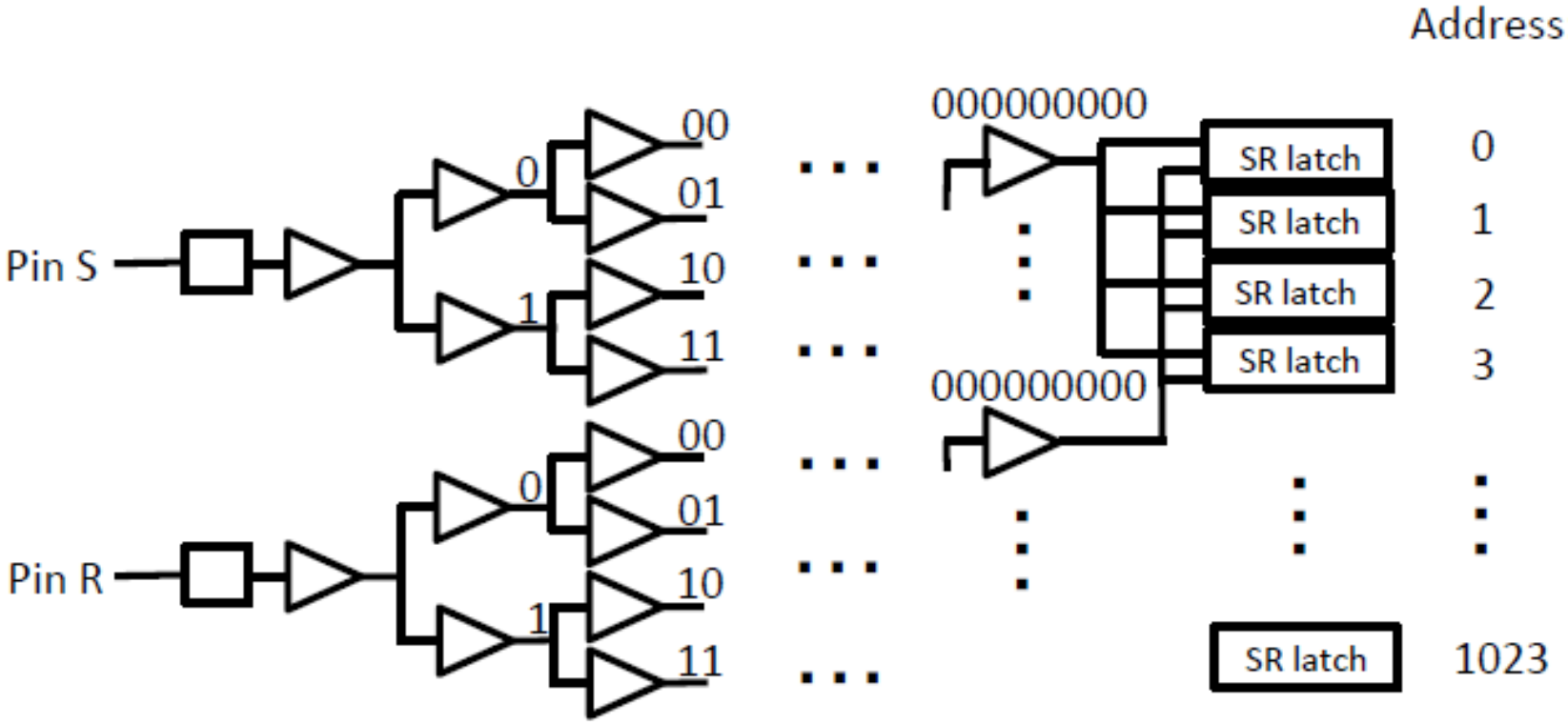
ΔV = VB1- VB2

Outline

- Principle
- Analysis
- Conclusions

Test chip architecture

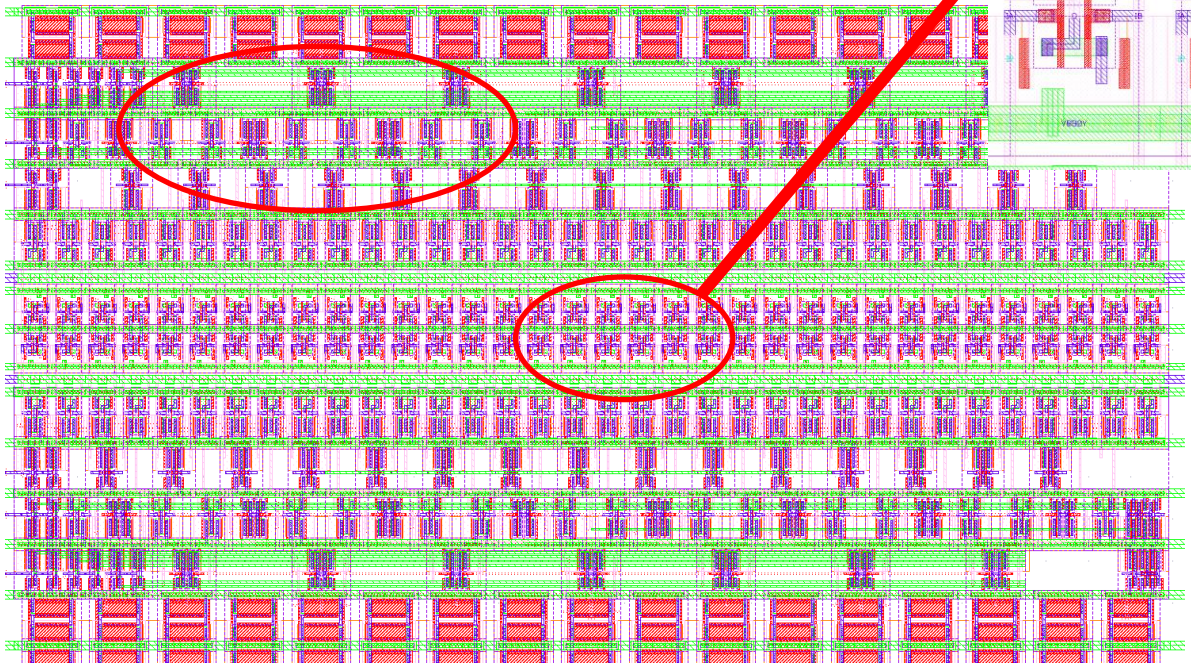
1024 SR latches driven by a buffer tree

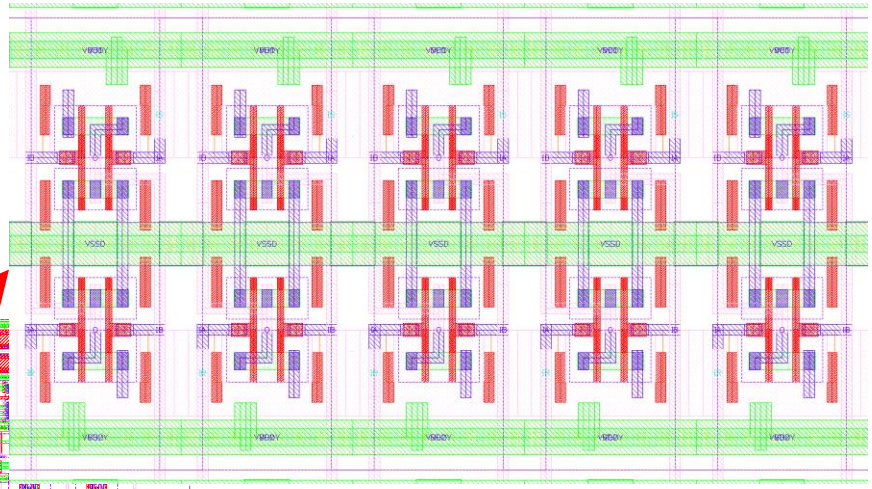


Techno = UTBB FD-SOI 28nm

Layout

buffers



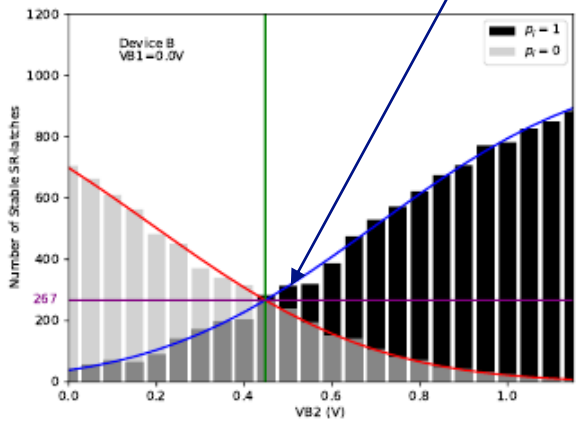


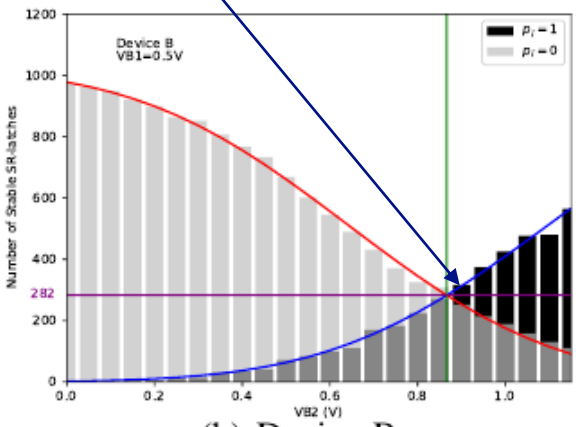
latches

Adjustment by VB1-VB2 for PUF

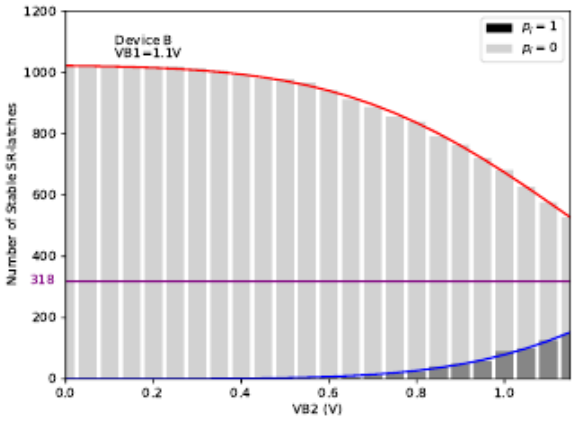
PUF: number of stable latches (pi=0 or 1 after 1000 tries)

Optimal point (as many 0 as 1)





(b) Device B



VB1 = 0V

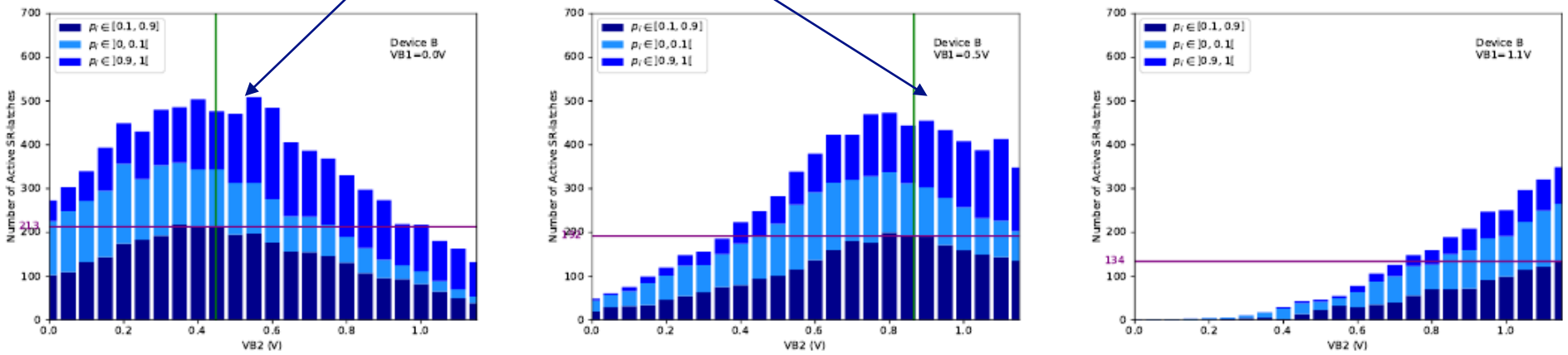
VB1 = 0.5V

VB1 = 1.1V

Adjustment by VB1-VB2 for TRNG

TRNG: number of unstable latches (pi ∈ [0.1,0.9] after 1000 tries)

Optimal point



(b) Device B

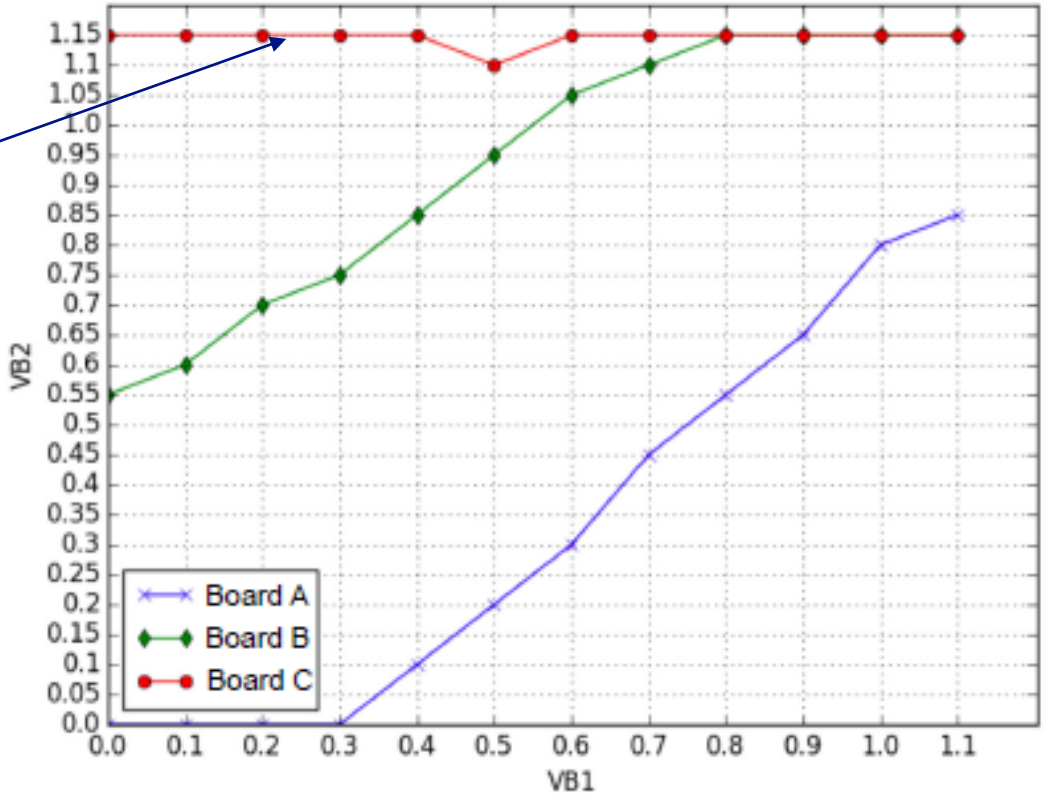
VB1 = 0V VB1 = 0.5V VB1 = 1.1V

The Optimal point is the same for PUF and TRNG !

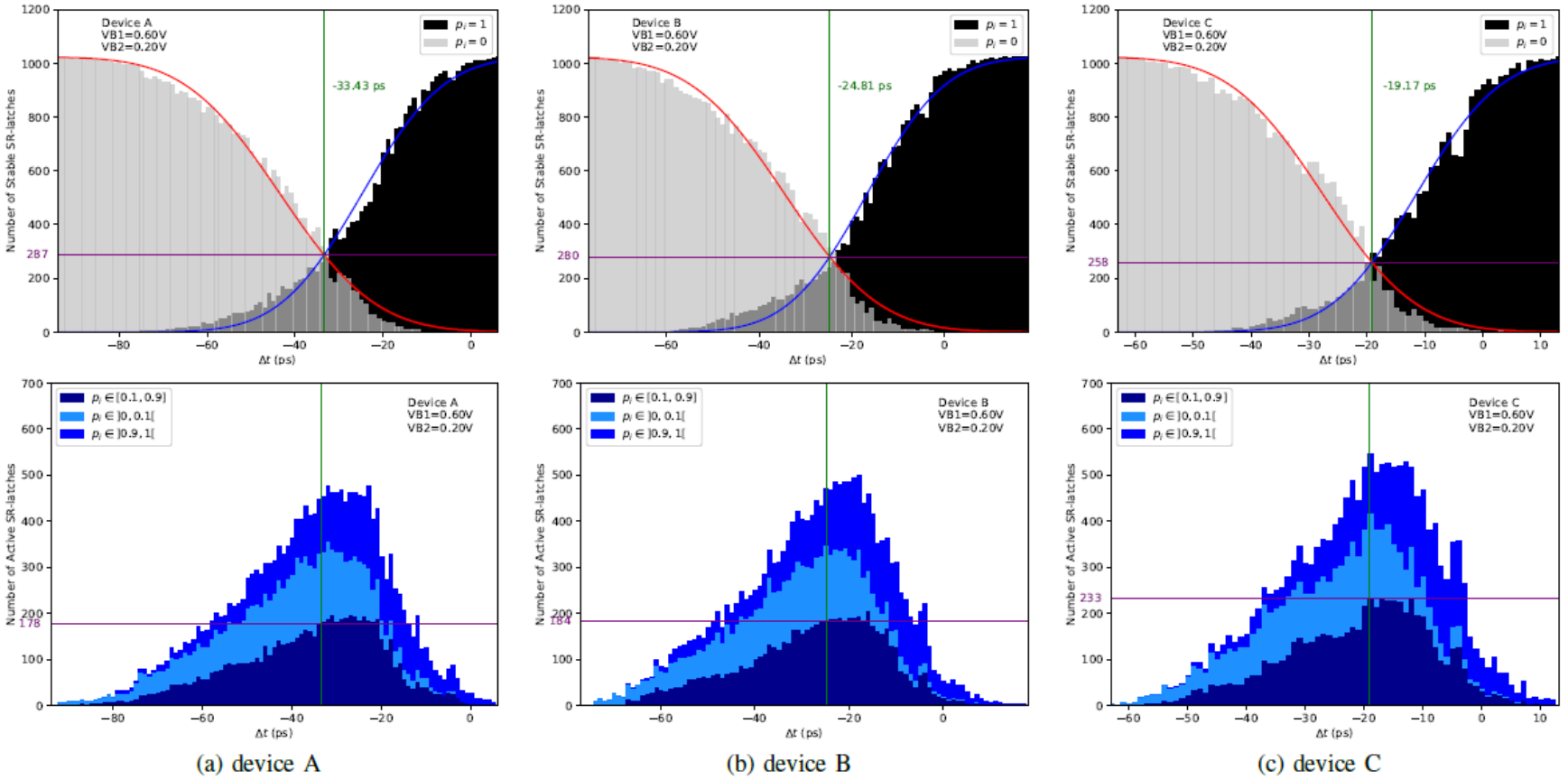
Impact of the process

VB1-VB2 at the optimal point is constant for a given device and is specific to a device

Device C not significant as the VB range is limited due to a bug in the test chip



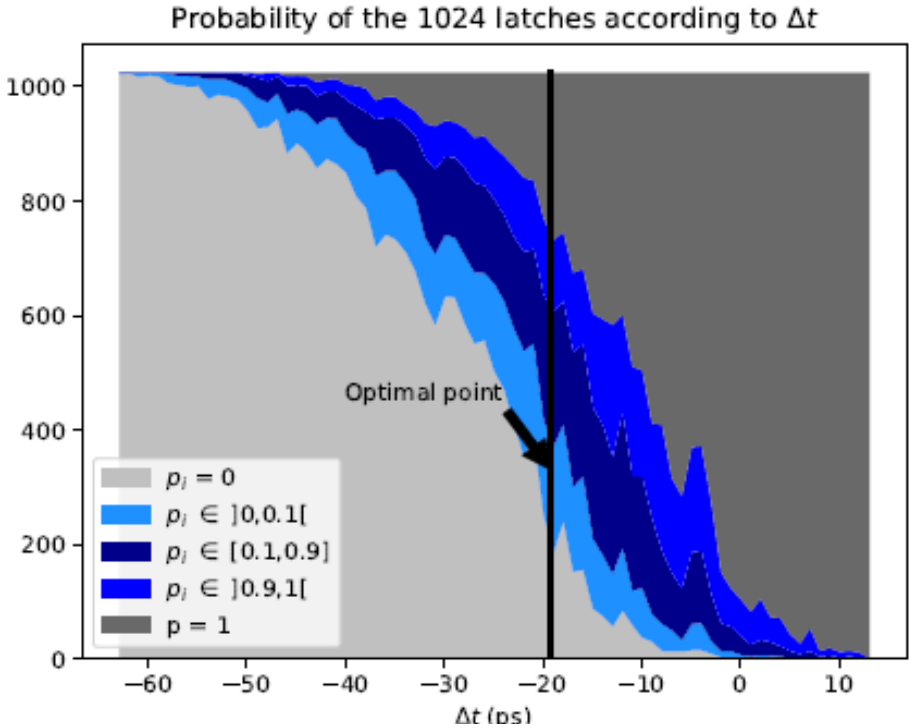
Analysis with the timing generator



(a) device A (b) device B (c) device C

The optimal point is the same for the PUF and TRNG, but different from a device to another

Number of latches in PUF or TRNG at Optimal point



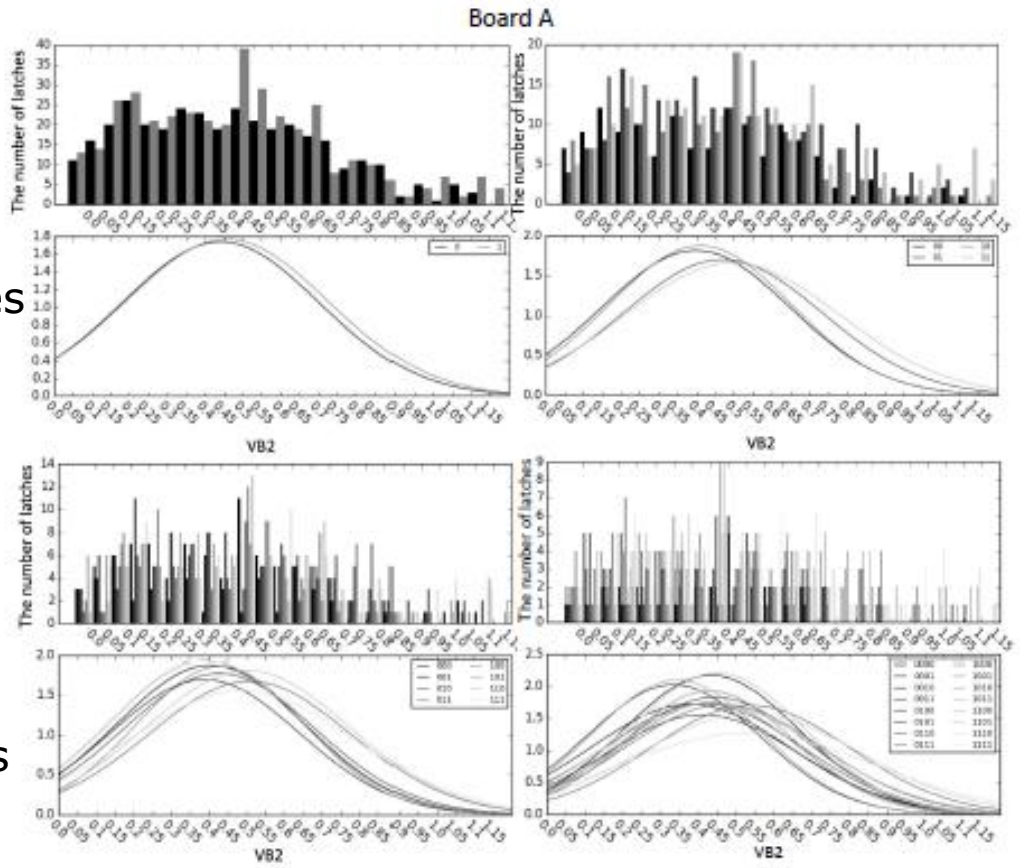
Device	Optimal point	stable latches at 0 or 1	unstable latches with $p_i \in [0.1, 0.9]$
A	-33.43ps	287	178
B	-24.81ps	280	184
C	-19.17ps	258	233

Table I: Number of latches at the optimal point.

Imbalance due to P/R

Number of latches with p_i=0.5

2 main branches



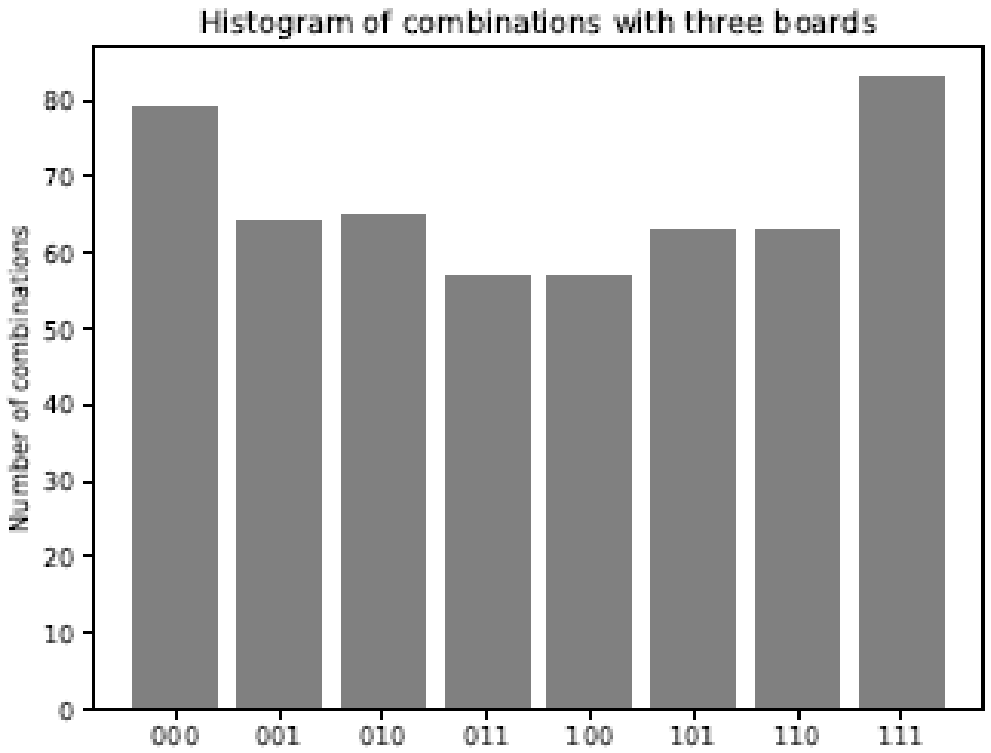
4 sub-branches

8 sub-branches

16 sub-branches

Entropy

Combinations for stable latches between 3 devices



H=2.98 bits instead of 3

Outline

- Principle
- Analysis
- Conclusions

Conclusions

- **Simple structure to get PUF-TRNG**
  - High speed TRNG
  - Reliable PUF as the reliabilty of each latch can be known
- **Every device needs to be adjusted to the optimal point**
  - The optimal point is when as many '0' as '1'
- **FD-SOI technology allows to obtain the optimal point by body biasing**
- **The buffer tree and the number of latches could be largely reduced**

THANK YOU FOR YOUR ATTENTION !