CRYPTARCHI 2018

18-19 June 2018

Mixed PUF-TRNG using Body Biasing in FD-SOI

Jean-Luc DANGER, Télécom ParisTech

In collaboration with:

Risa Yashiro, Kazuo Sakiyama (UEC)

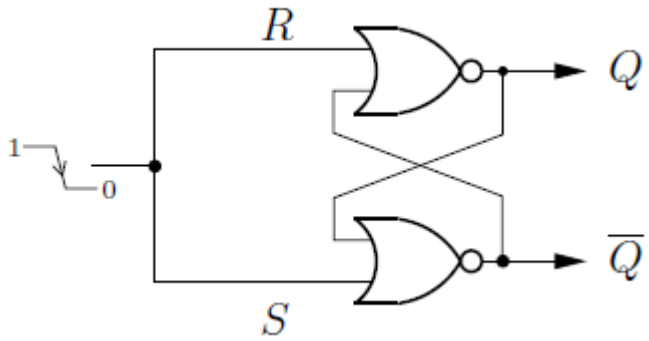
Noriyuki Miura, Makoto Nagata (Kobe University)

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

Outline

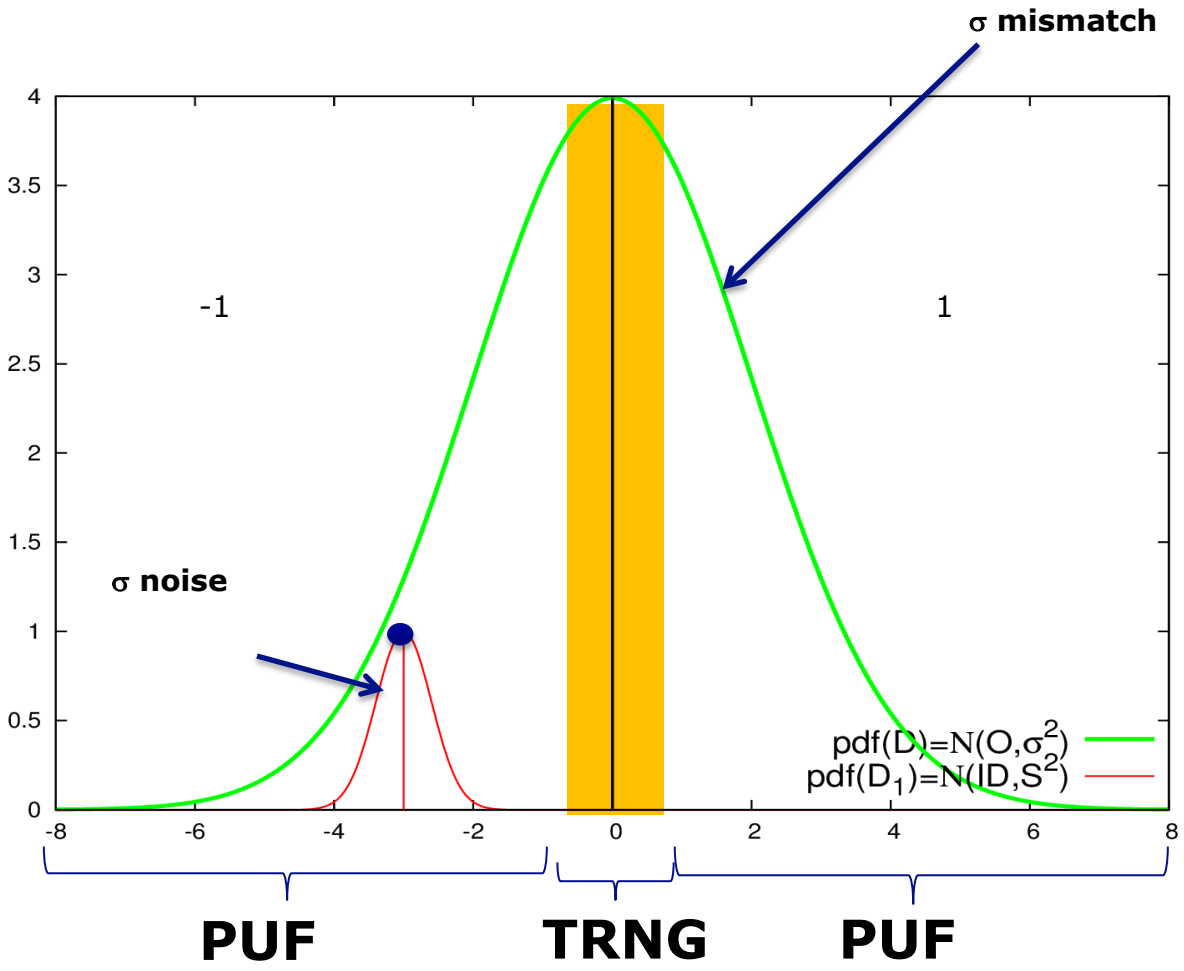
- Principle
- Analysis
- Conclusions

SR-latch as PUF -TRNG

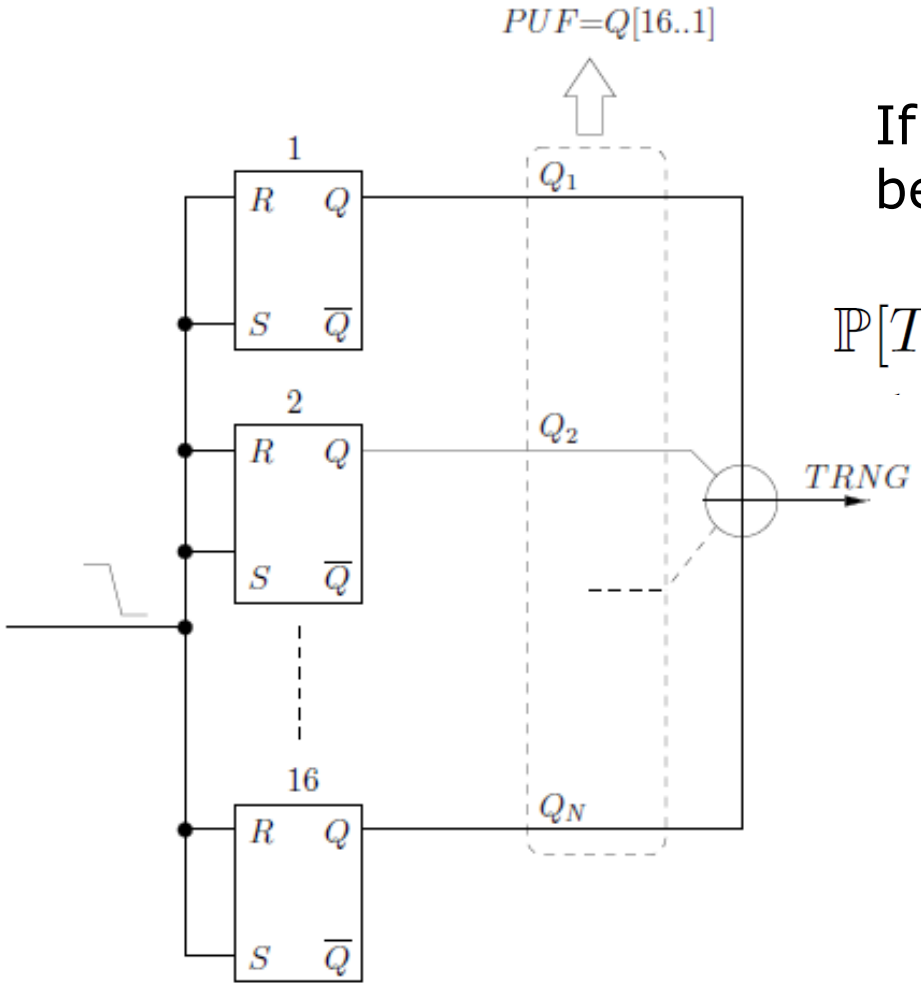


Small imbalance => metastability => **TRNG**
Big imbalance => stability => **PUF**

PUF-TRNG according to T-su distribution



SR-latch as PUF -TRNG



If noise is independent between latches:

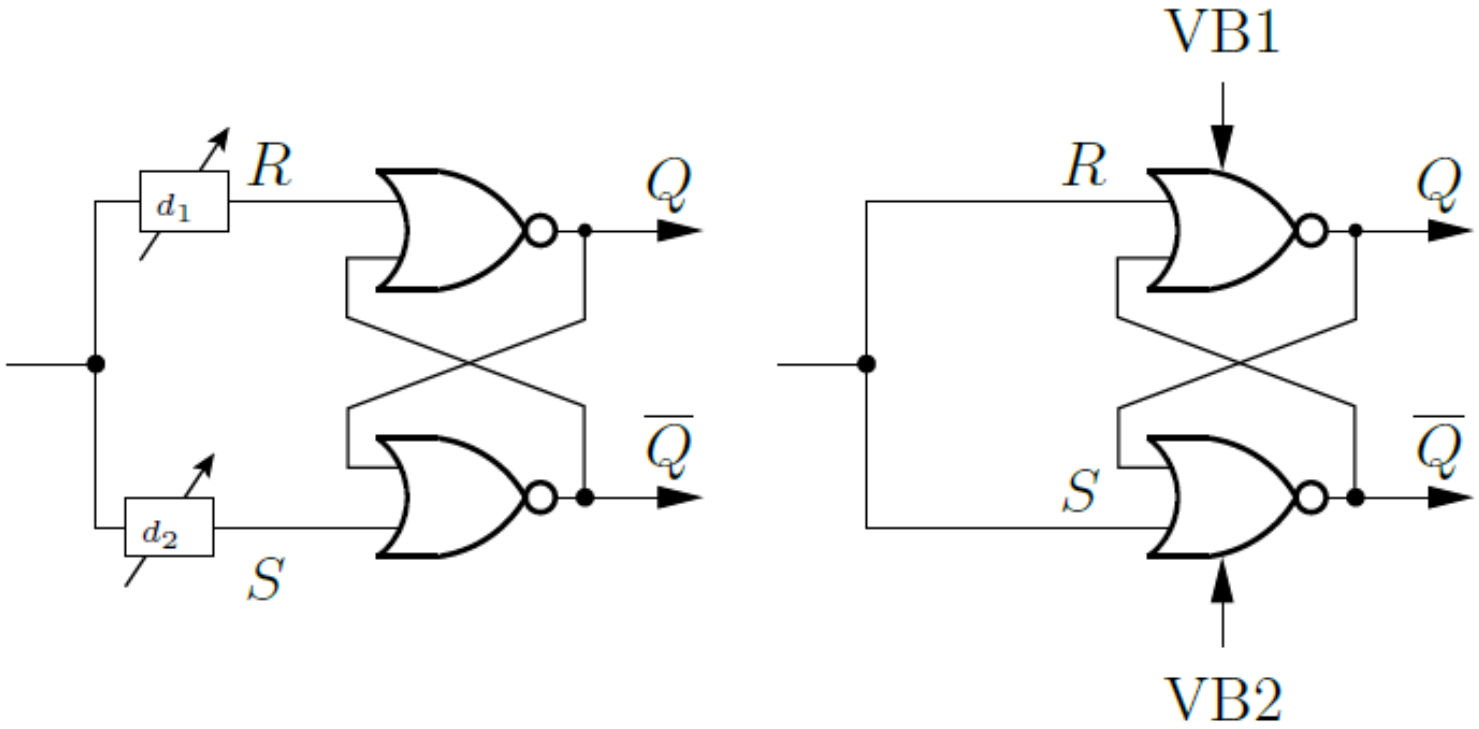
$$\mathbb{P}[TRNG = 0] = \frac{1 + (2p_i - 1)^N}{2}$$

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

Entropy=0.997 ➡ N=12

AIS31

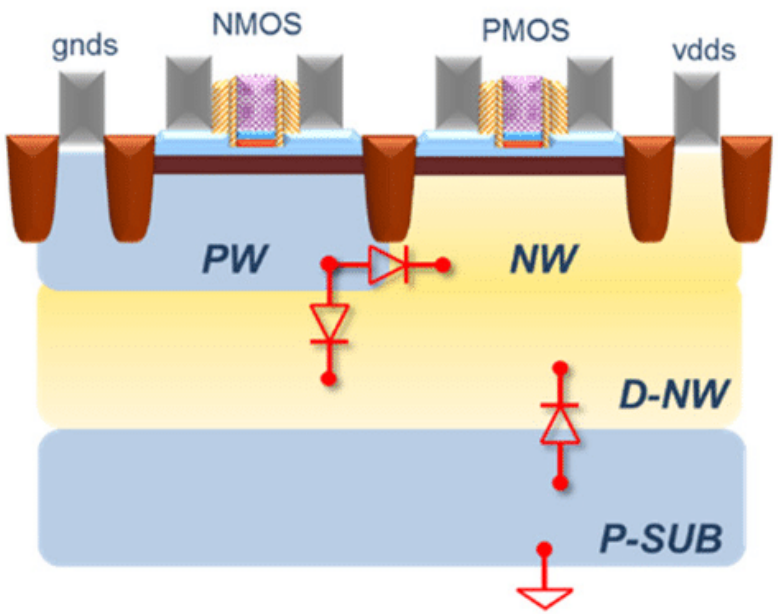
SR-latch T_su adjustment in FD-SOI



Delay adjustment
Not so easy to design in ASIC

→ FD-SOI Body biasing

FD-SOI Body bias



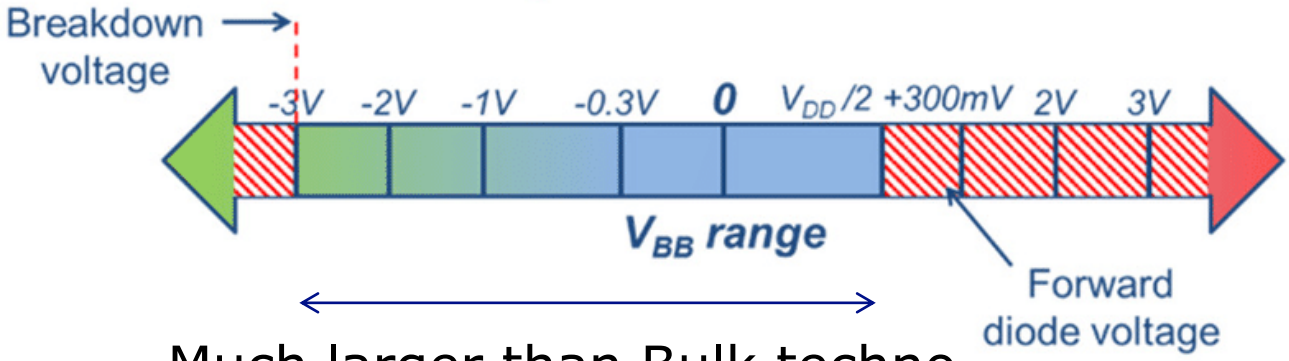
Well voltages

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

$GNDs = V_{BB}$

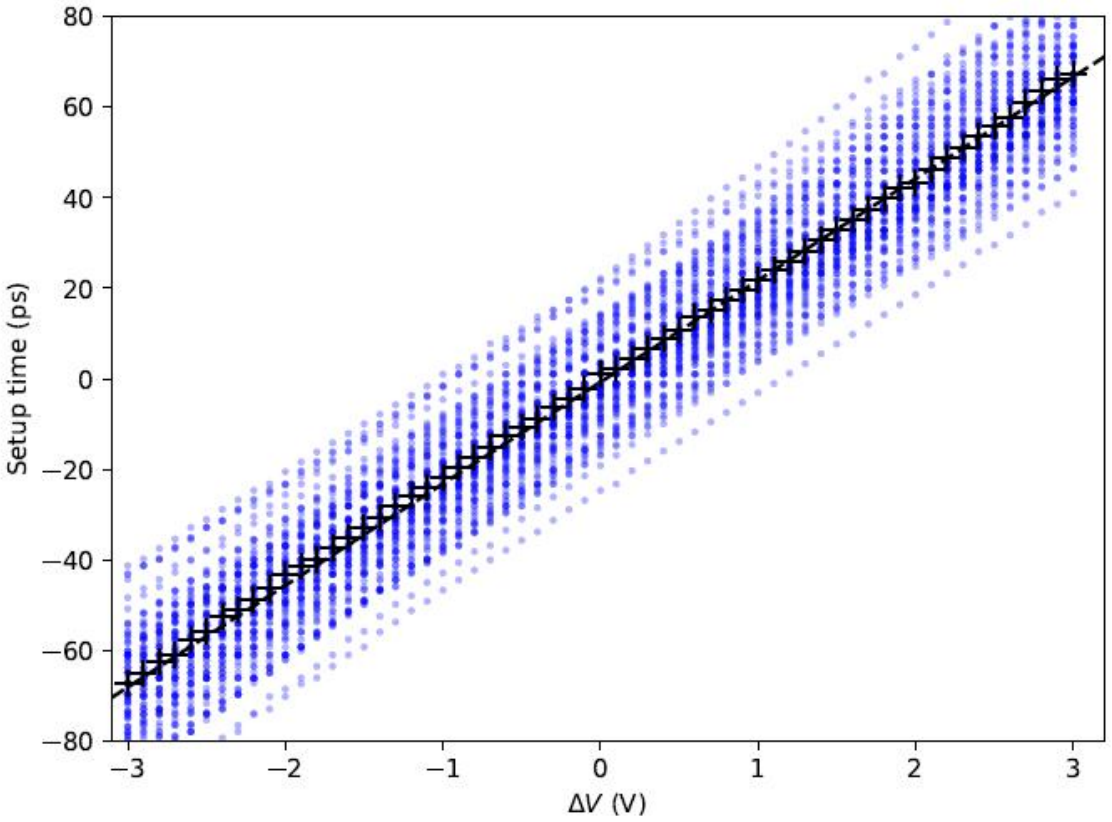
Back-Bias Range

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



Much larger than Bulk techno

Set-up time vs Body Bias



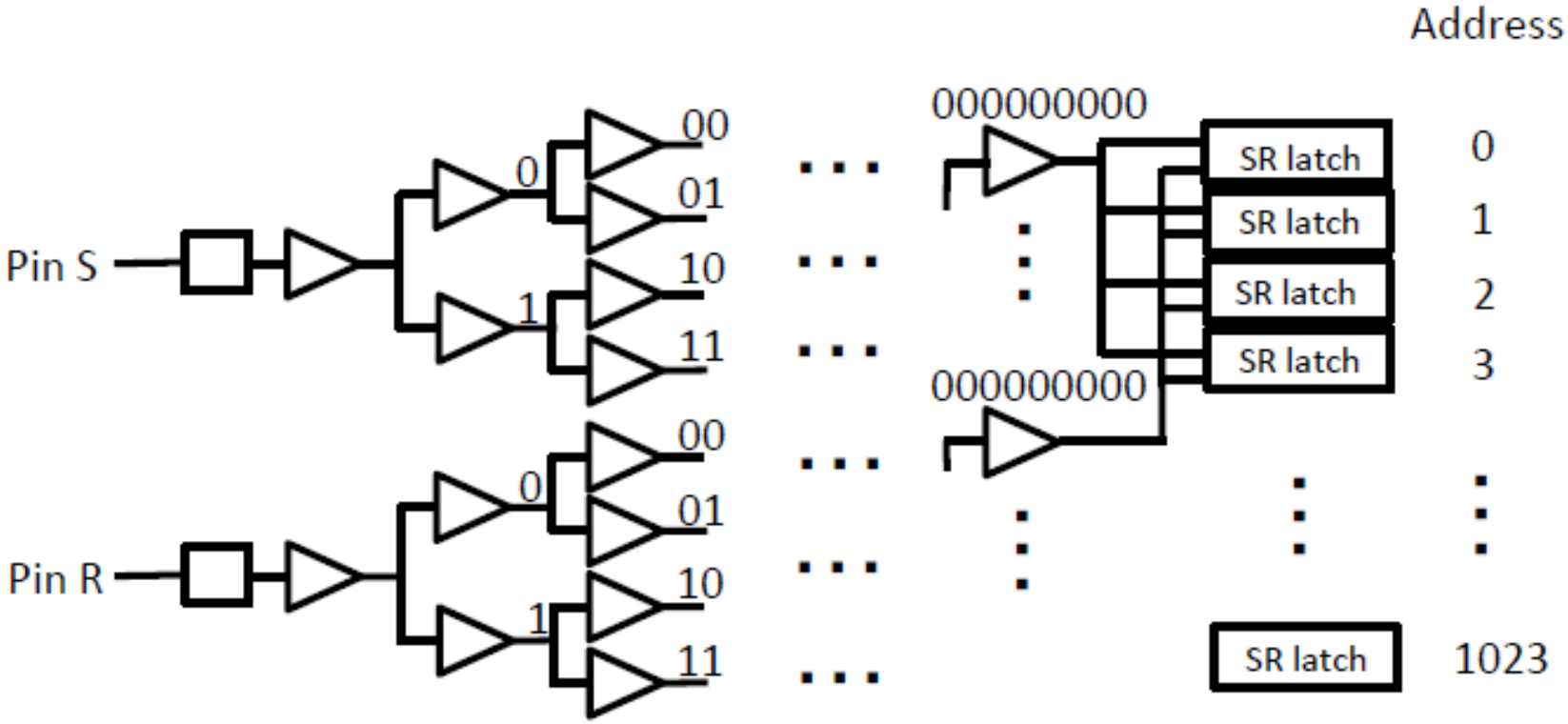
$\Delta V = VB1 - VB2$

Outline

- Principle
- Analysis
- Conclusions

Test chip architecture

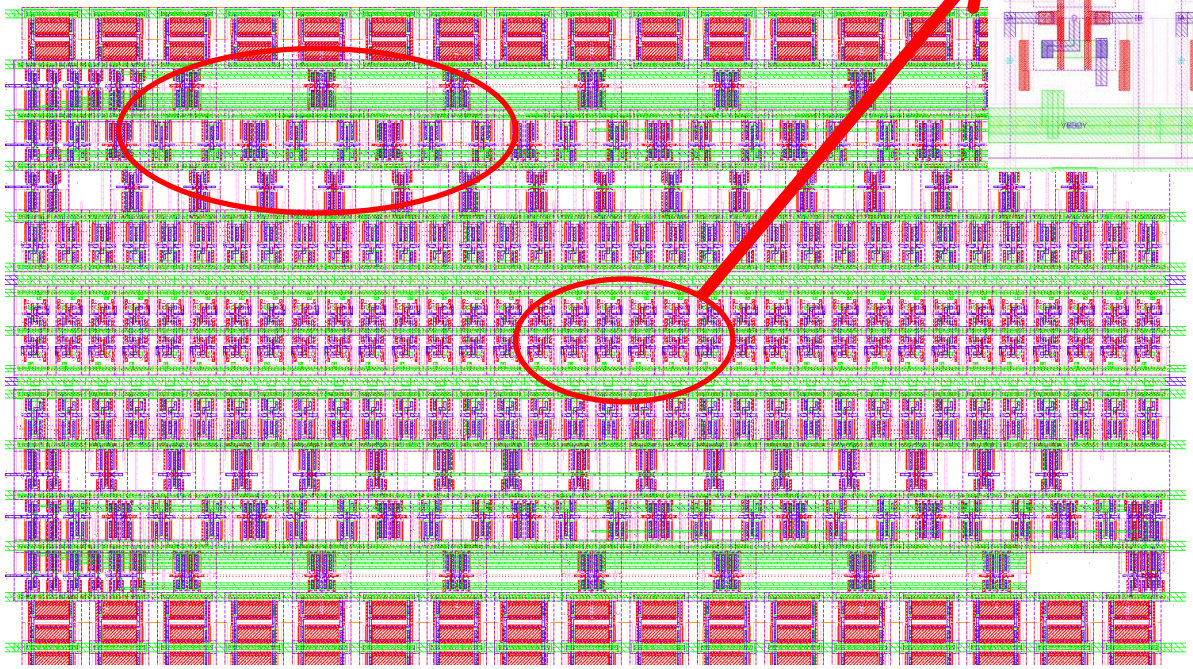
1024 latches driven by a buffer tree

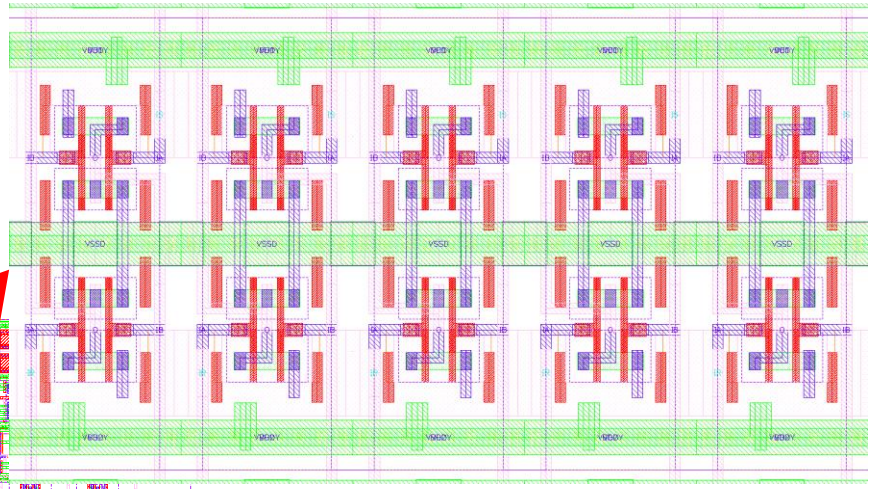


Techno = UTBB FD-SOI 28nm

Layout

buffers



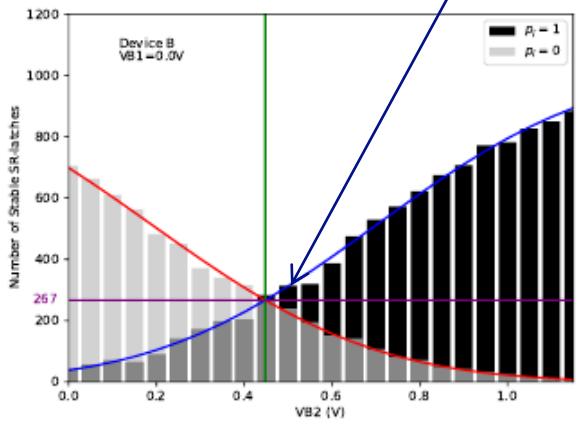


latches

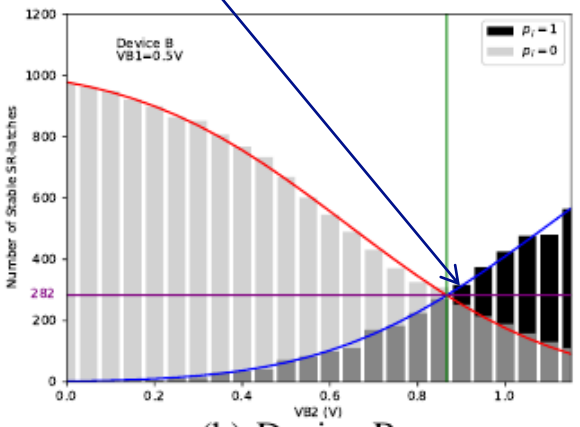
Adjustment by VB1-VB2 for PUF

PUF: number of stable latches (after 1000 tries)

Optimal point (max entropy)

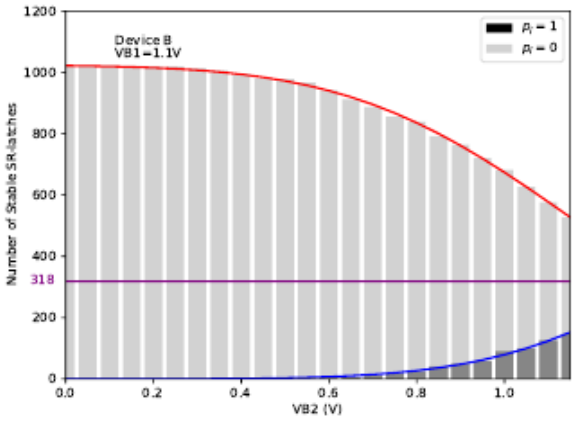


VB1 = 0V



(b) Device B

VB1 = 0.5V

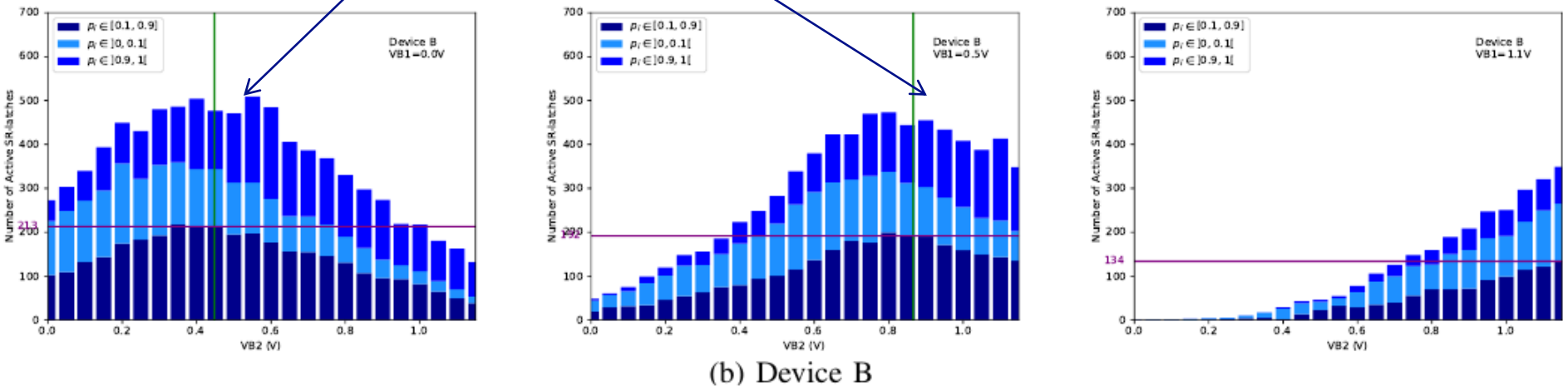


VB1 = 1.1V

Adjustment by VB1-VB2 for TRNG

TRNG: number of unstable latches

Optimal point



(b) Device B

VB1 = 0V

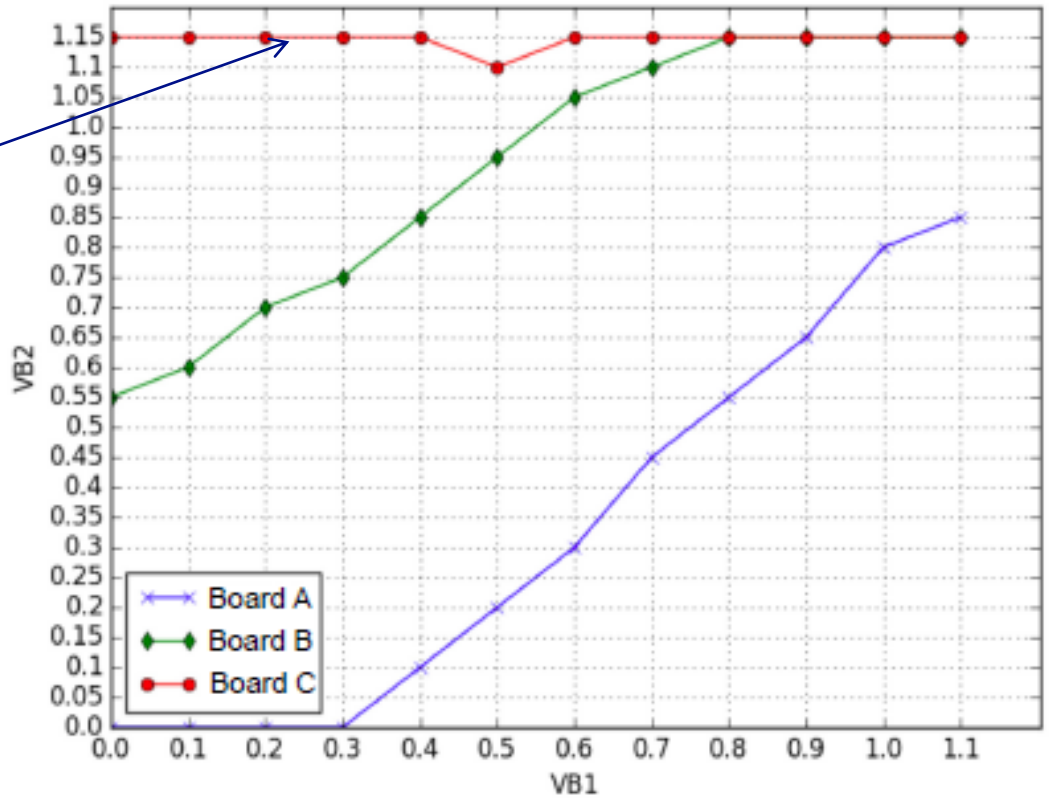
VB1 = 0.5V

VB1 = 1.1V

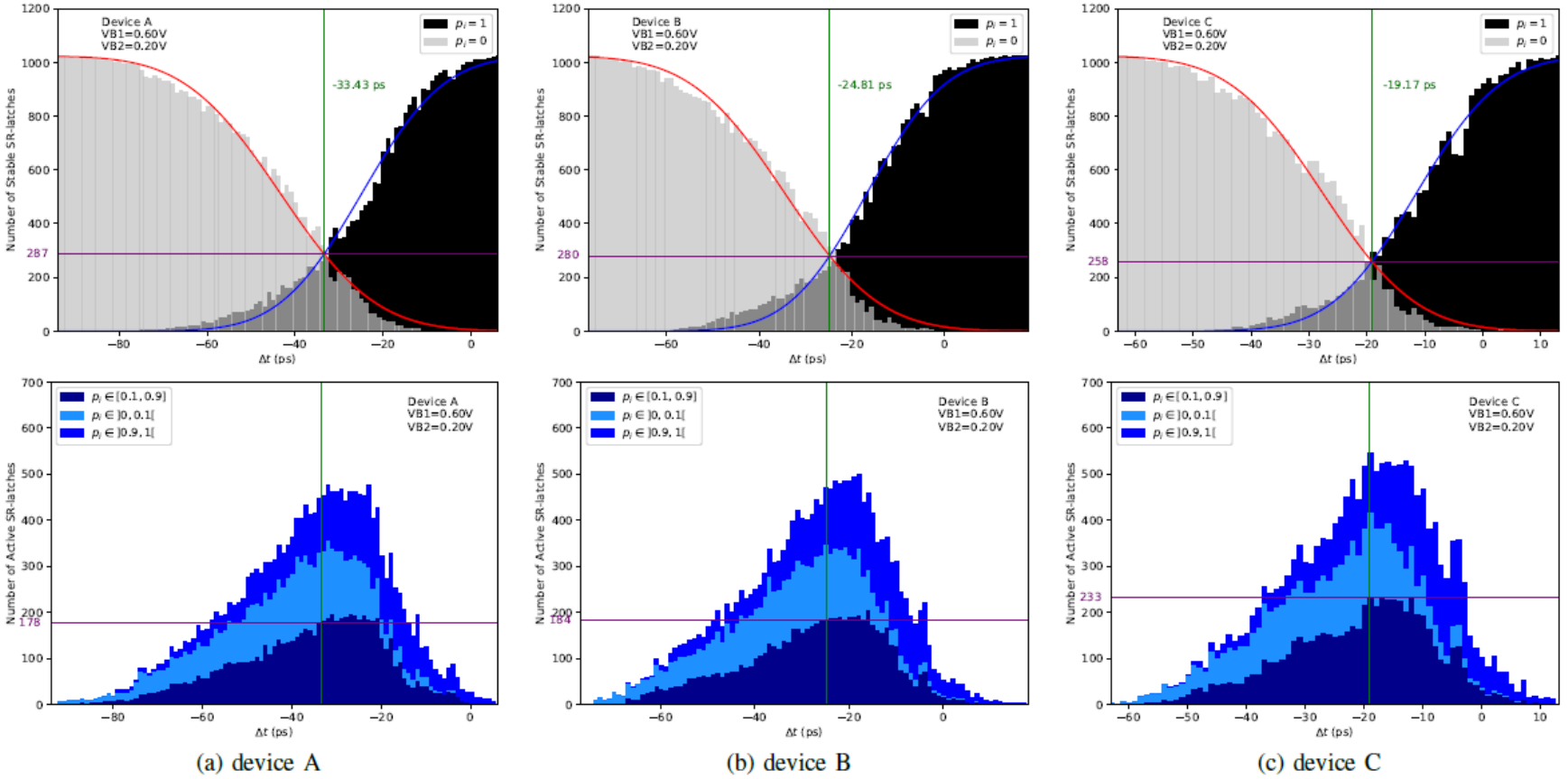
Optimal point: the same for PUF and TRNG !

VB1-VB2 at the optimal point is specific to a device

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



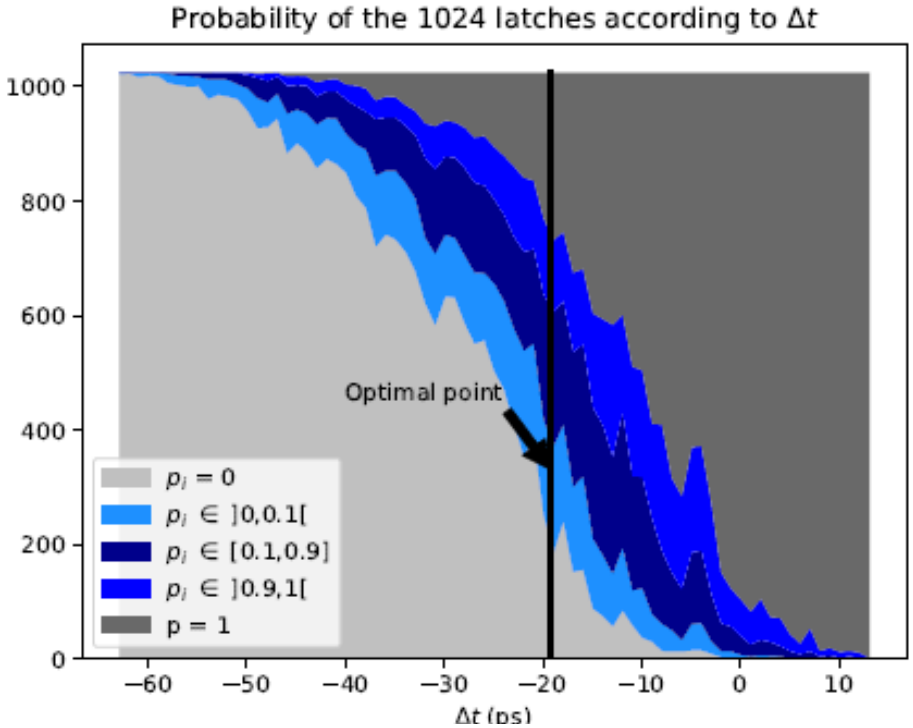
Analysis with the timing generator



(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



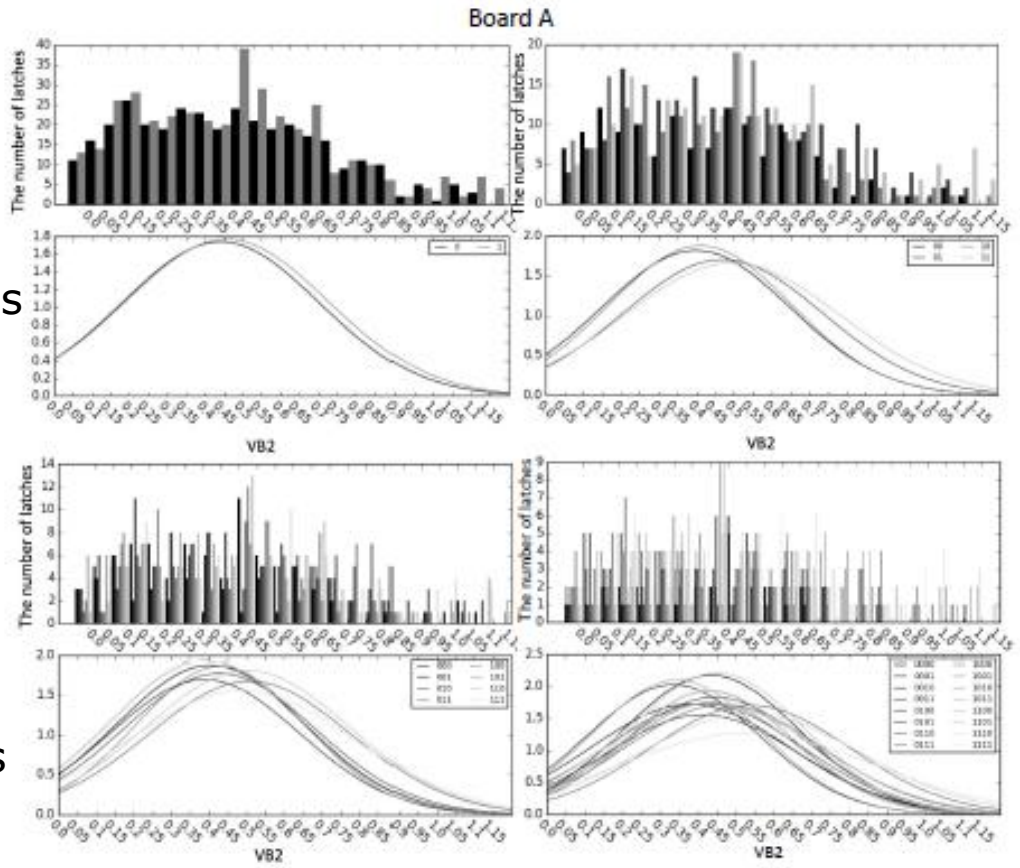
Device	Optimal point	stable latches at 0 or 1	unstable latches with $p_i \in [0.1, 0.9]$
A	-33.43ps	287	178
B	-24.81ps	280	184
C	-19.17ps	258	233

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



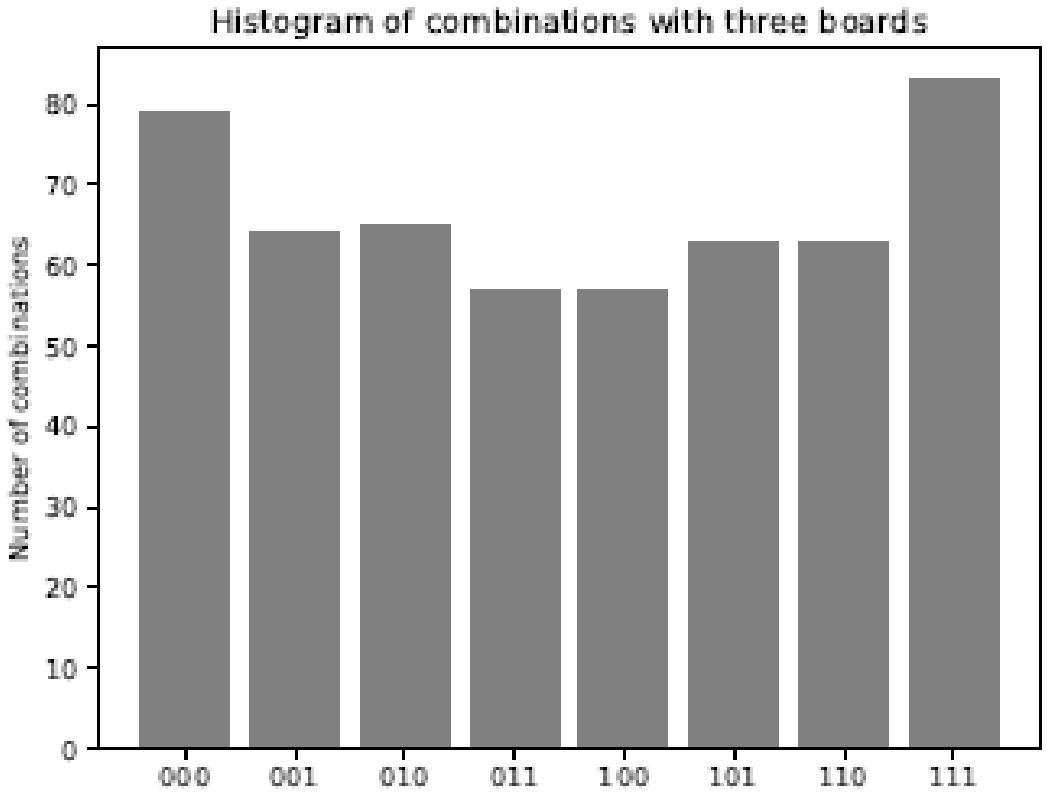
4 sub-branches

8 sub-branches

16 sub-branches

Entropy

Combinations for stable latches between 3 devices



H=2.98 bits

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 !