A Reliable Low-area Low-power PUF-based Key Generator

Dr. Raimondo Luzzi, Infineon Technologies AG

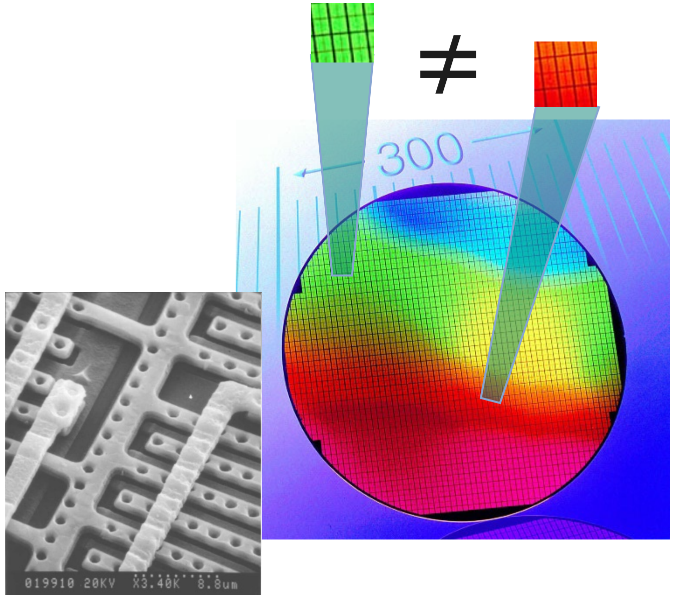
ECW, November 18-21, 2024, Rennes

Agenda

- Two-Stage ID (TSID) PUF cell vs. standard latch
- Pre-selection technique
- 128-bit key generator implementation
- Experimental results in 65nm
- Conclusions

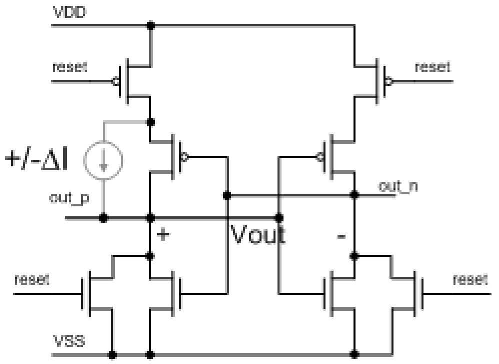
Physically unclonable functions as “fingerprints” of objects

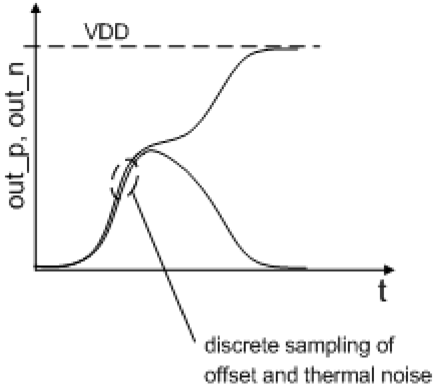
- extracting small variations which make each micro electronic device unique
- variations beyond manufacturer’s control
- generating an ID code on the fly
- secure against probing (at least before digitalization…)
- in high sec applications: additional security feature, not replacing NVM stored keys



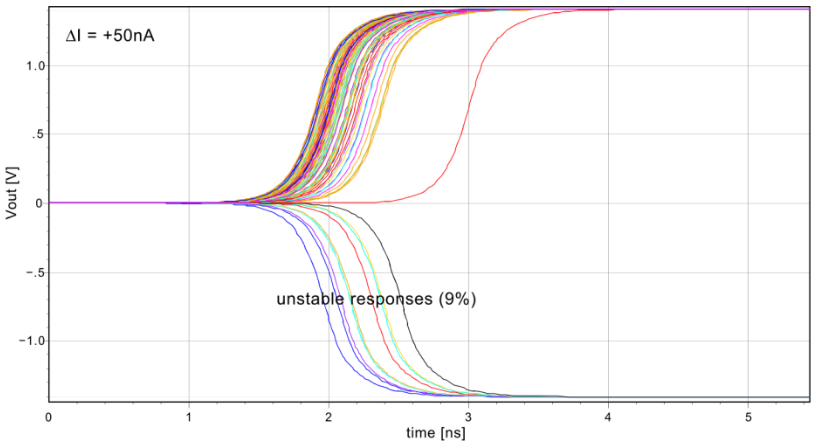
Latch vs. Two-stage ID (TSID) cell

- Latch

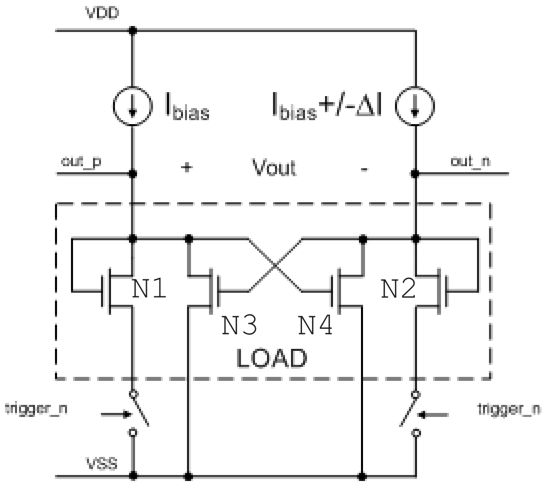


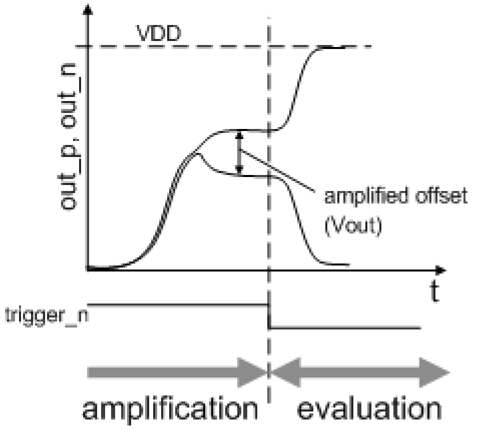


transient noise simulation (100 runs)

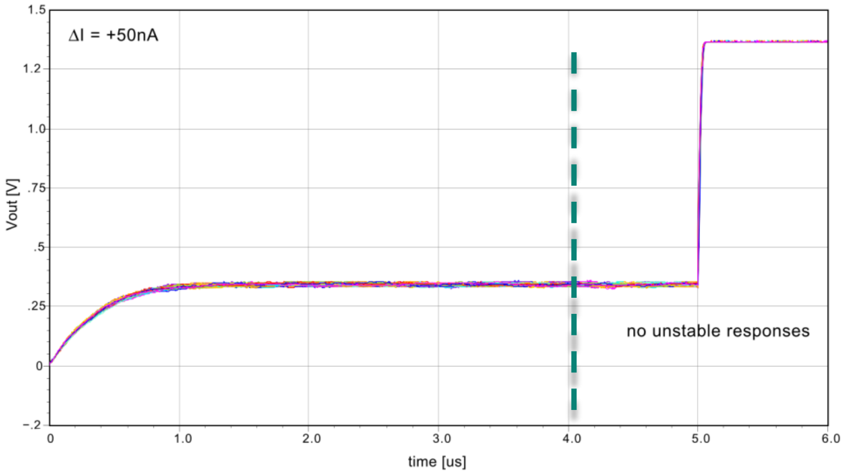


- Two-Stage ID cell



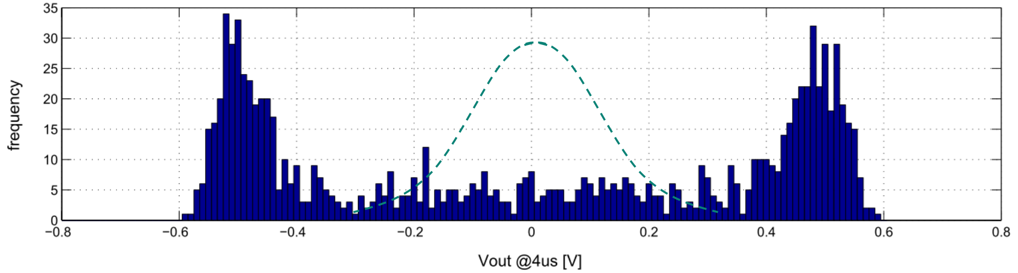


transient noise simulation (100 runs)

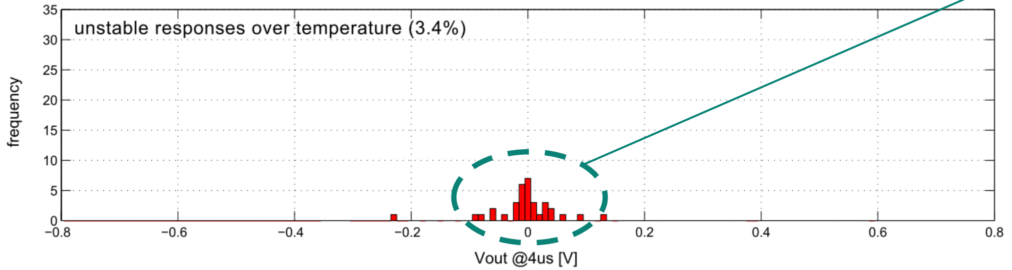


Temperature instability

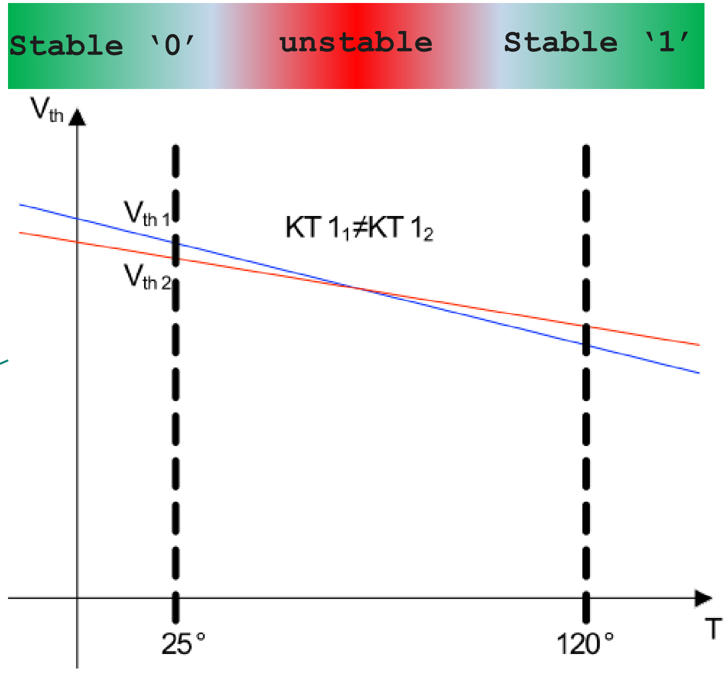
Monte Carlo simulation (1000 runs) @25°C



Monte Carlo simulation (1000 runs) @-40°C/+120°C



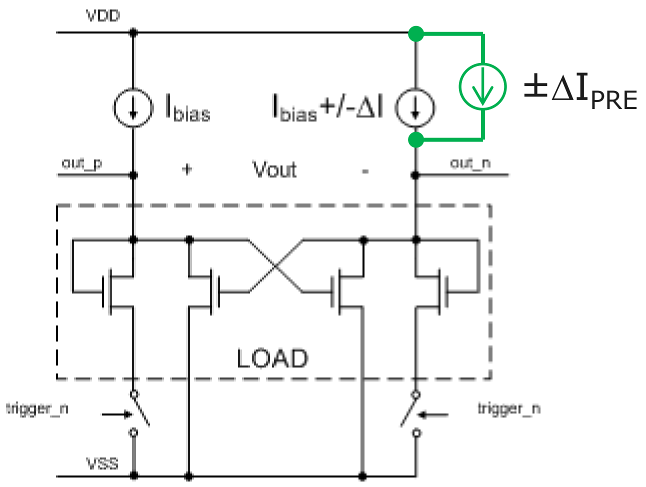
Distribution of unstable cells: V_{out}@-40°C ≠ V_{out}@120°C

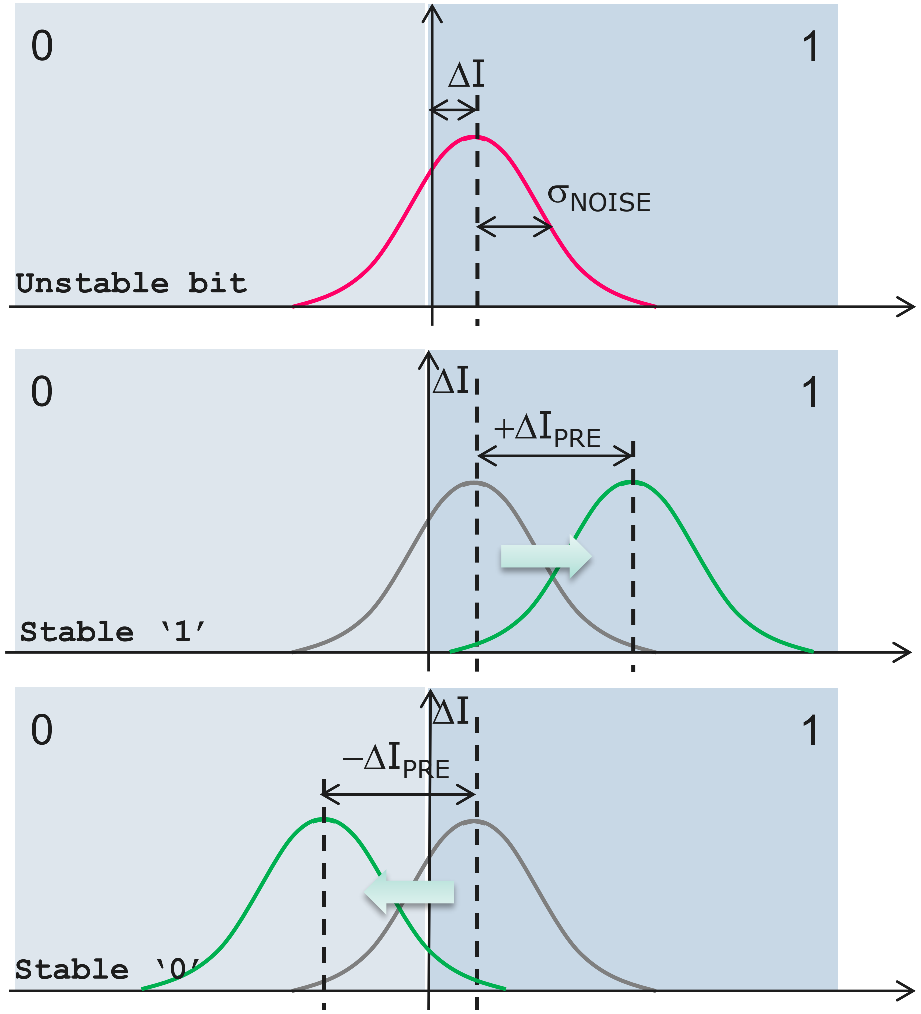


- Due to the mismatch of the V_{th} temperature coefficient KT1, the output may change its value → ca. **3.4%** unstable bits in simulation

Pre-selection [Hofer et al. CHES 2010]

- Idea: select those cells that provide a reasonable degree of mismatch

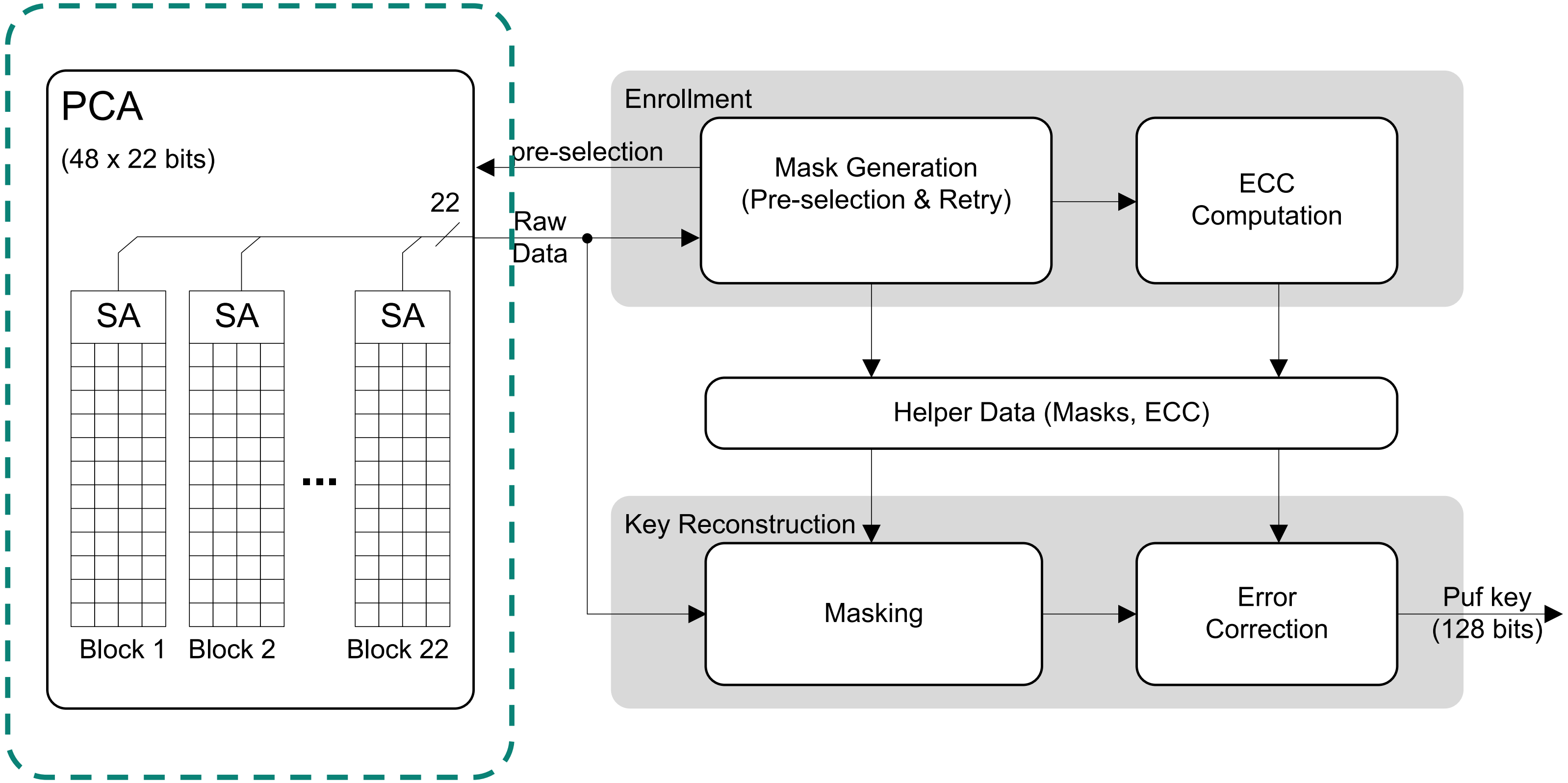




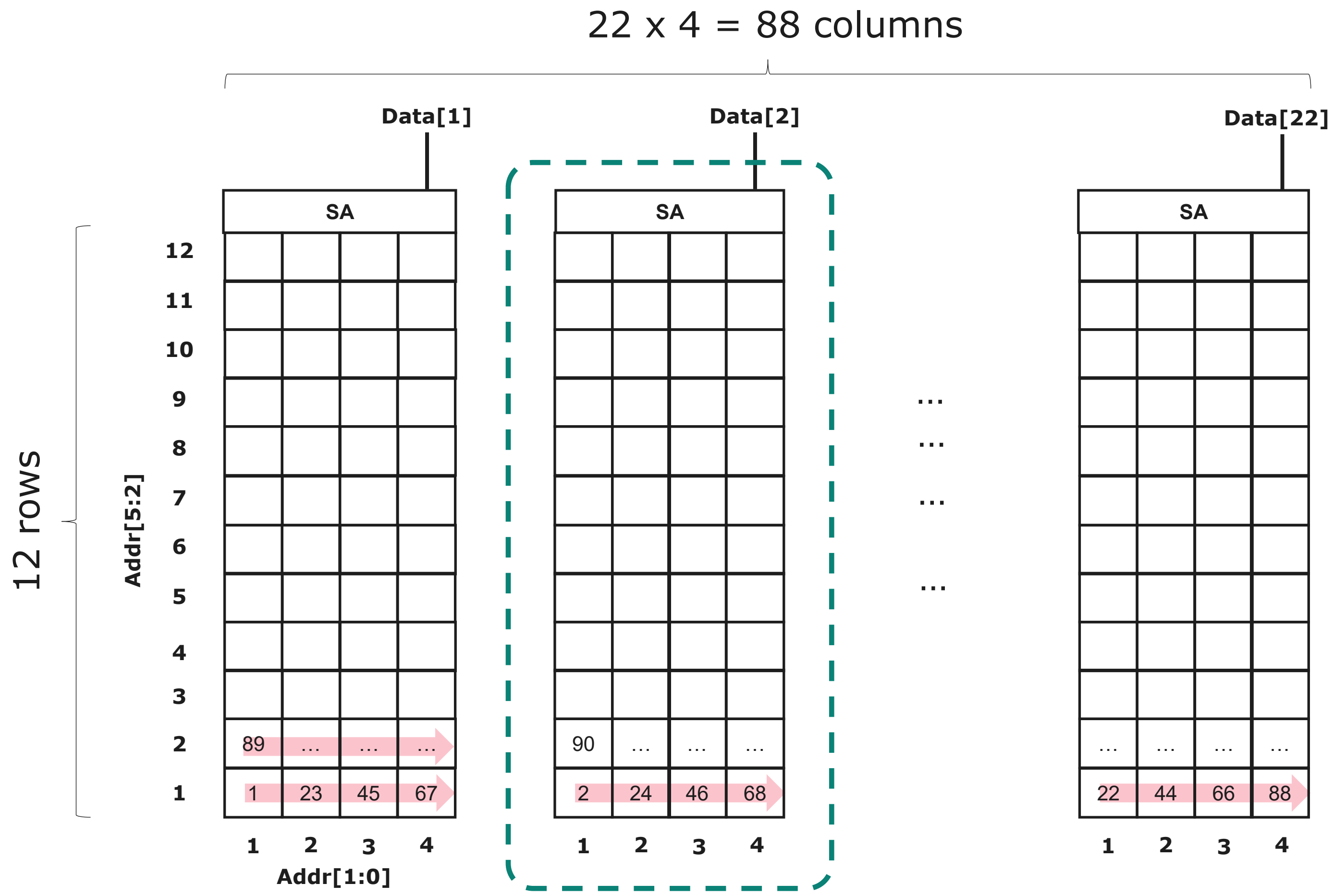
- If out@$+\Delta I_{PRE}$ ≠ out@$-\Delta I_{PRE}$, the cell is marked as unstable and sort out

M. Hofer, C. Böhm, "An Alternative to Error Correction for SRAM-Like PUFs", Proc. CHES 2010, LNCS 6225, pp. 335-350, 2010

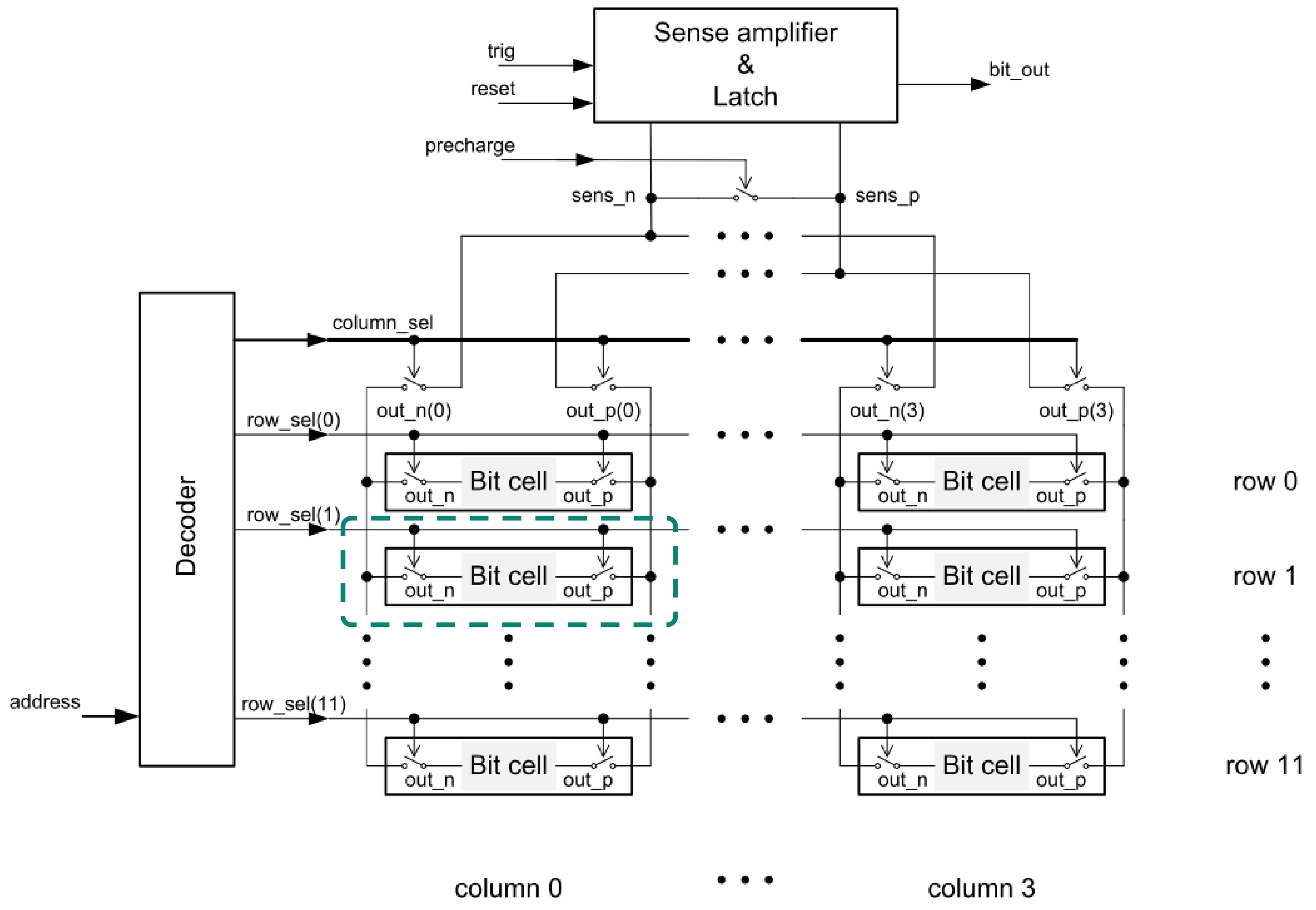
TSID PUF Key Generator



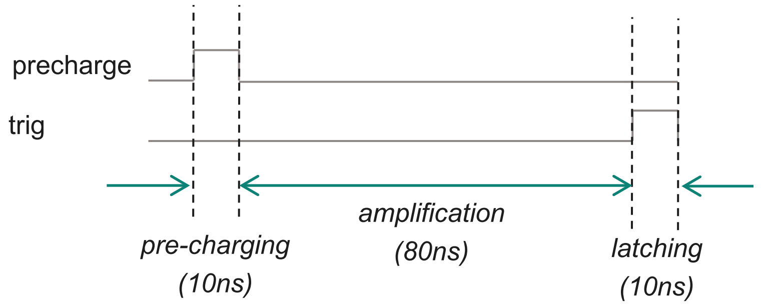
PUF Cell Array (PCA)

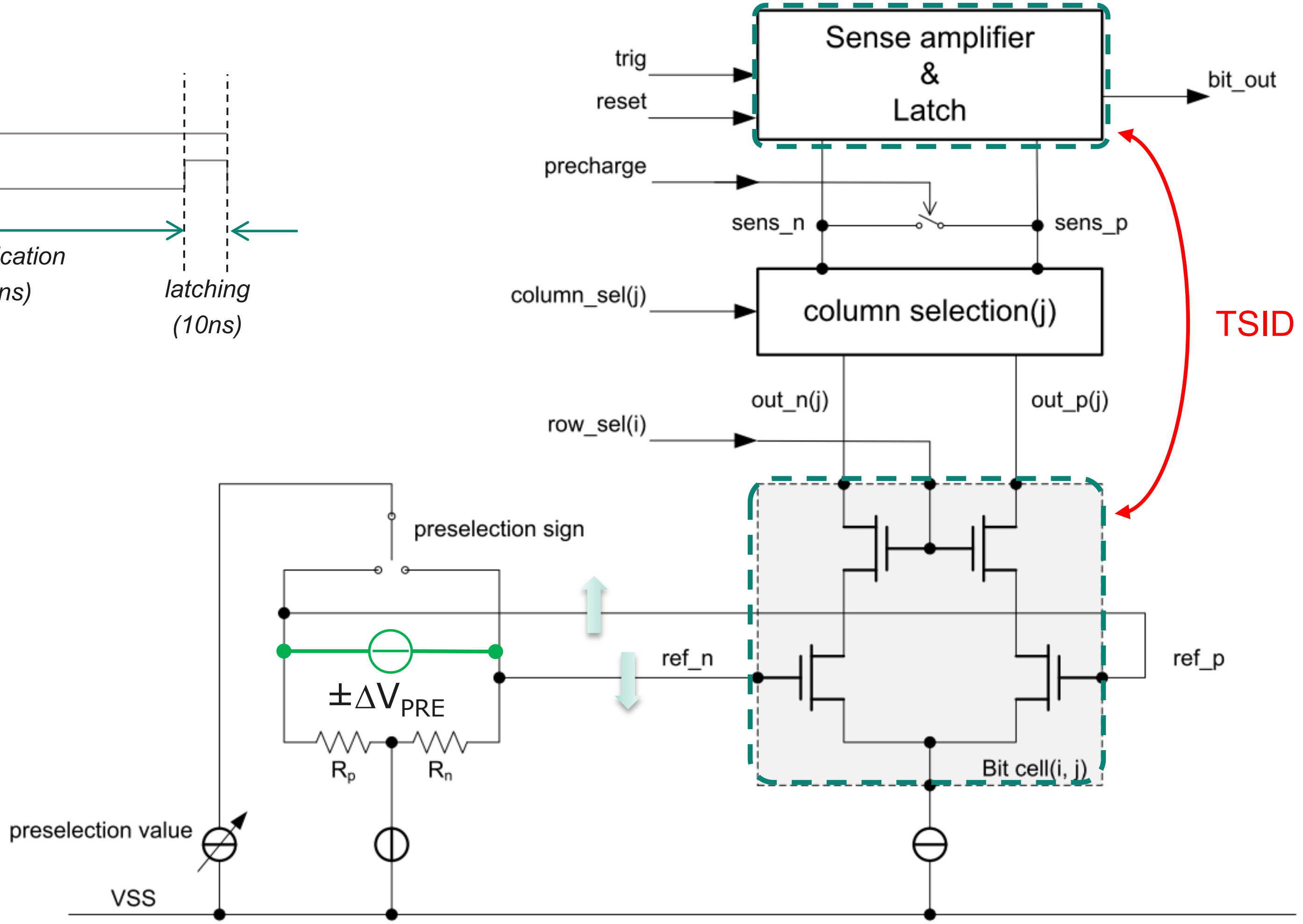


Block implementation



Cell implementation (with pre-selection)



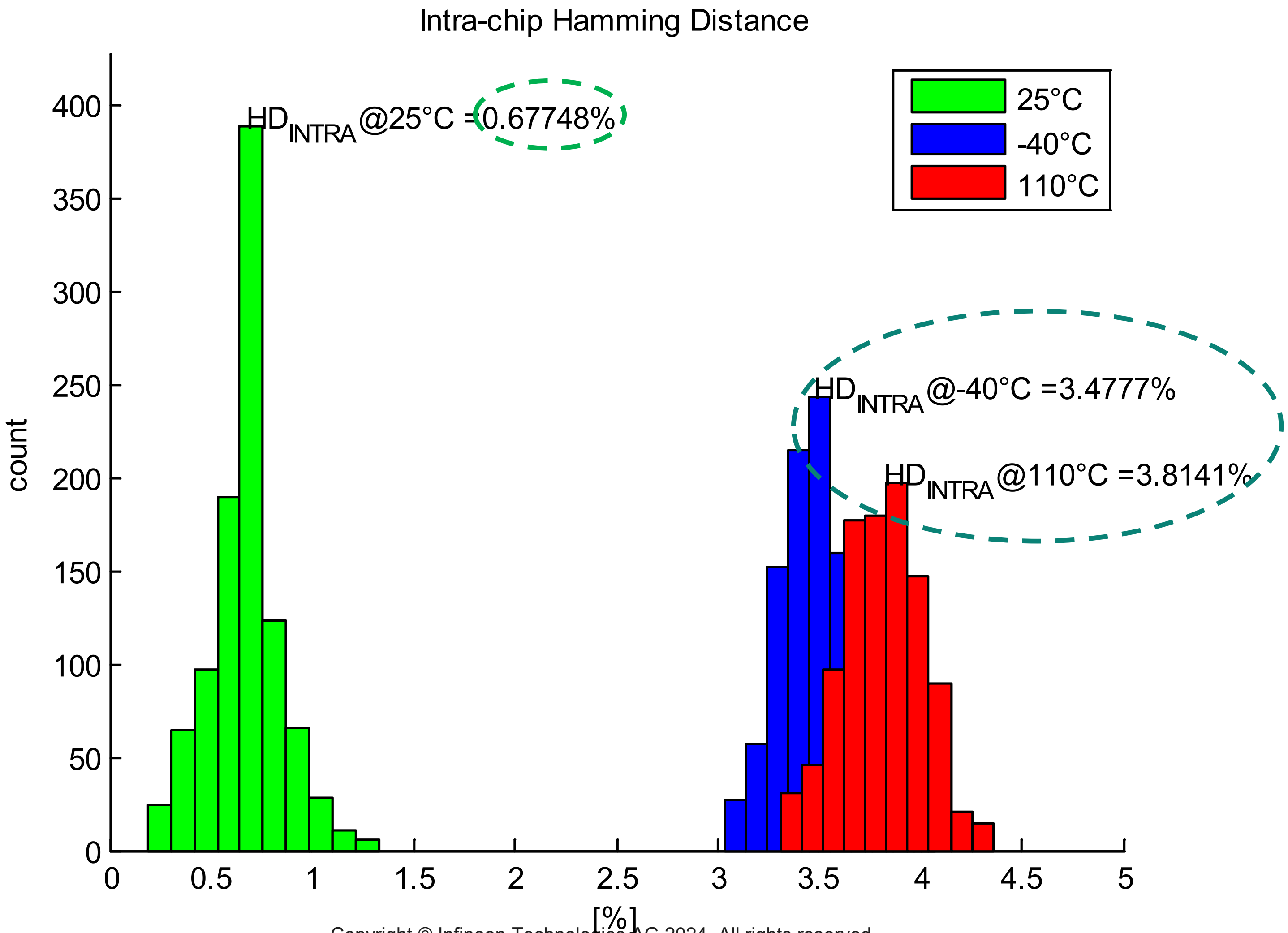


Experimental results

- Intra-chip Hamming distance
- Pre-selection test
- Stability
- Inter-chip Hamming distance
- Correlation between two neighboring bits

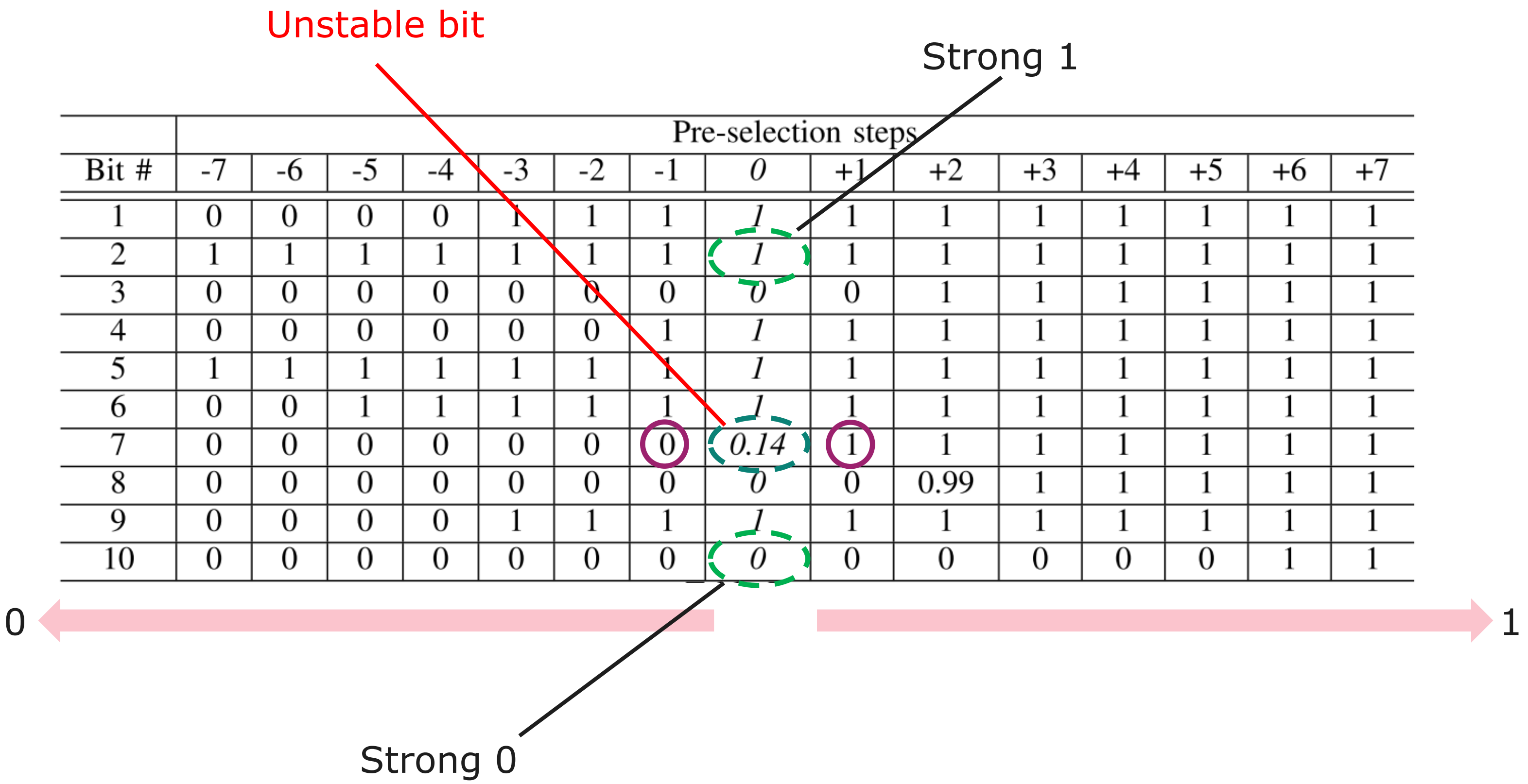
Intra-chip Hamming Distance

- NOM module, **1000 readouts**
- Reference run generated @25°C
- **no pre-selection**



Basic pre-selection test

- NOM module, **100 readouts**
- Reference run generated @25°C

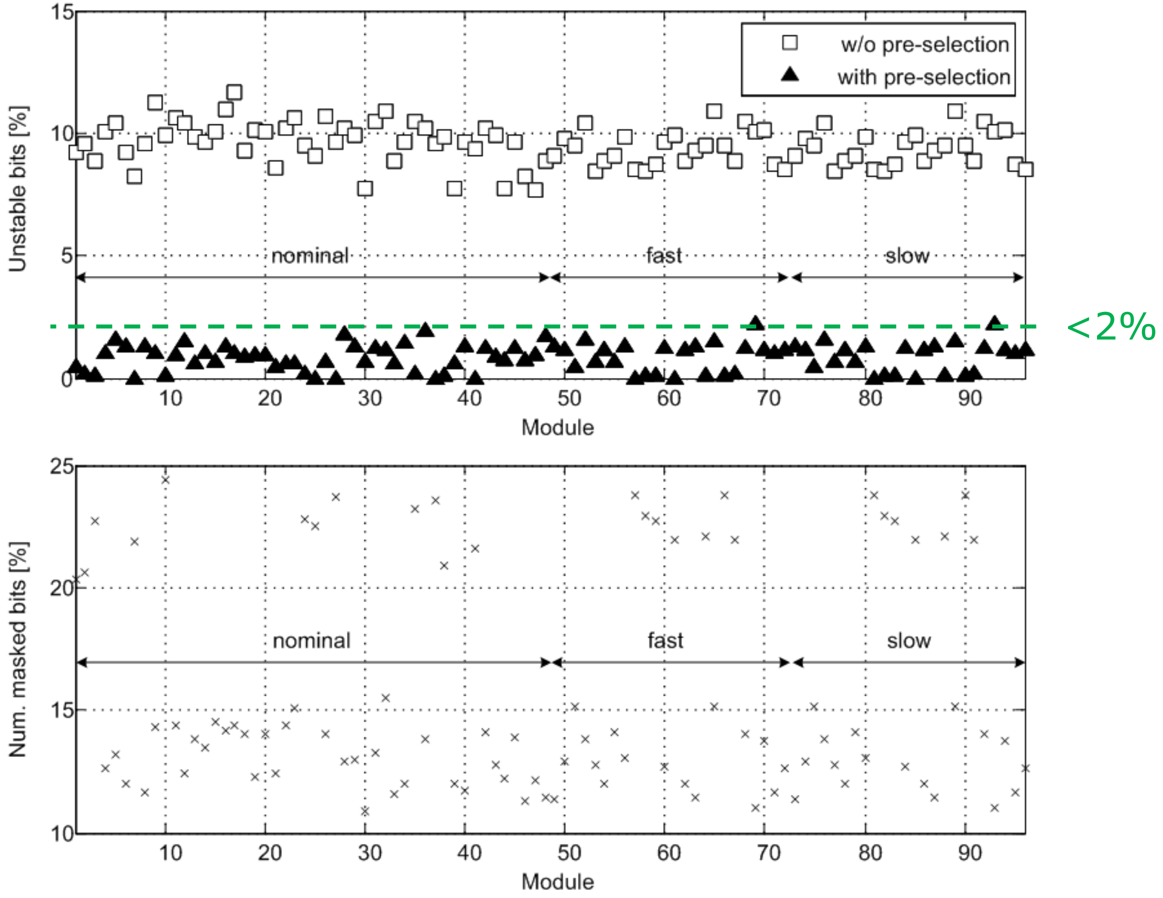


	Pre-selection steps														
Bit #	-7	-6	-5	-4	-3	-2	-1	*0*	+1	+2	+3	+4	+5	+6	+7
1	0	0	0	0	1	1	1	*1*	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	*1*	1	1	1	1	1	1	1
3	0	0	0	0	0	0	0	*0*	0	1	1	1	1	1	1
4	0	0	0	0	0	0	1	*1*	1	1	1	1	1	1	1
5	1	1	1	1	1	1	1	*1*	1	1	1	1	1	1	1
6	0	0	1	1	1	1	1	*1*	1	1	1	1	1	1	1
7	0	0	0	0	0	0	0	*0.14*	1	1	1	1	1	1	1
8	0	0	0	0	0	0	0	*0*	0	0.99	1	1	1	1	1
9	0	0	0	0	1	1	1	*1*	1	1	1	1	1	1	1
10	0	0	0	0	0	0	0	*0*	0	0	0	0	0	1	1

Unstable bit
Strong 1
Strong 0
0
1

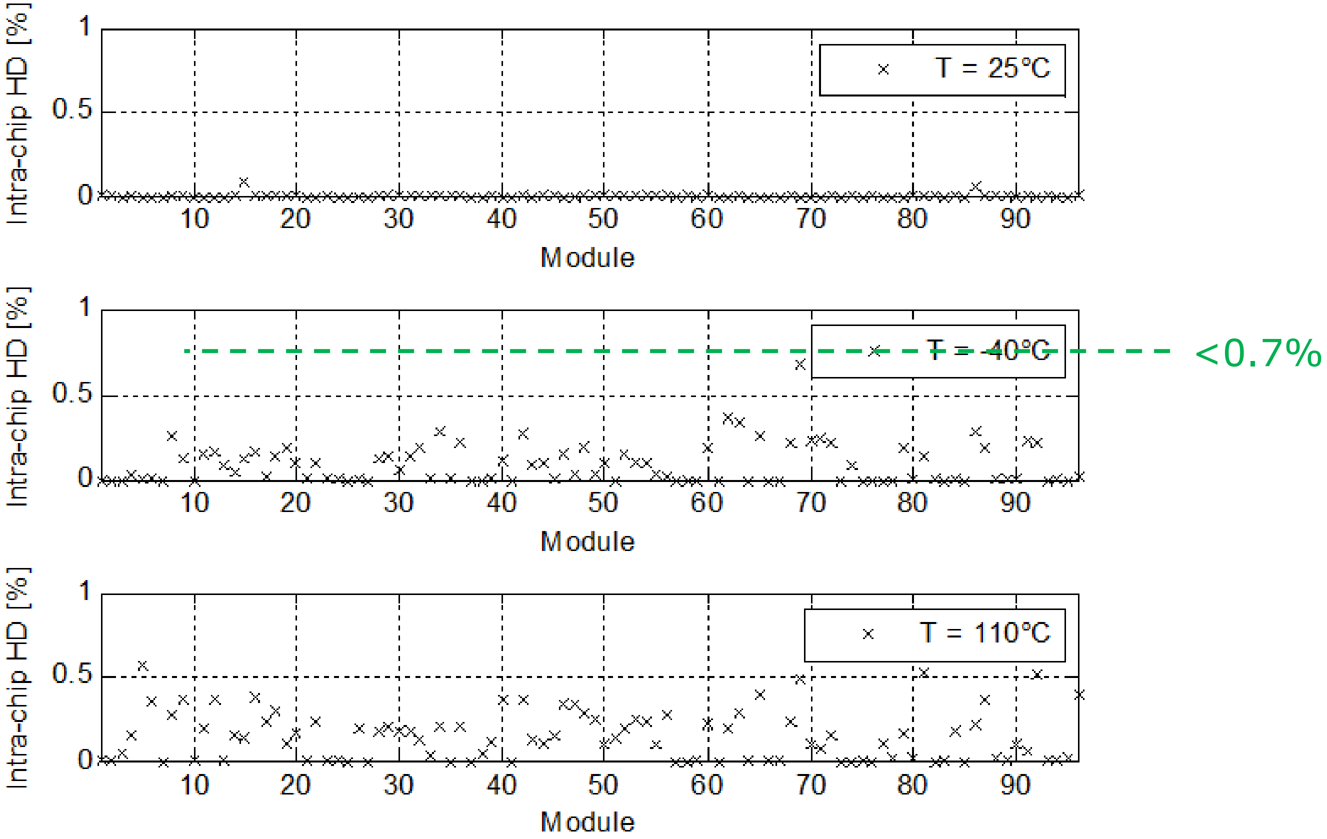
Stability

- 96 modules (NOM/FAST/SLOW), **1000 readouts**
- Reference run generated @25°C
- Tested temperatures: -40°C/+25°C/+110°C
- **with and w/o pre-selection**
- readout of the PUF repeated **16 times** (for both pre-selection directions)



Intra-chip Hamming Distance

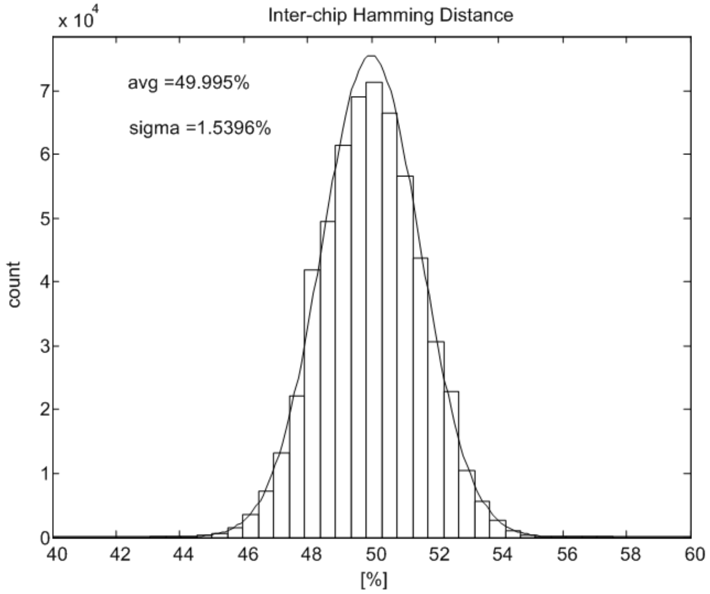
- 96 modules (NOM/FAST/SLOW), **1000 readouts**
- Reference run generated @25°C
- Tested temperatures: -40°C/+25°C/+110°C
- **with pre-selection**
- readout of the PUF repeated **16 times** (for both pre-selection directions)

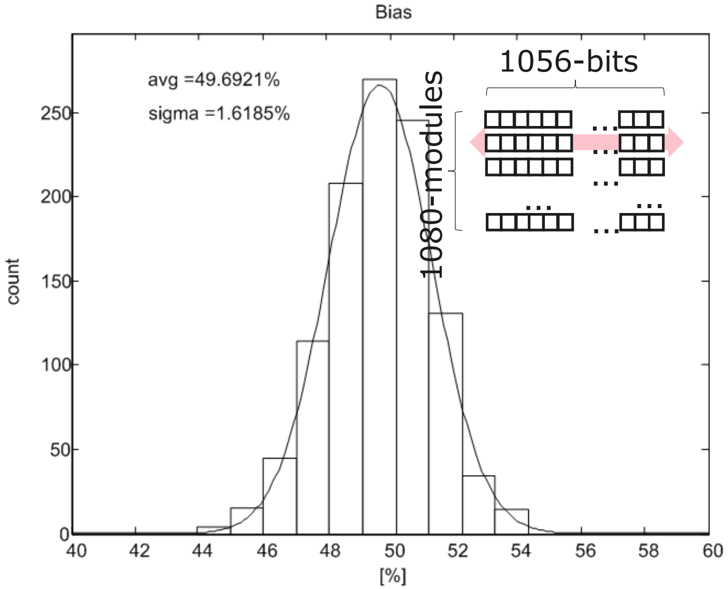


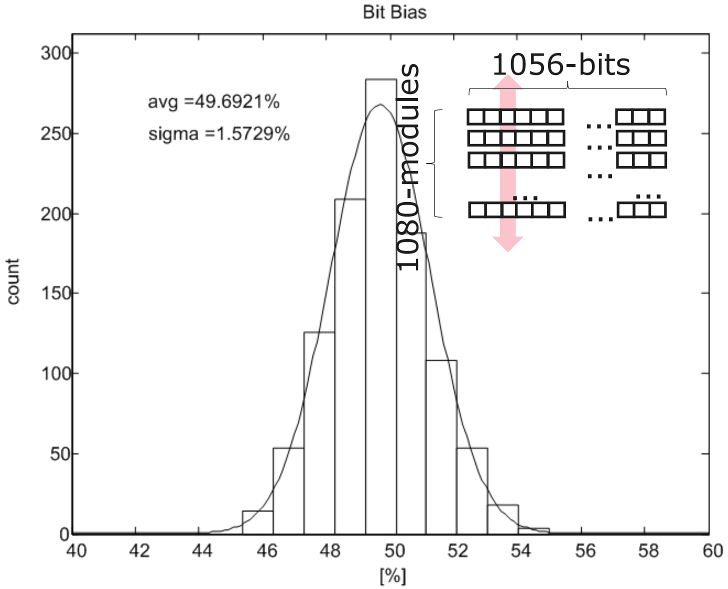
- Worst case intra-chip HD @-40°C: 0.7%

Inter-chip Hamming Distance & Bias

- **1080** modules (NOM/SLOW/FAST x360)
- Inter-chip HD = 49.995%
- Bias = 49.6921%
- Bit bias = 49.6921%







Correlation between neighboring bits

- Horizontal correlation:

$$R_H(j,i) = \left| \frac{1}{N} \sum_{k=1}^{N} \left(PCA_k(i,j) \oplus PCA_k(i,j+1)\right) - 0.5 \right|$$

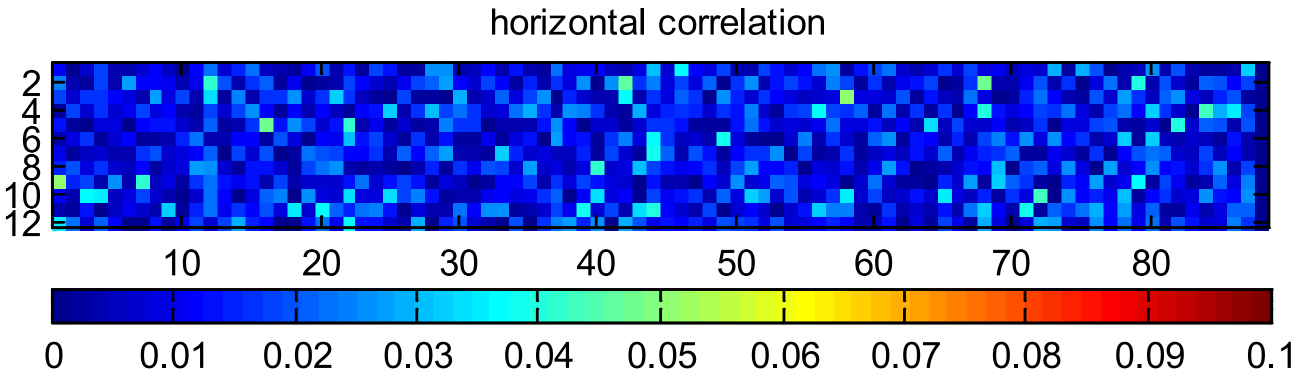
- Vertical correlation:

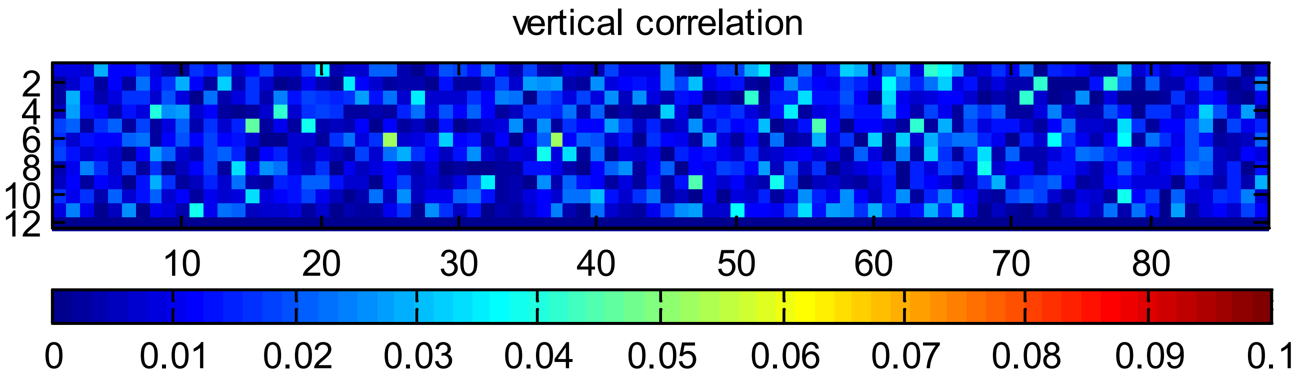
$$R_V(j,i) = \left| \frac{1}{N} \sum_{k=1}^{N} \left(PCA_k(i,j) \oplus PCA_k(i+1,j)\right) - 0.5 \right|$$

- where: N is the number of tested modules and $PCA_k(i,j)$ is the bit in position (i,j) of the k-th module

Correlation between neighboring bits

- 1080 modules (10x36 NOM, 10x36 FAST, 10x36 SLOW)





Conclusions

- A 128-bit PUF-based key generator using the TSID cell and the pre-selection technique
- Low area:
  - □ Total PCA area: 3250um^2, bit cell area: 2.4um^2 (< 4 times smaller than a SRAM cell)
- Low power:
  - □ Energy consumption per bit: 42fJ/bit.
- Reliability:
  - □ Intra-chip HD < 0.7% (under all conditions)
  - □ After 10^6 key reconstruction @-40°C and + 110°C, on 2000 devices from different wafers

  (in total **5 x 10^9** key generations), no single fail has been detected!

Thank you!

Infineon

german brand award '24
corporate brand of the year