Partial Implementation

A Reconfigurable SRAM based CMOS PUF with Challenge to Response Pairs

**S. Baek, G.H. Yu, J. Kim, C.T. NGO,
J.K. Eshraghian and J.P. Hong**

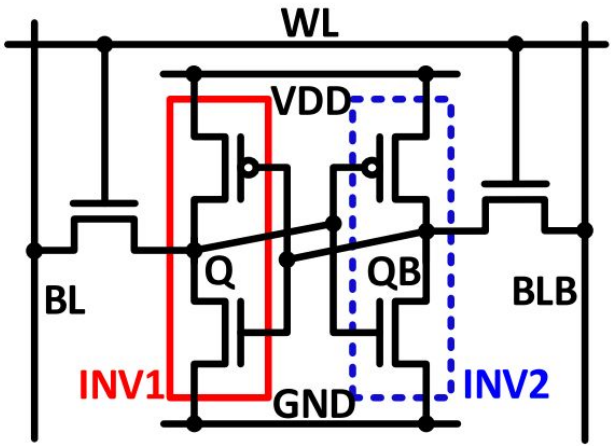
Jinay Dagli [20110084] and Neel Shah [20110187]
Department of Electrical Engineering, Indian Institute of Technology Gandhinagar
{jinay.dagli, shah.neel}@iitgn.ac.in

09th Nov 2022

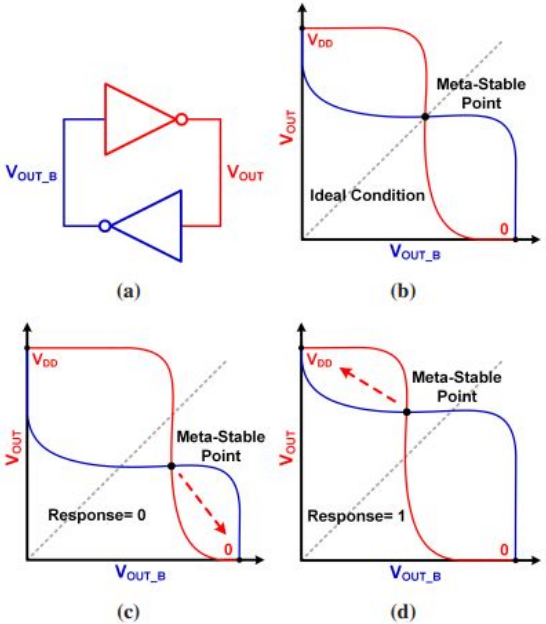
Outline

- Recap
- Reconfigurable SRAM-based PUF
- Schematic
- Circuit Implementation
- Simulations
- Results
- Future Plan

Recap



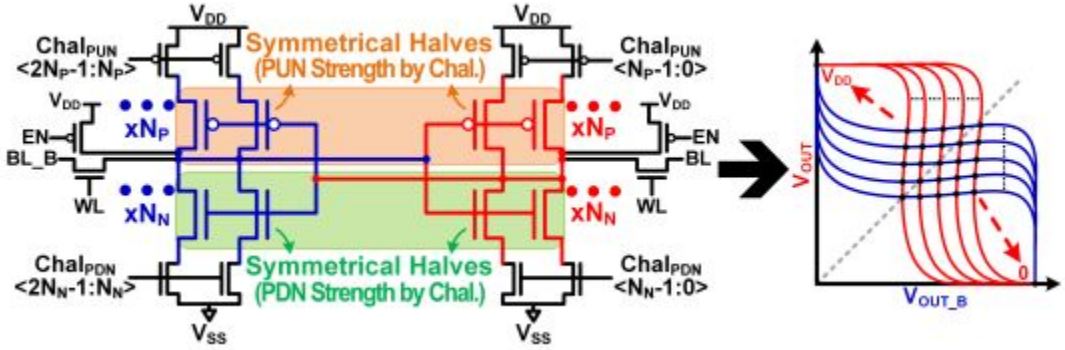
SRAM Cell, V_{th} differences in the transistors result in the SRAM powering up in either a logic "0" (Q = 0, QB = 1) or logic "1" (Q = 1, QB = 0).



Voltage Transfer Characteristics of Conventional SRAM PUF

C. Herder, M. -D. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1126-1141, Aug. 2014, doi: 10.1109/JPROC.2014.2320516.

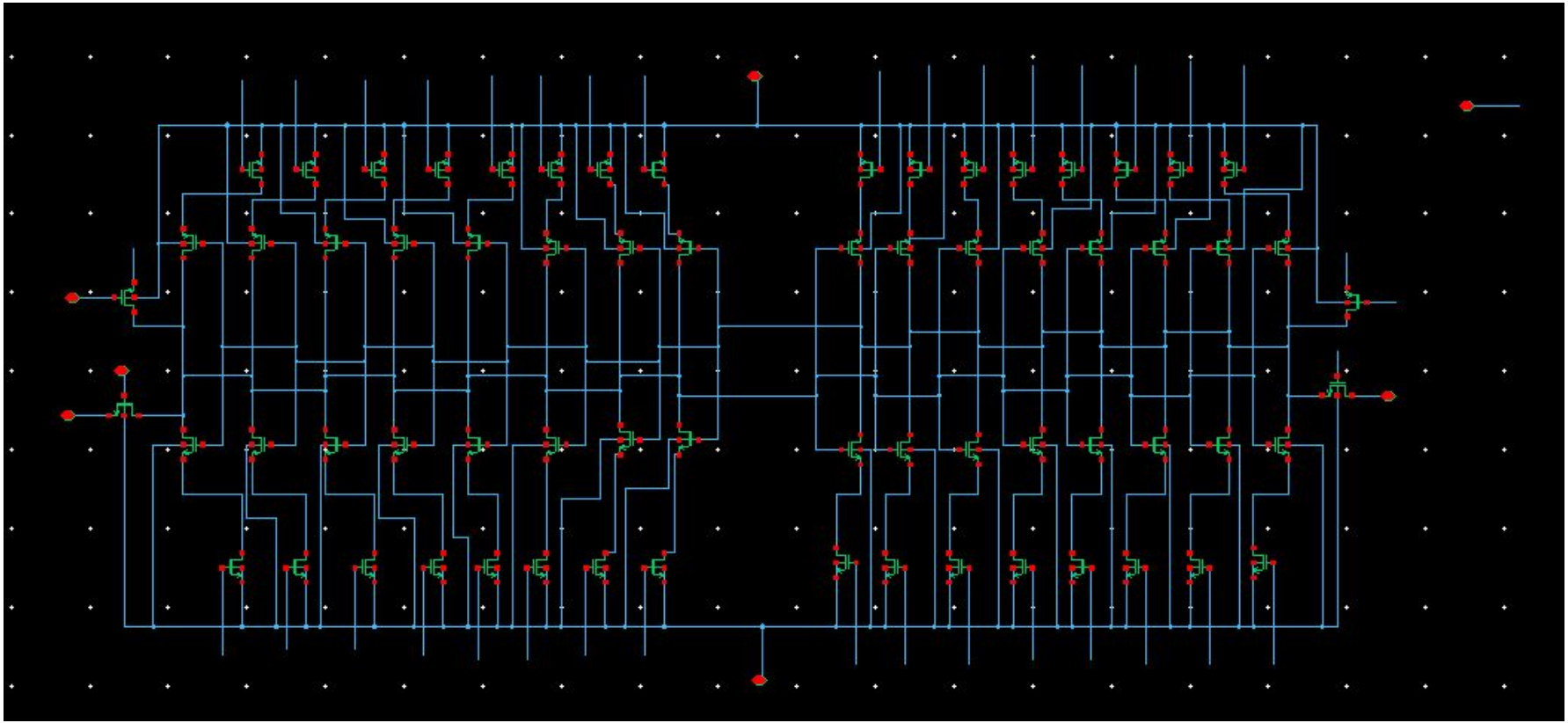
Reconfigurable SRAM-based PUF



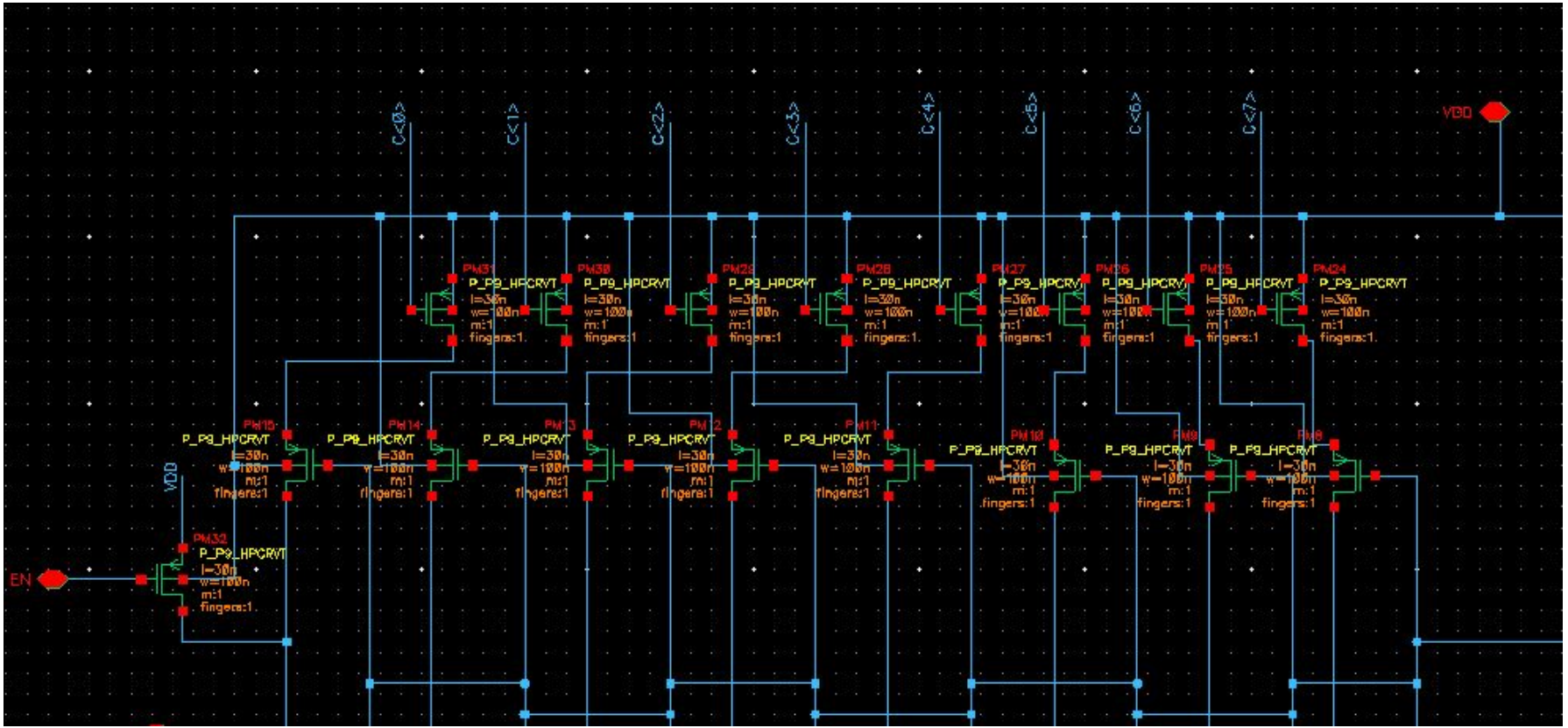
The reconfigurable SRAM cell comprises of multiple cross-coupled inverters with challenge inputs applied to switching transistors to reconfigure the relative strength of the pull-up network (PUN) and pull-down network (PDN).

S. Baek, G. -H. Yu, J. Kim, C. T. Ngo, J. K. Eshraghian and J. -P. Hong, "A Reconfigurable SRAM Based CMOS PUF With Challenge to Response Pairs," in IEEE Access, vol. 9, pp. 79947-79960, 2021

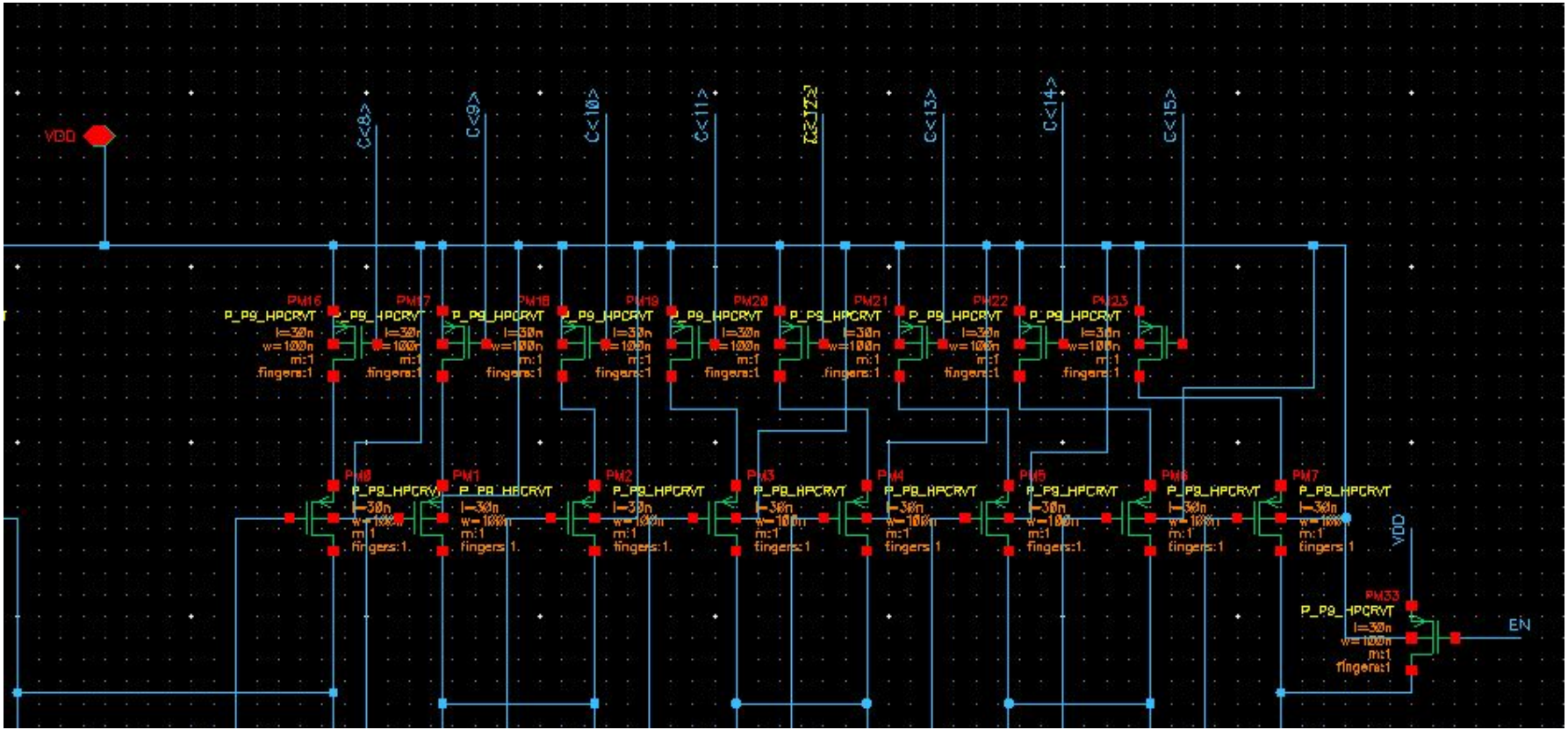
Schematic (SRAM-PUF Cell)



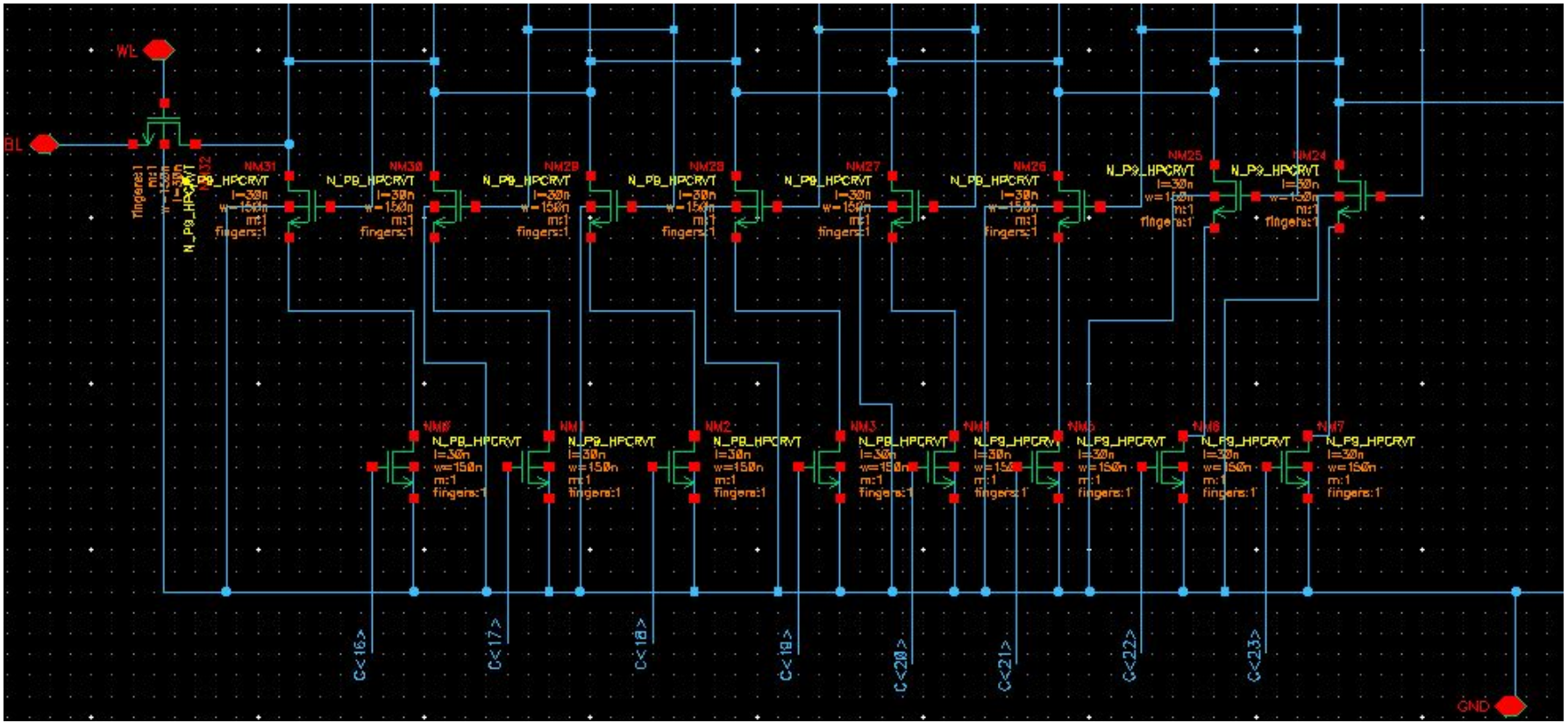
Schematic (Top Left of Cell)



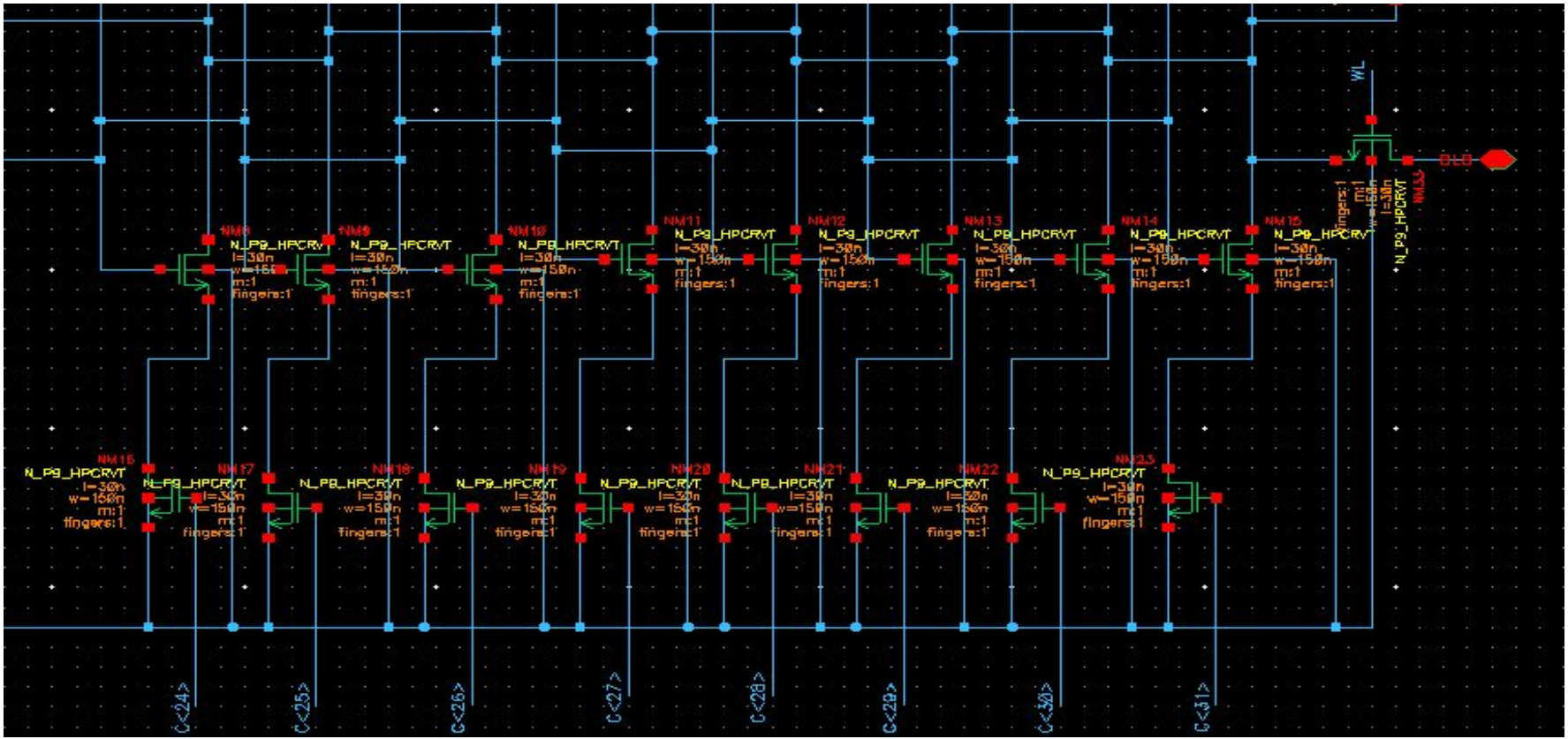
Schematic (Top Right of Cell)



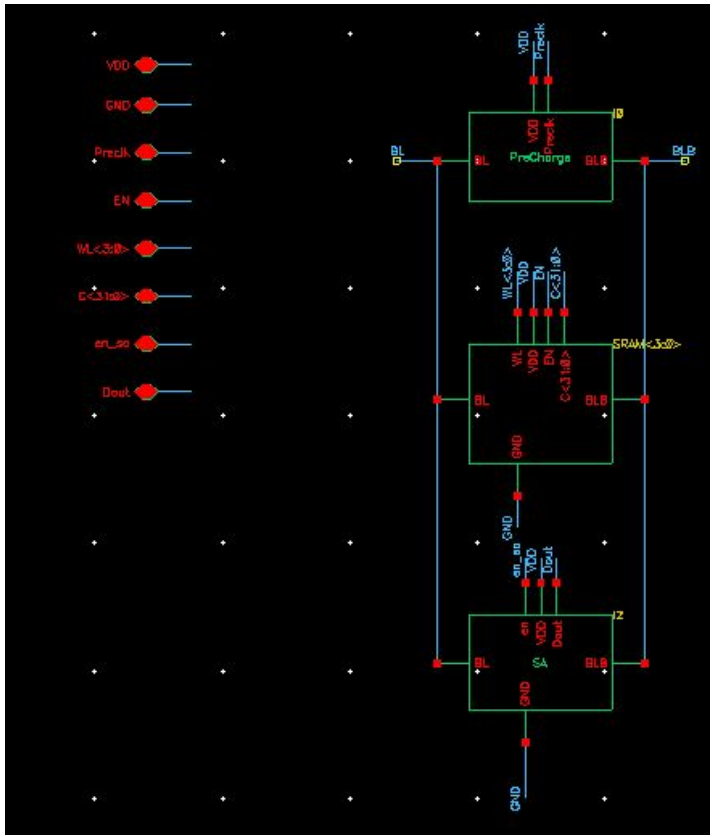
Schematic (Bottom Left of Cell)



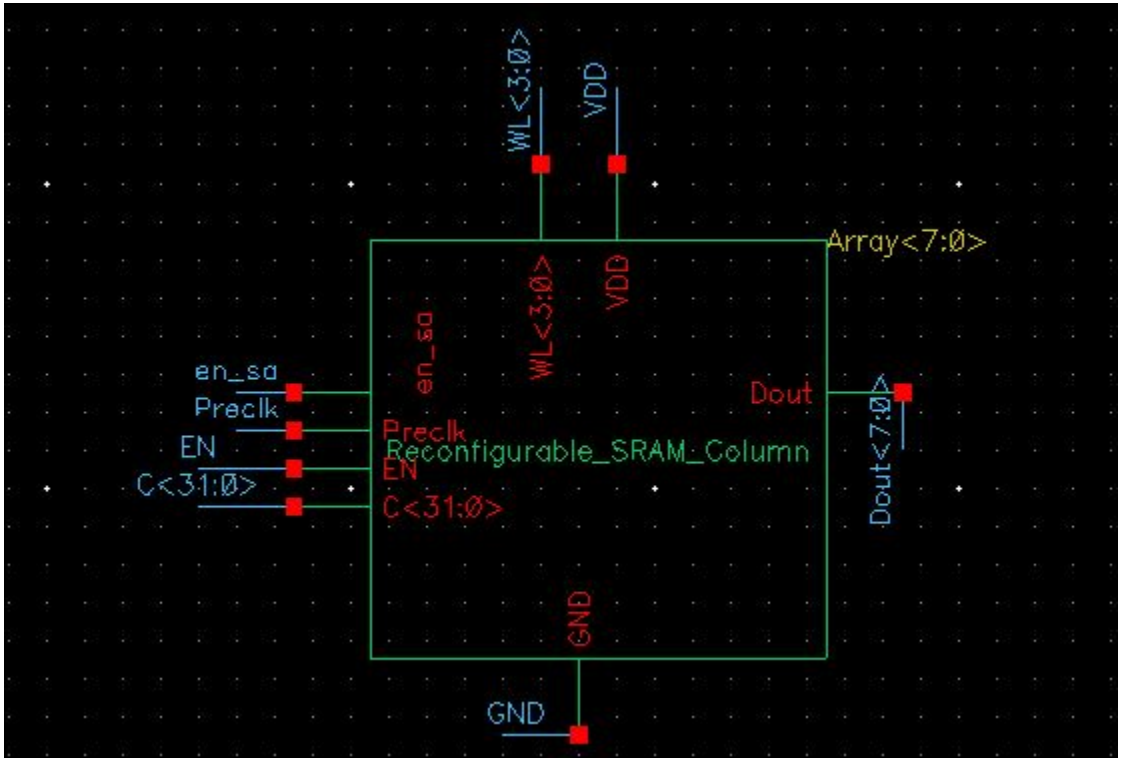
Schematic (Bottom Right of Cell)



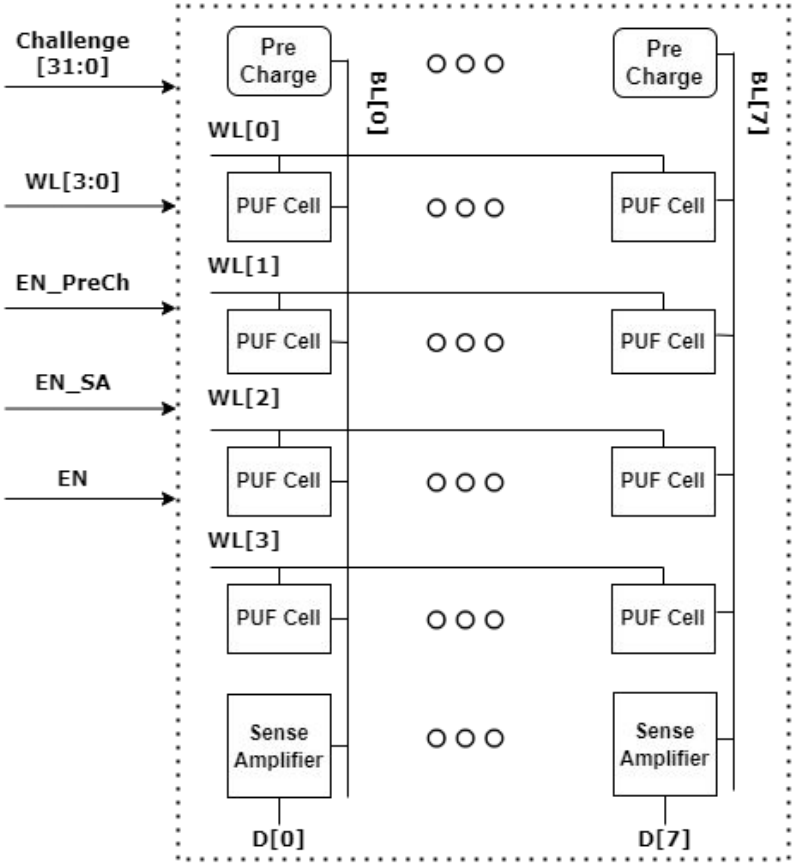
Schematic (SRAM-PUF Column)



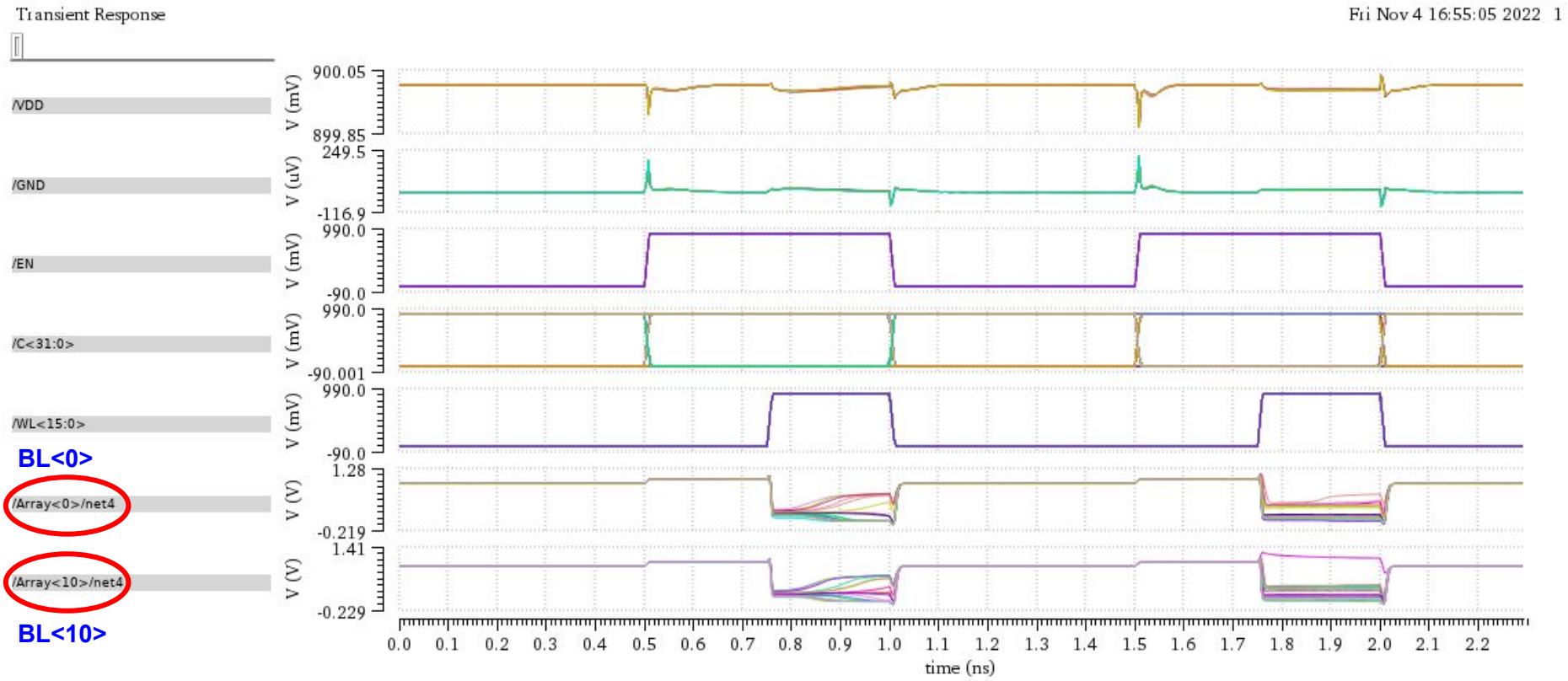
Schematic (SRAM-PUF Array)



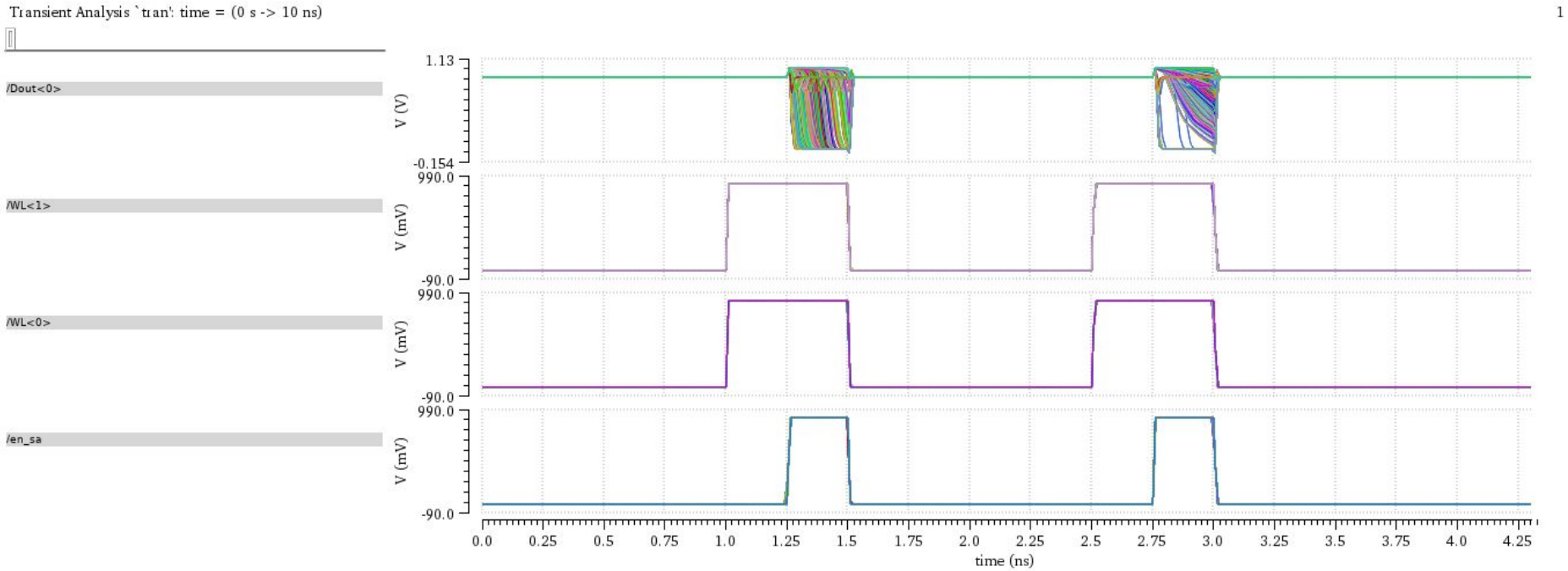
Circuit Implementation



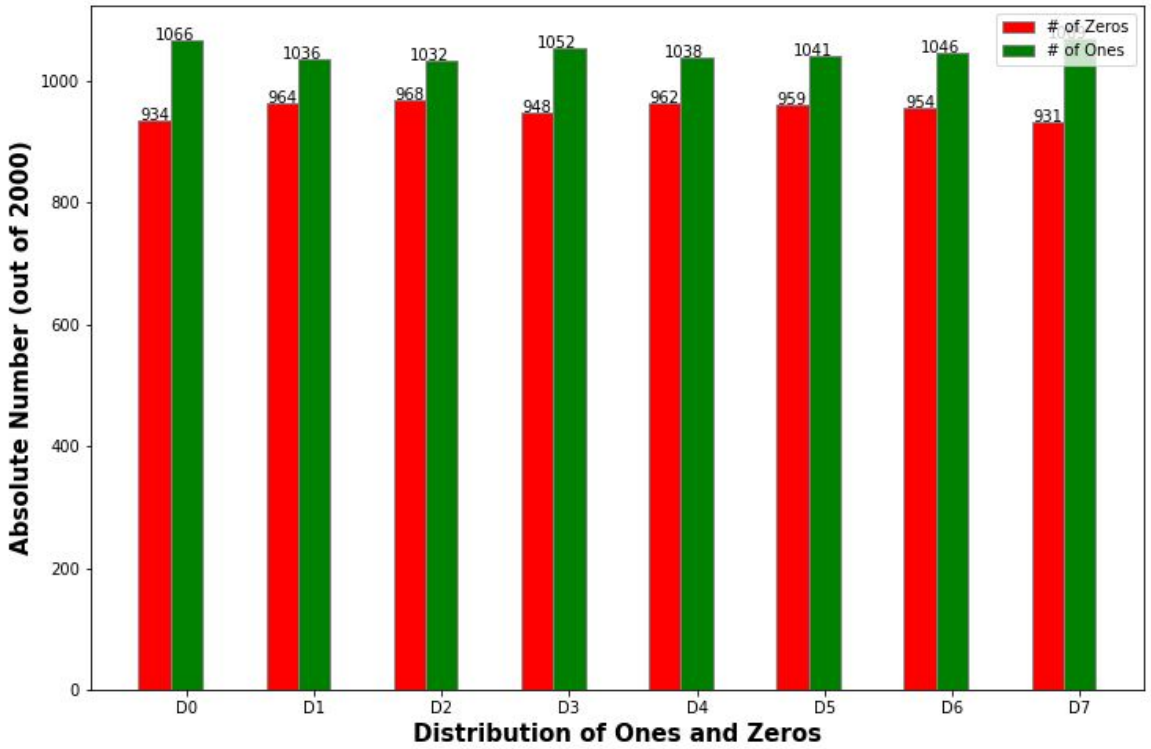
Simulations



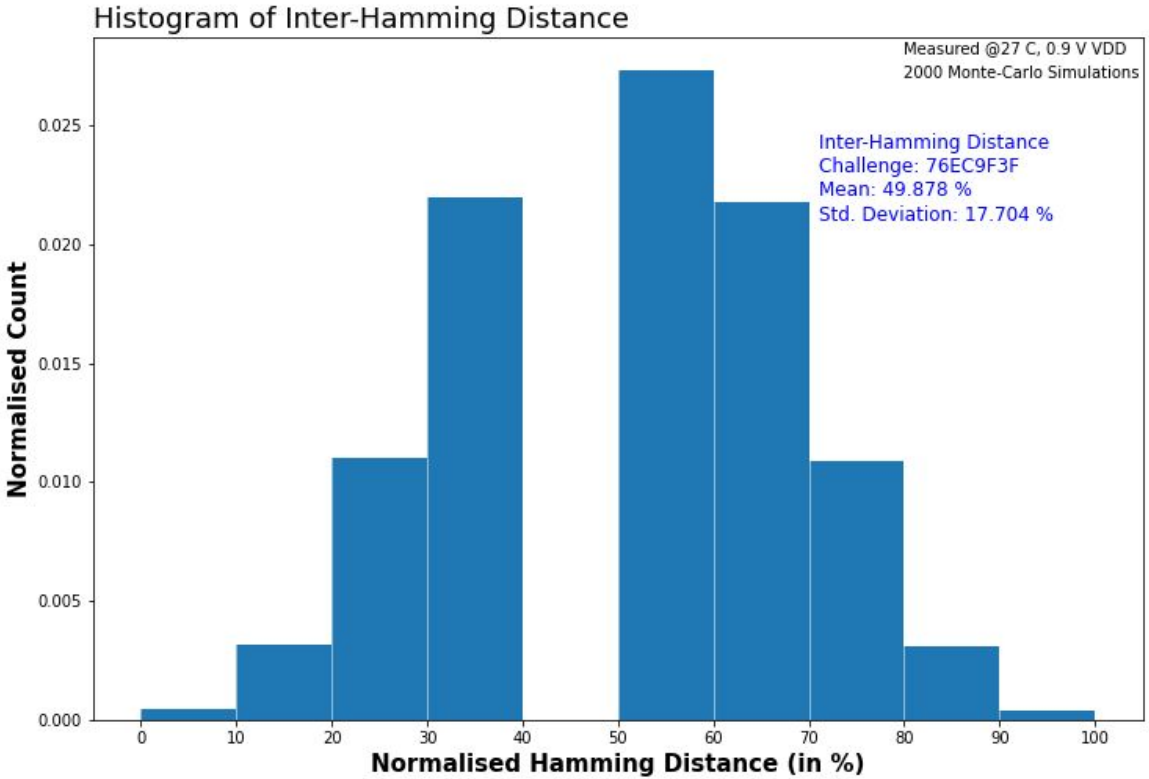
Simulations



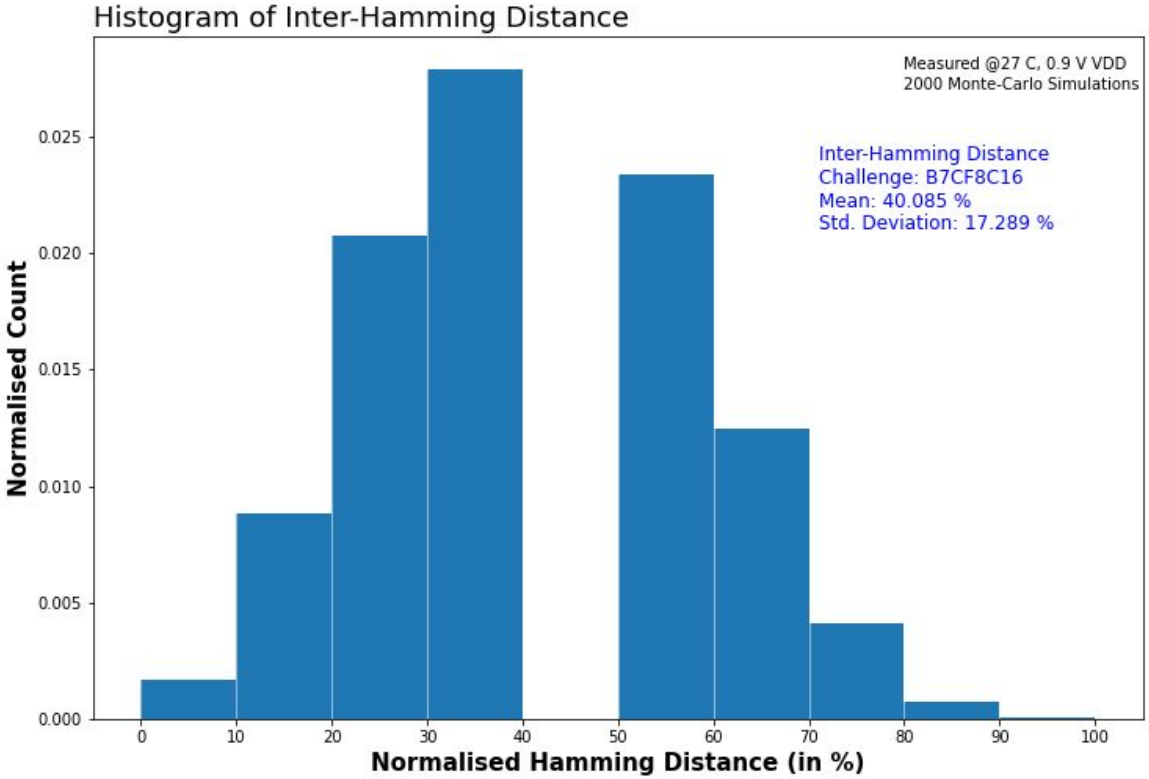
Results (Hamming Weight)



Results (Inter-Hamming Distance)



Results (Inter-Hamming Distance)



Results (NIST Test)

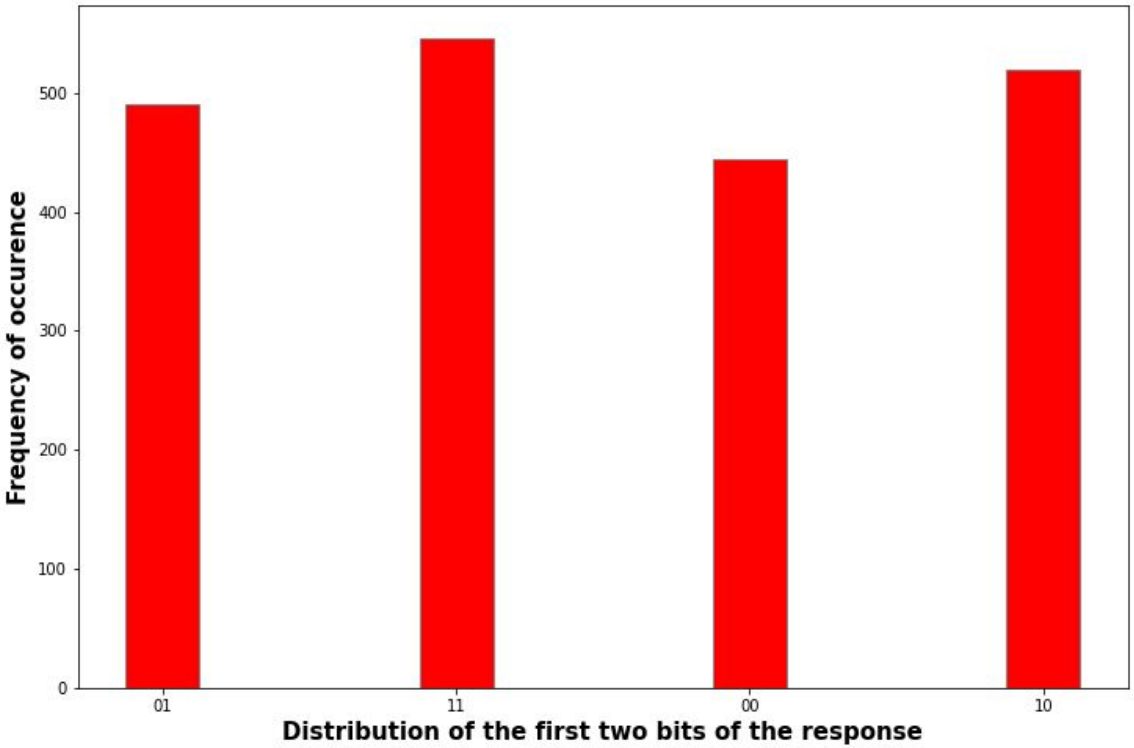
TEST	Result
Monobit Test	PASS
Frequency Within Block Test	PASS
Runs Test	PASS
Longest Run Ones in a Block Test	PASS
Binary Matrix Rank Test	PASS
DFT Test	PASS
Non-Overlapping Template Matching Test	PASS

Results (NIST Test)

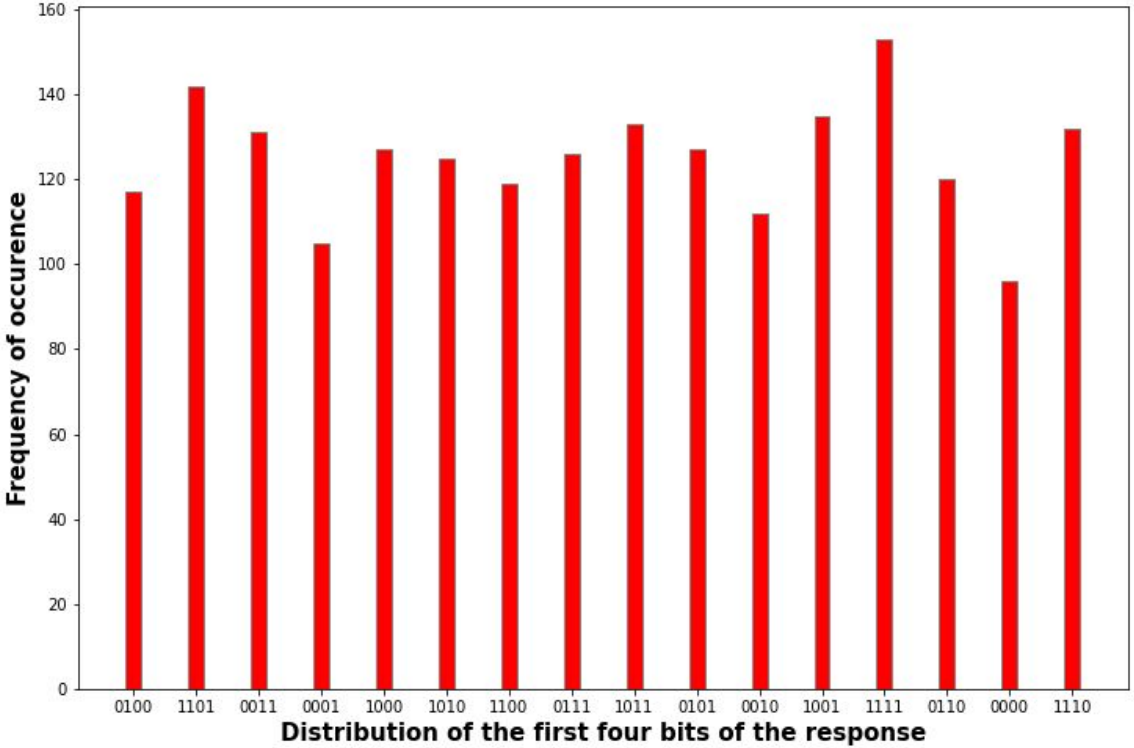
Overlapping Template Matching Test	FAIL
Maurers Universal Test	FAIL
Linear Complexity Test	FAIL
Serial Test	PASS
Approximate Entropy Test	PASS
Cumulative Sums Test	PASS
Random Excursion Test	FAIL
Random Excursion Variant Test	PASS

11 Out of 15 Tests Passed !

Test of Uniformity (Data Visualization)



Test of Uniformity (Data Visualization)



Results (BER)

- The worst case bit error on keeping the supply voltage constant when temperature was made 80° C, is calculated using the difference between the elements of the dataset generated from the two simulations.
- Bit Error was measured when the same challenge was provided to get an 8-bit response at different temperatures.
- The worst case BER in this case is found to be 3.7% !
- Furthermore, the supply voltage could also be changed and the responses could be observed. It is expected that this bit error rate would increase further.

Future Plan

- To measure inter-hamming distance for more challenge inputs and plot the histogram of mean resulting from all cases.
- To measure intra-hamming distance and plot the histogram.
- Layout of the Reconfigurable SRAM-PUF Array.
- Subsequently, measure the core area, energy consumption and throughput.
- Compare the results with **S. Jeloka et al.** which proposed a sequence dependent challenge-response PUF using 28nm 6T SRAM.

Thank You!

Any Questions?

Source : Google Images