Final Presentation

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

20th Nov 2022

Outline

- Objective
- Introduction
- Why Physically Unclonable Functions (PUFs)?
    - Significance of PUFs
    - Classification of PUFs
- Conventional SRAM-based PUF
- Reconfigurable SRAM-based PUF
- Schematic
- Circuit Implementation
- Simulations
- Results

Objective

➢ Implement the Reconfigurable SRAM-PUF Design

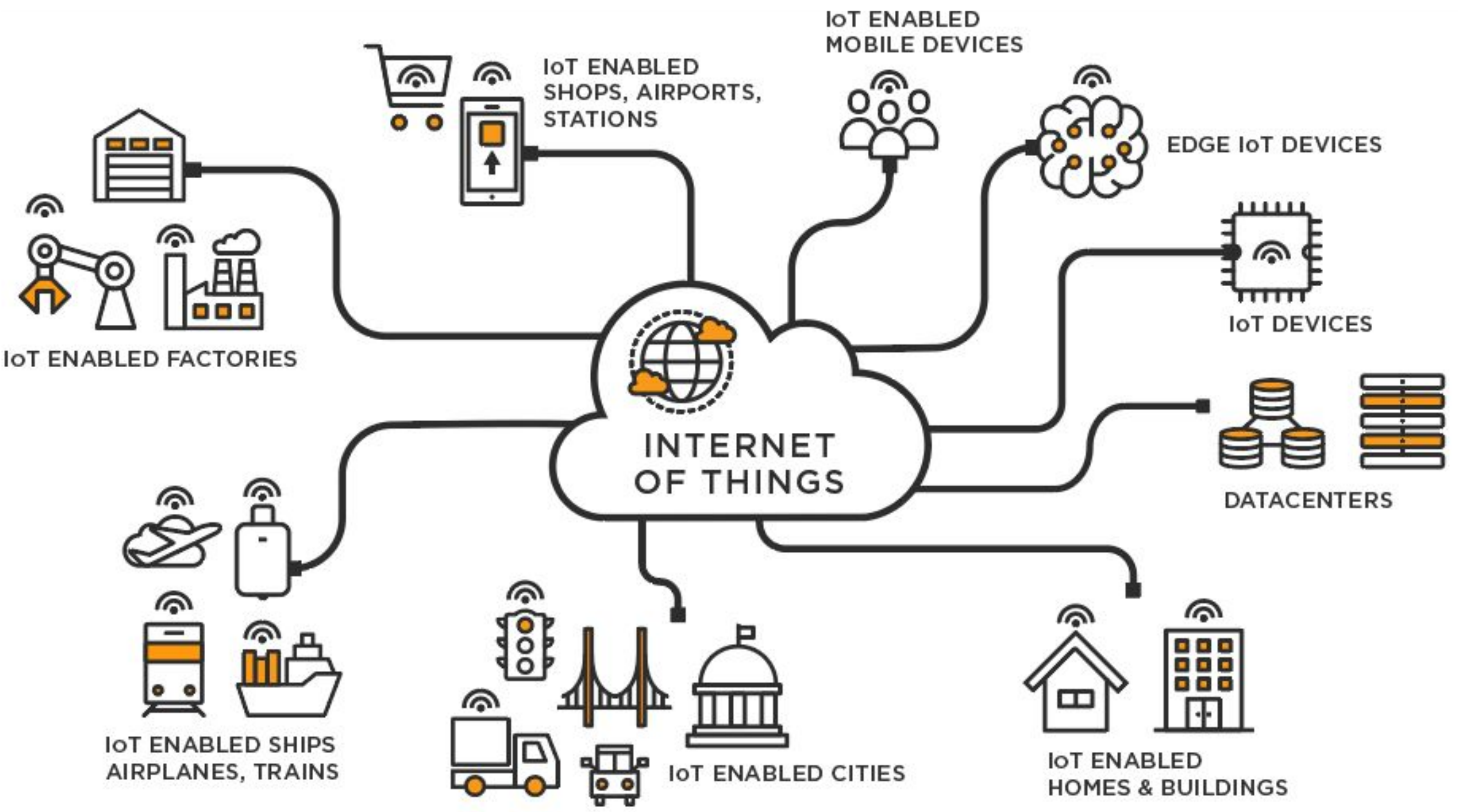
- ○ The paper by S. Baek et al. proposes reconfigurable SRAM-PUF with multiple CRPs. We had to implement it on 28 nm technology to check the scalability.

➢ Analysis of Randomness in the PUF Design

- ○ Analyze the PUF design in terms of possible number of CRPs, randomness in response bits generated, static power, average dynamic energy etc. by performing various simulations.

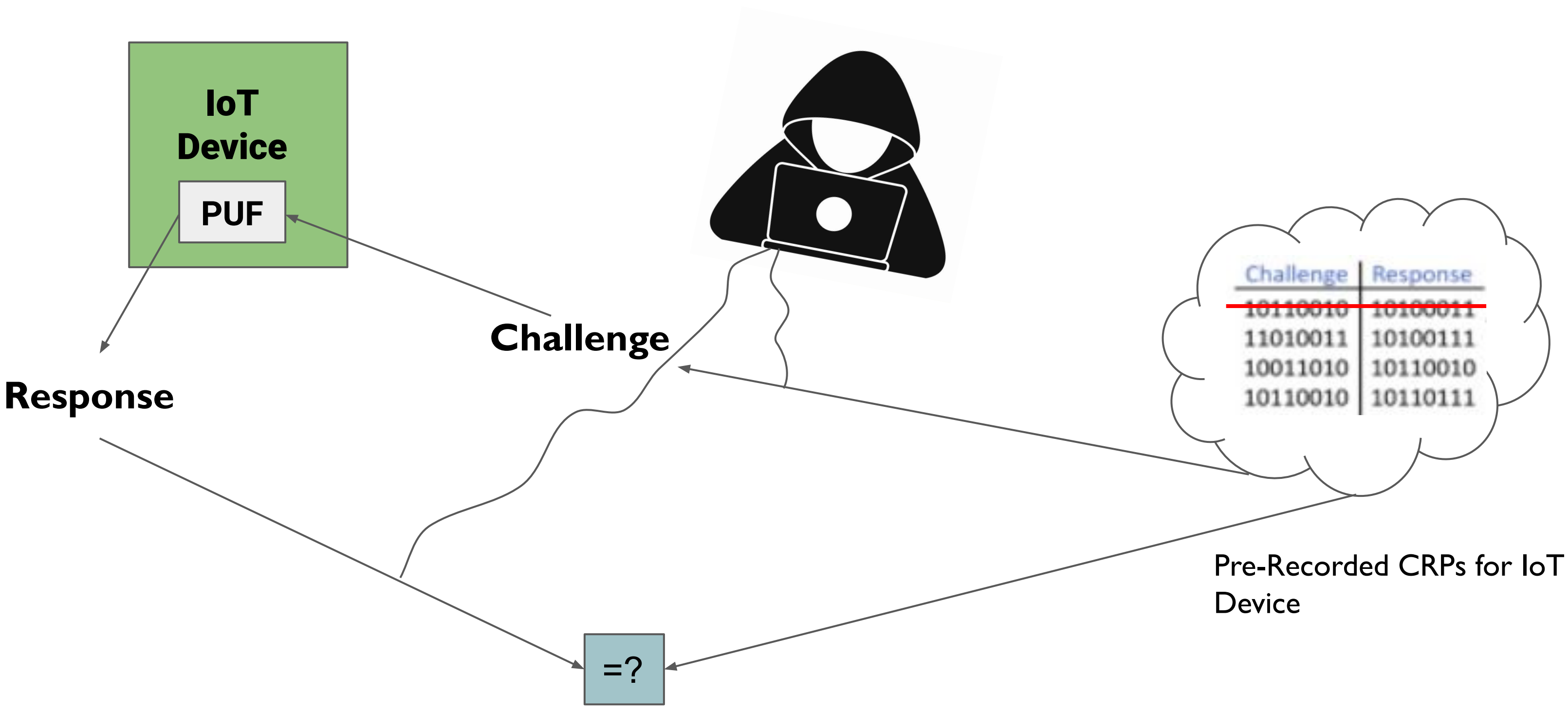
J. -W. Nam, J. -H. Ahn and J. -P. Hong, "Compact SRAM-Based PUF Chip Employing Body Voltage Control Technique," in *IEEE Access*, vol. 10, pp. 22311-22319, 2022, doi: 10.1109/ACCESS.2022.3153359.

Introduction


IoT ENABLED SHOPS, AIRPORTS, STATIONS
IoT ENABLED MOBILE DEVICES
EDGE IoT DEVICES
IoT ENABLED FACTORIES
IoT DEVICES
INTERNET OF THINGS
DATACENTERS
IoT ENABLED SHIPS AIRPLANES, TRAINS
IoT ENABLED CITIES
IoT ENABLED HOMES & BUILDINGS

Source : Google Images

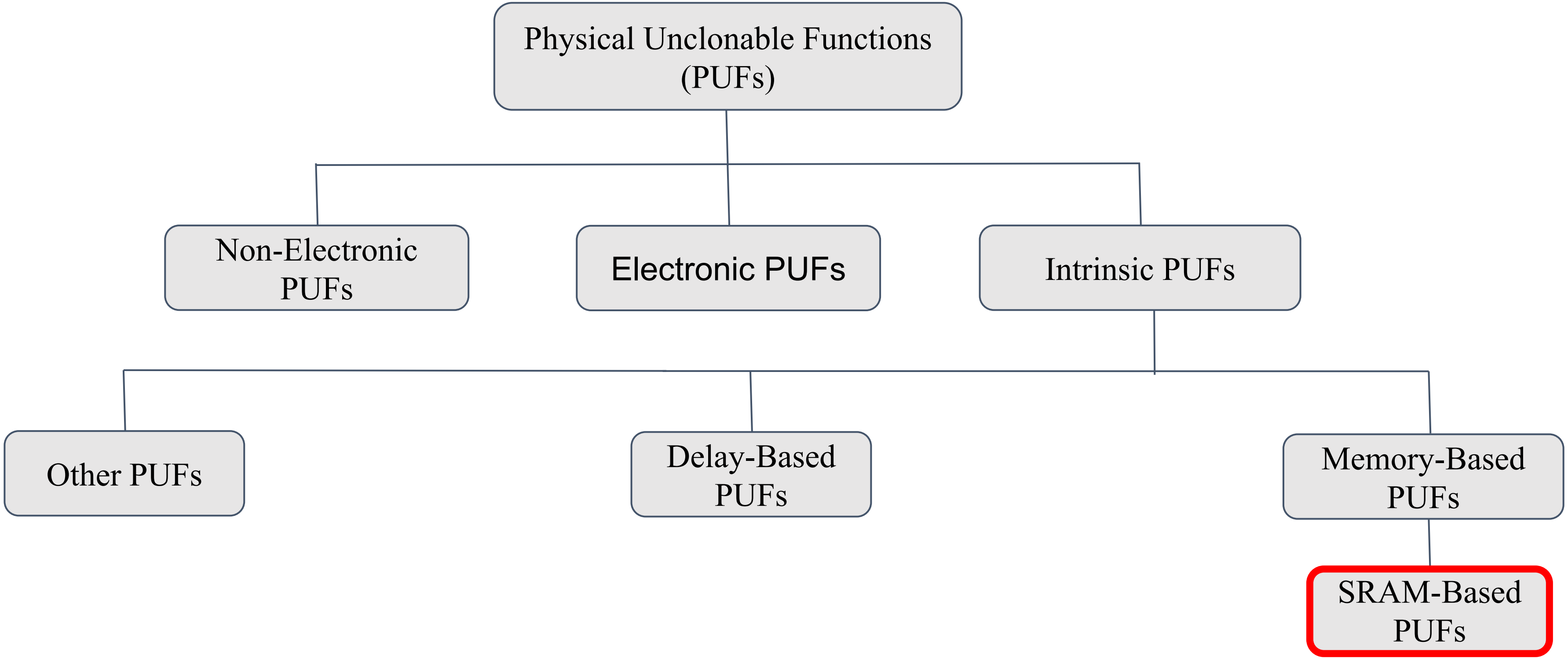
Significance of PUFs



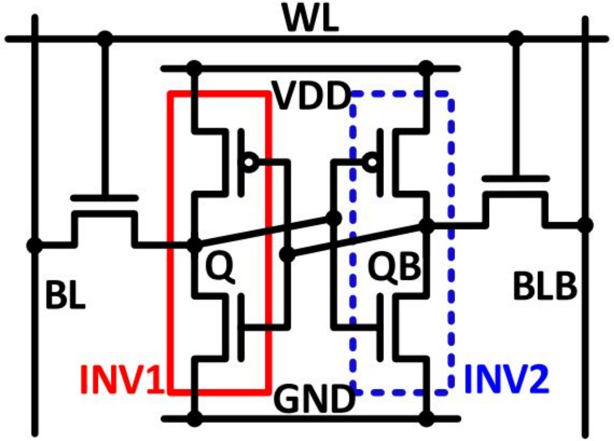
Challenge	Response
~~10110010~~	~~10100011~~
11010011	10100111
10011010	10110010
10110010	10110111

Pre-Recorded CRPs for IoT Device

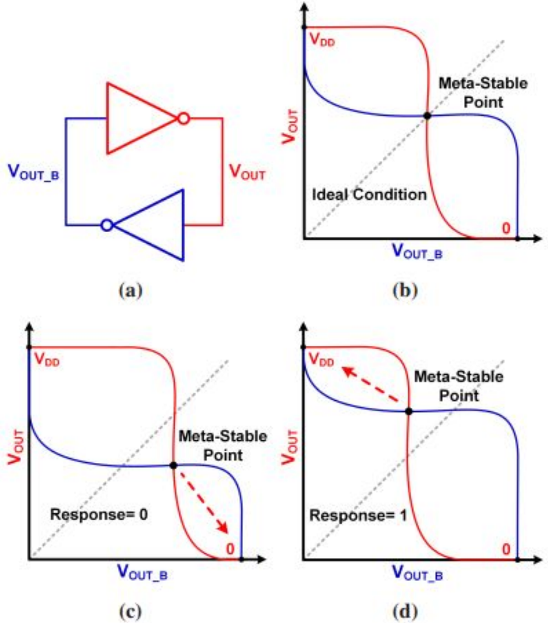
Classification of PUFs



Conventional SRAM-based PUF



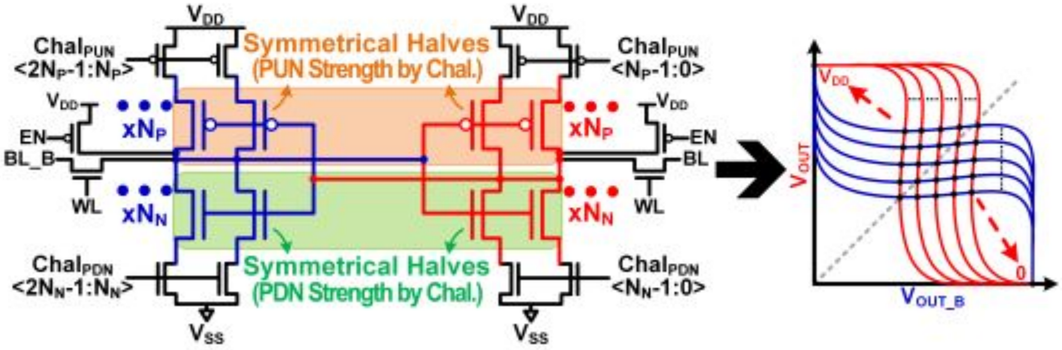
SRAM Cell, V_{th} differences in the transistors result in the SRAM powering up in either a logic "0" (Q = 0, QB = 1) or logic "1" (Q = 1, QB = 0).



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.

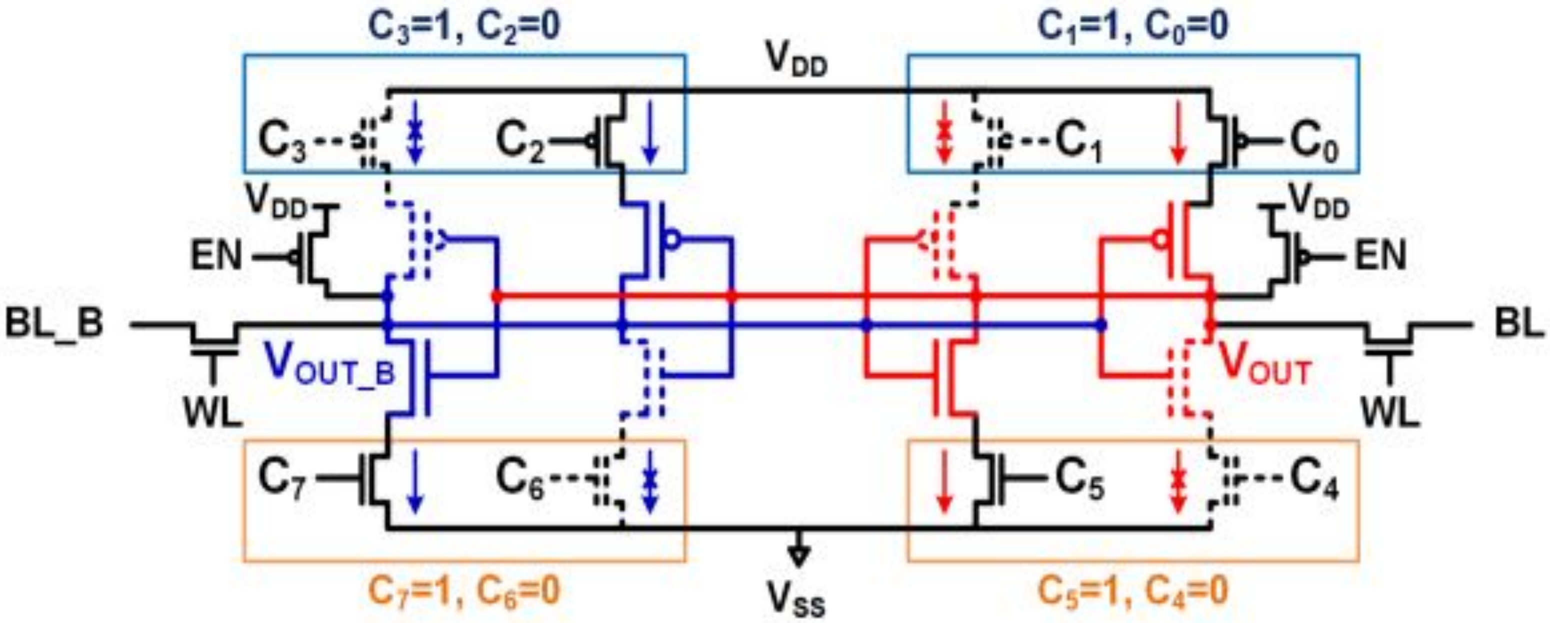
Reconfigurable SRAM-based PUF



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).

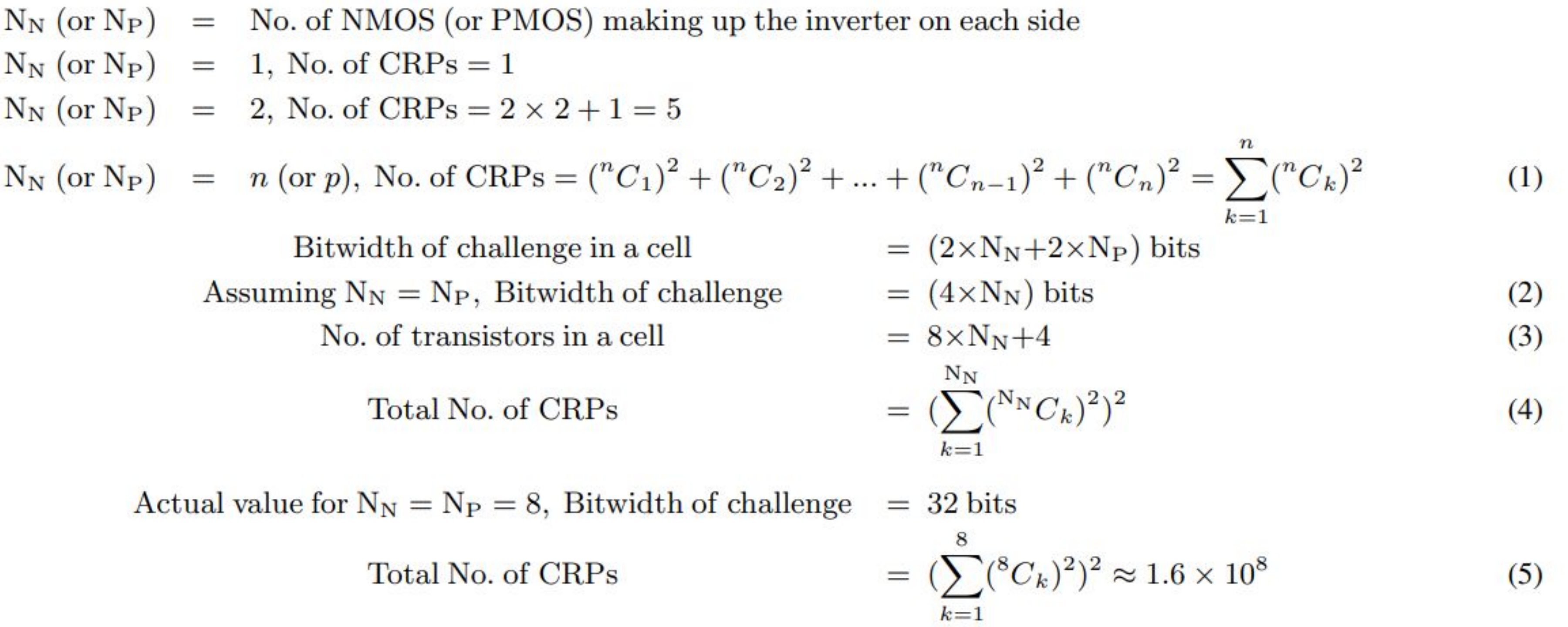
S. Baek, G. -H. Yu, J. Kim, C. T. Ngo, J. K. Eshraghian and J. -P. Hong, "A Reconfigurable SRAM Based CMOS PUF With Challenge to Response Pairs," in IEEE Access, vol. 9, pp. 79947-79960, 2021

Reconfigurable SRAM-based PUF (An Example)



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

Reconfigurable SRAM-PUF (CRP Space Calculation)



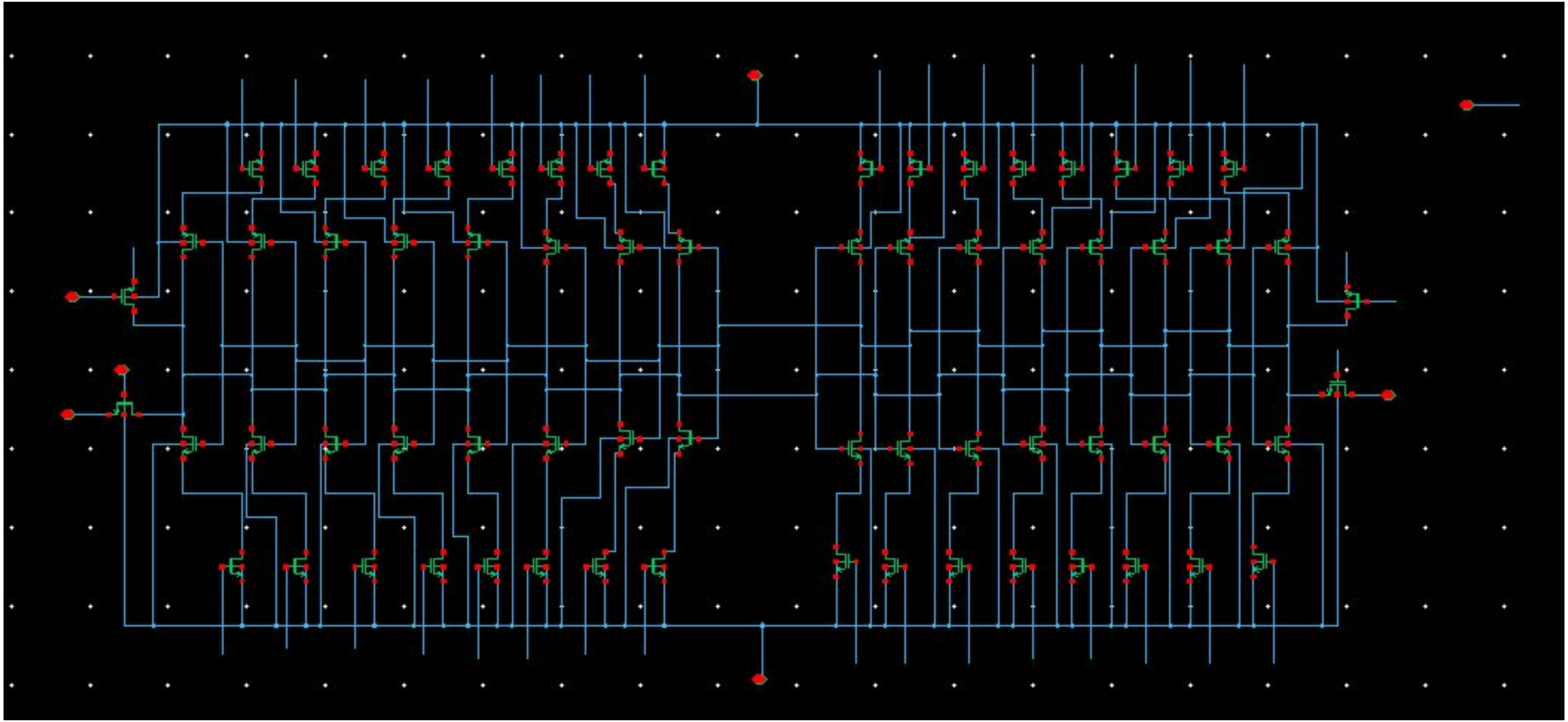
$$
\begin{aligned}
\mathrm{N_N}\ (\text{or } \mathrm{N_P}) &= \text{No. of NMOS (or PMOS) making up the inverter on each side} \\
\mathrm{N_N}\ (\text{or } \mathrm{N_P}) &= 1,\ \text{No. of CRPs} = 1 \\
\mathrm{N_N}\ (\text{or } \mathrm{N_P}) &= 2,\ \text{No. of CRPs} = 2 \times 2 + 1 = 5 \\
\mathrm{N_N}\ (\text{or } \mathrm{N_P}) &= n\ (\text{or } p),\ \text{No. of CRPs} = ({}^{n}C_1)^2 + ({}^{n}C_2)^2 + \ldots + ({}^{n}C_{n-1})^2 + ({}^{n}C_n)^2 = \sum_{k=1}^{n} ({}^{n}C_k)^2 \qquad (1)
\end{aligned}
$$

$$
\begin{aligned}
\text{Bitwidth of challenge in a cell} &= (2\times\mathrm{N_N}+2\times\mathrm{N_P})\ \text{bits} \\
\text{Assuming } \mathrm{N_N} = \mathrm{N_P},\ \text{Bitwidth of challenge} &= (4\times\mathrm{N_N})\ \text{bits} \qquad (2) \\
\text{No. of transistors in a cell} &= 8\times\mathrm{N_N}+4 \qquad (3) \\
\text{Total No. of CRPs} &= \Big(\sum_{k=1}^{\mathrm{N_N}} ({}^{\mathrm{N_N}}C_k)^2\Big)^2 \qquad (4)
\end{aligned}
$$

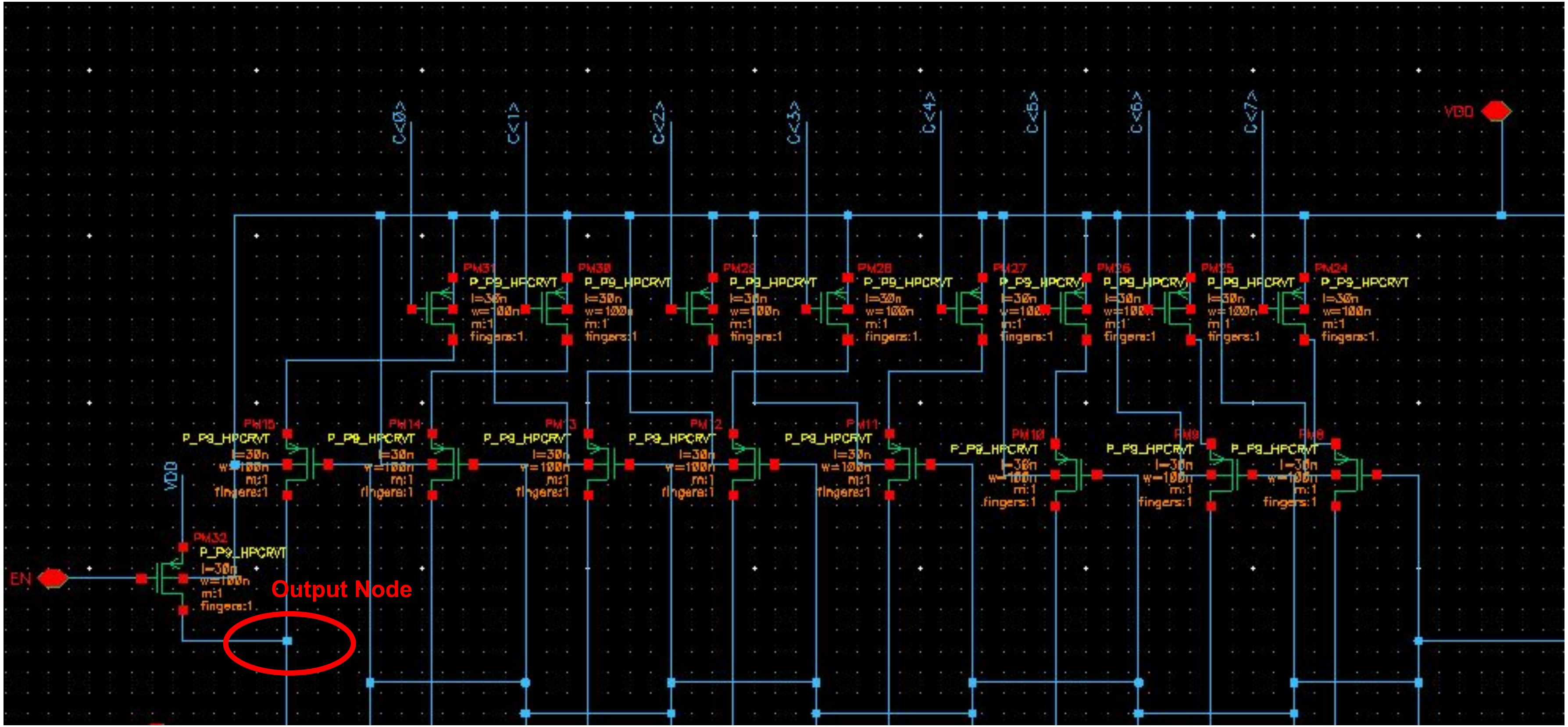
$$
\begin{aligned}
\text{Actual value for } \mathrm{N_N} = \mathrm{N_P} = 8,\ \text{Bitwidth of challenge} &= 32\ \text{bits} \\
\text{Total No. of CRPs} &= \Big(\sum_{k=1}^{8} ({}^{8}C_k)^2\Big)^2 \approx 1.6 \times 10^8 \qquad (5)
\end{aligned}
$$

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)

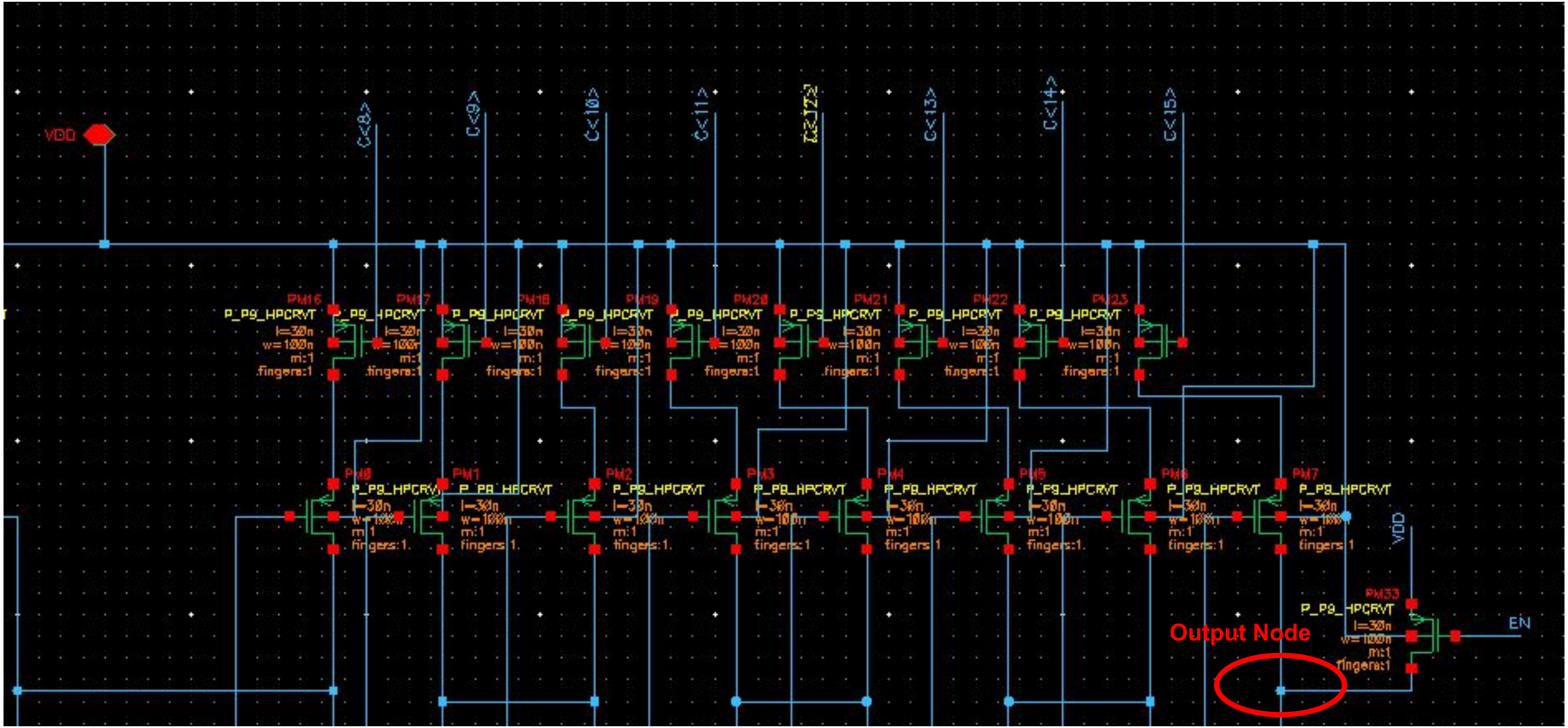


Schematic (Top Left of Cell)



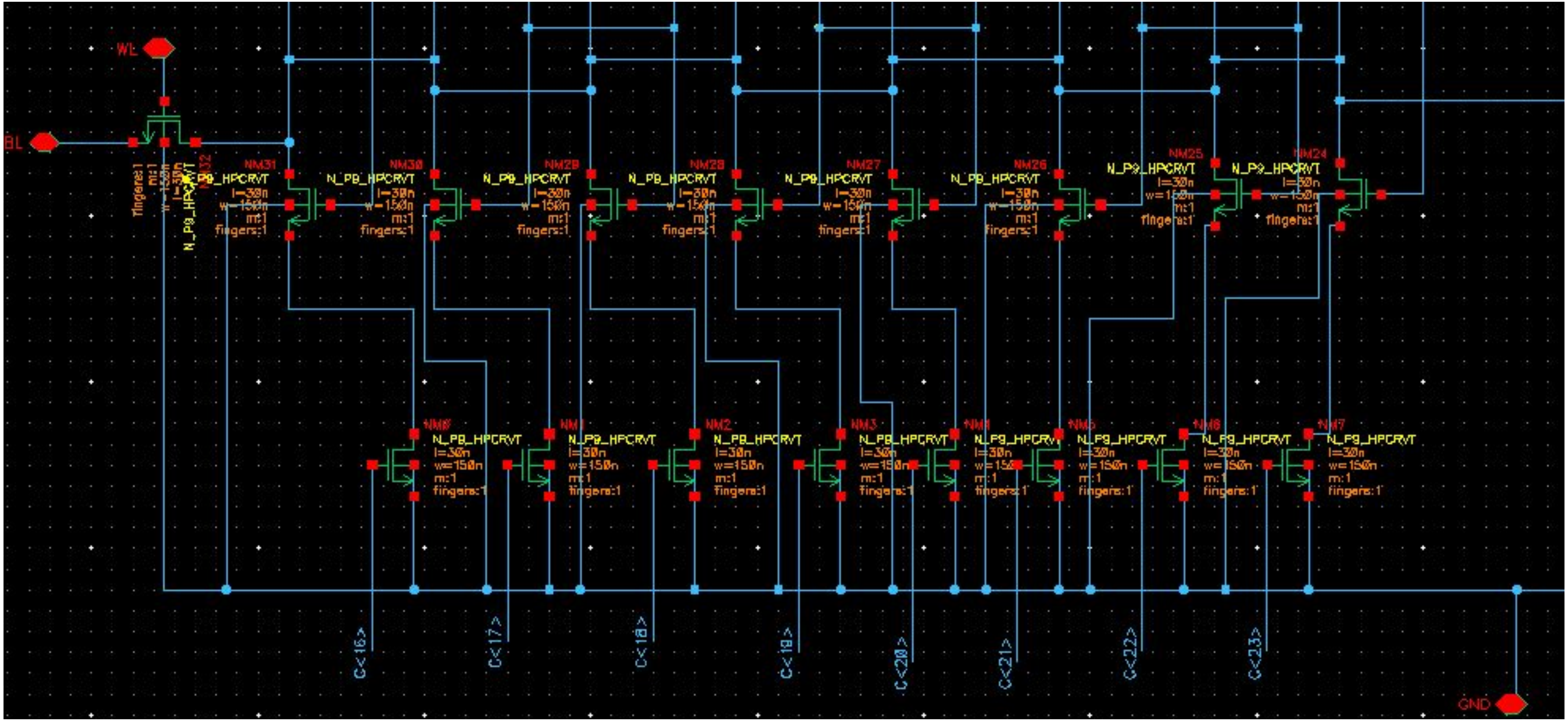
Output Node

Schematic (Top Right of Cell)

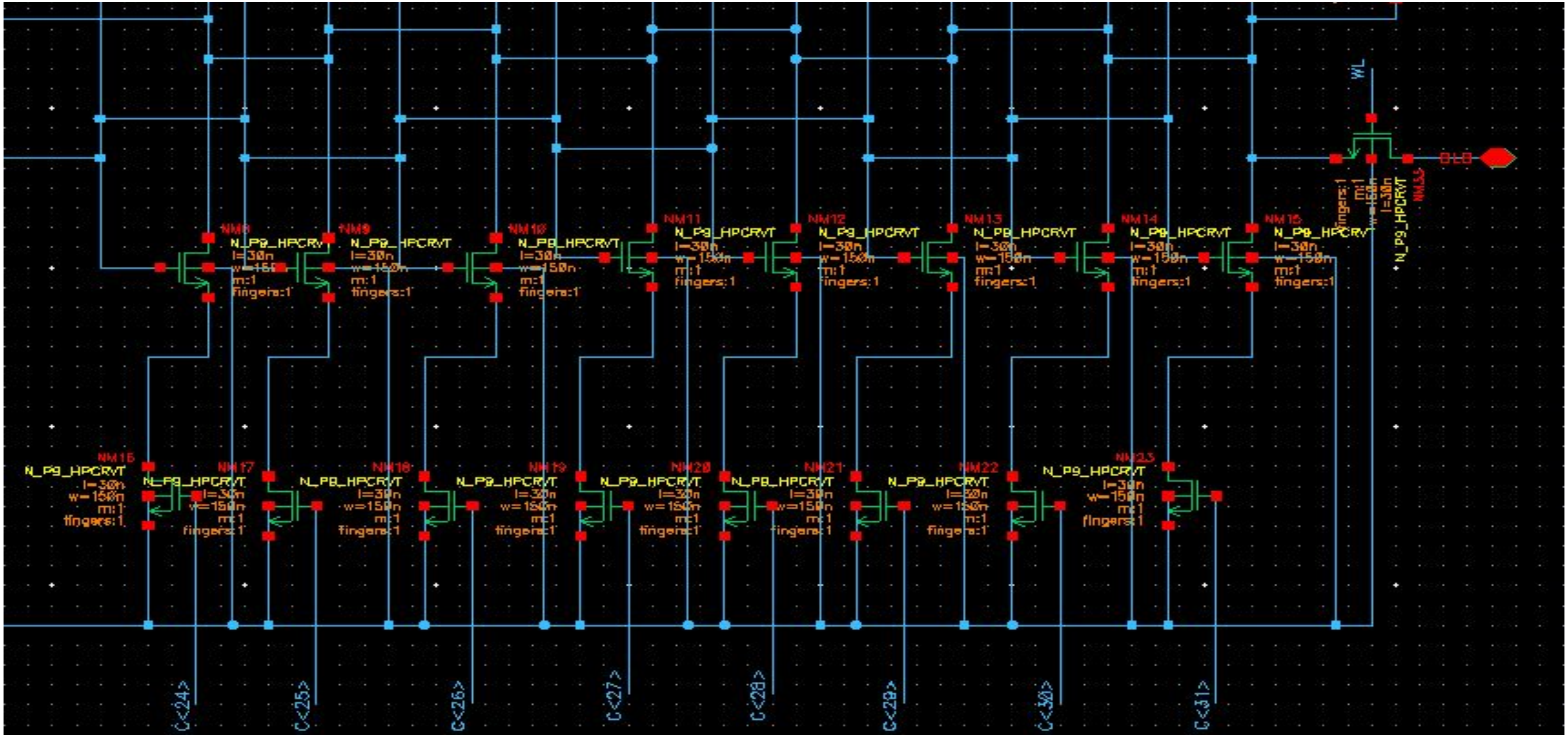


Output Node

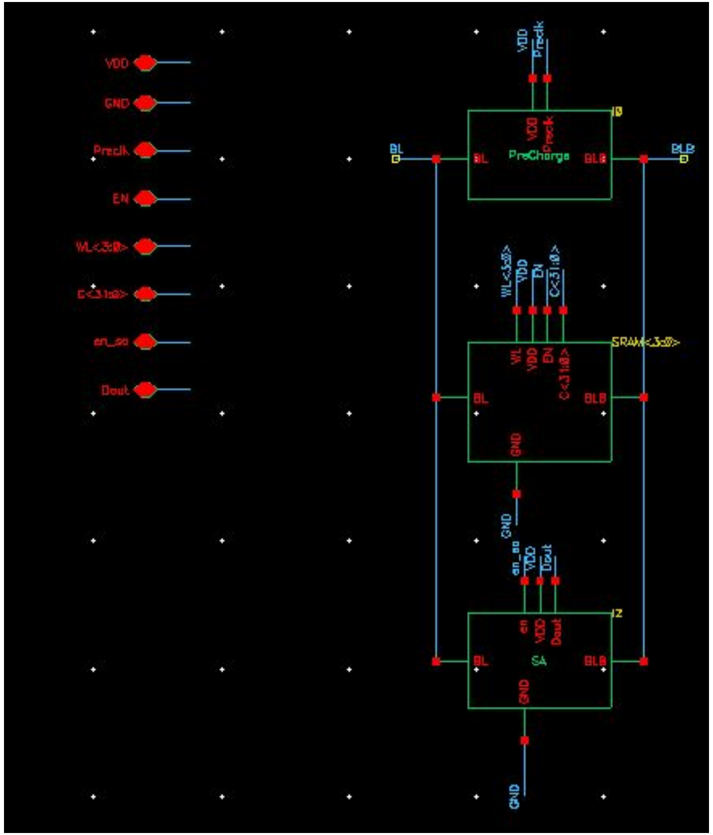
Schematic (Bottom Left of Cell)



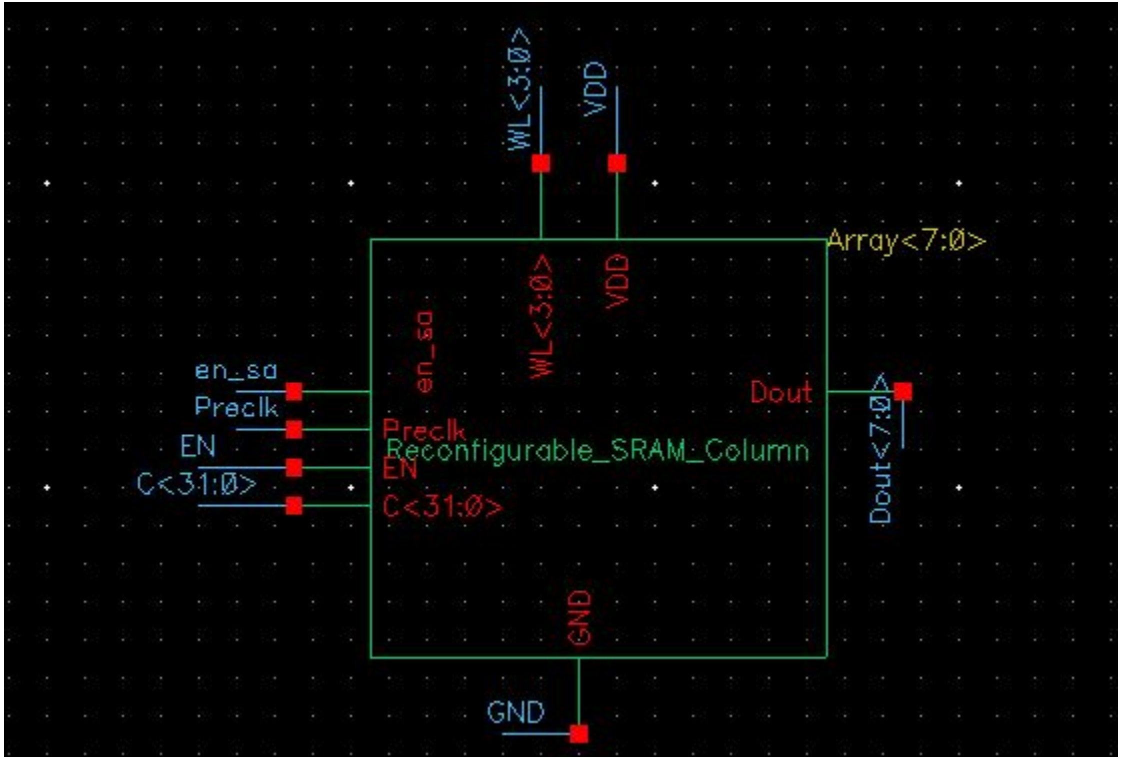
Schematic (Bottom Right of Cell)



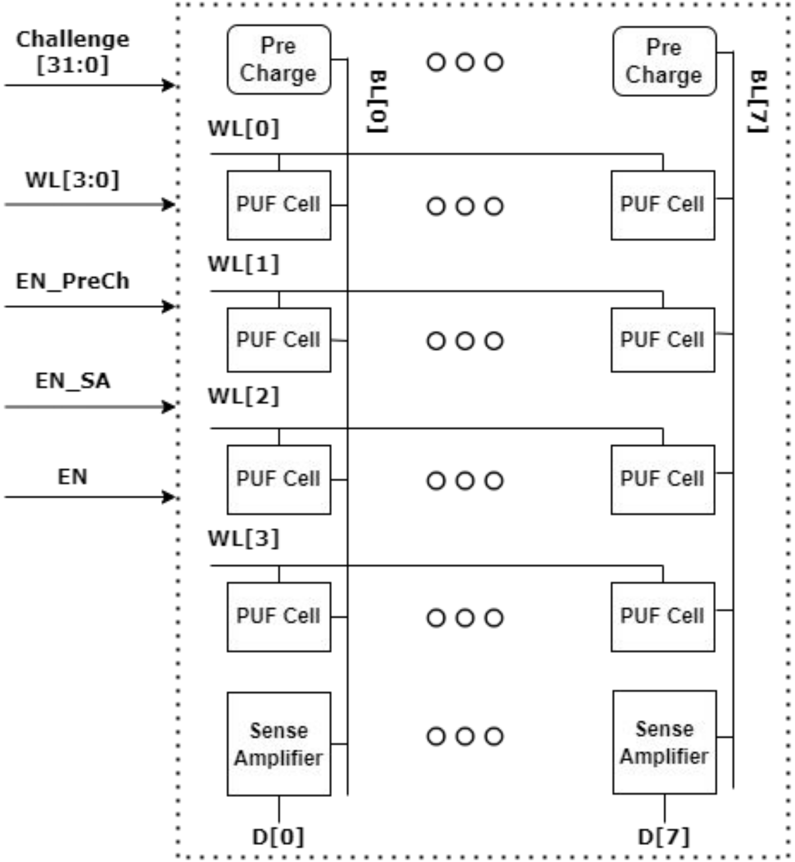
Schematic (SRAM-PUF Column)



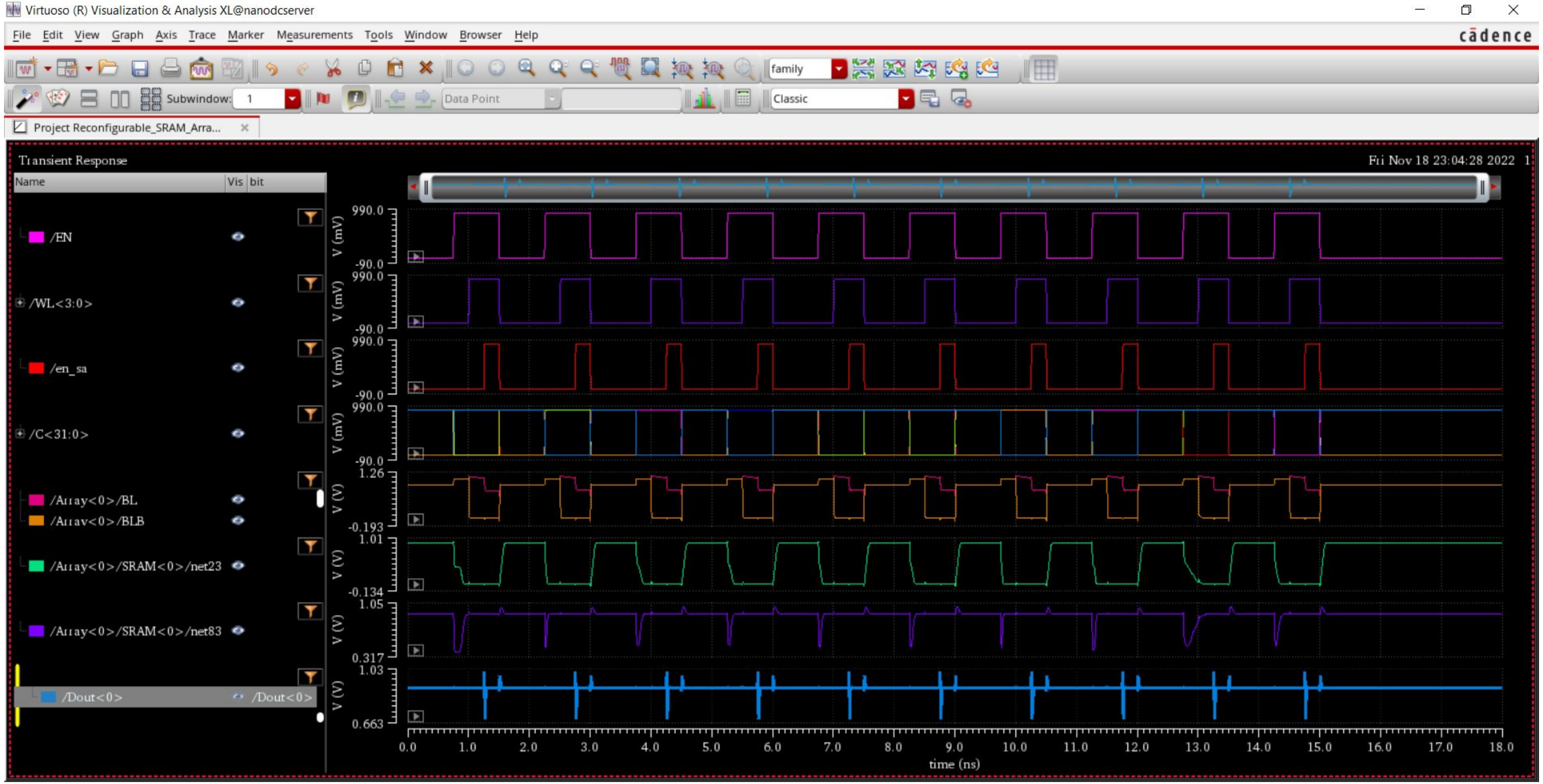
Schematic (SRAM-PUF Array)



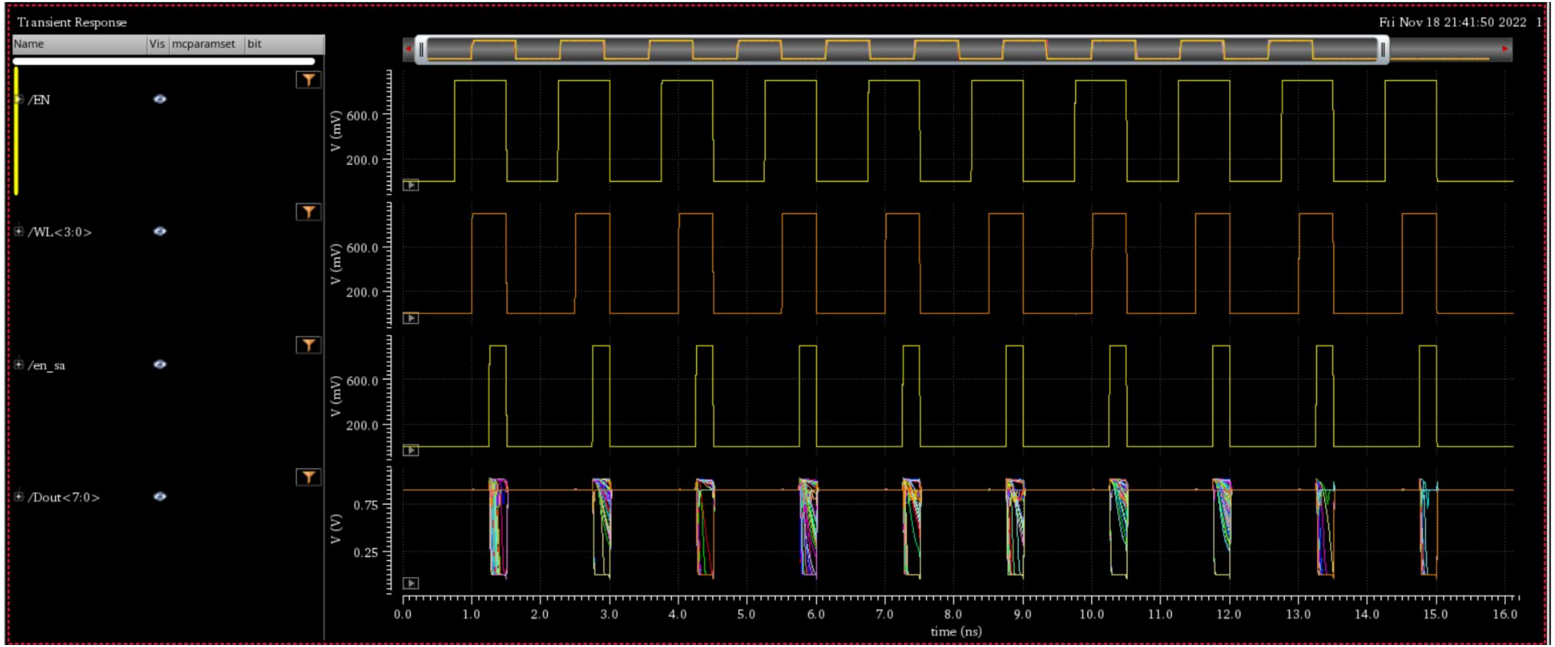
Circuit Implementation



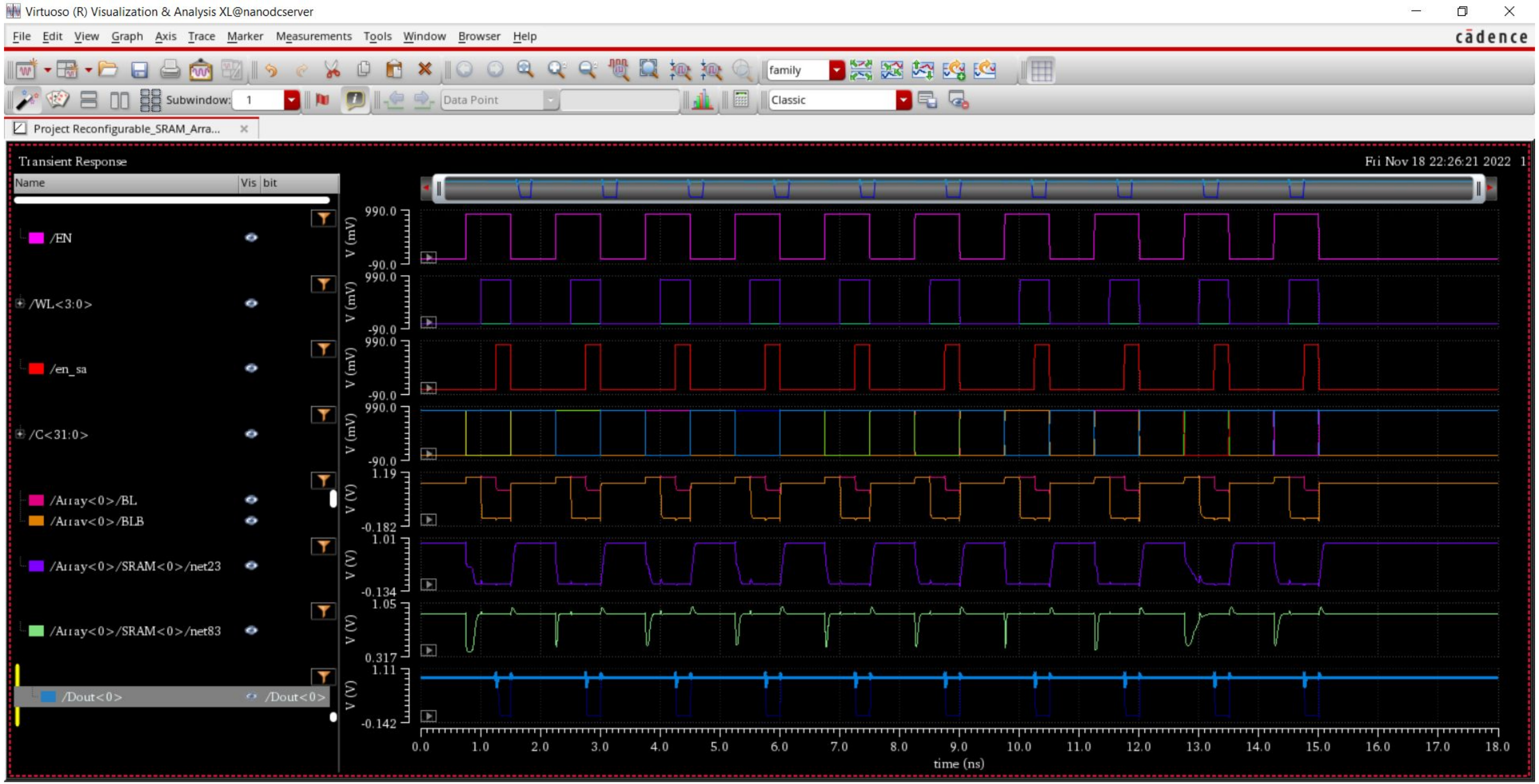
Simulations (ALL WL ON)



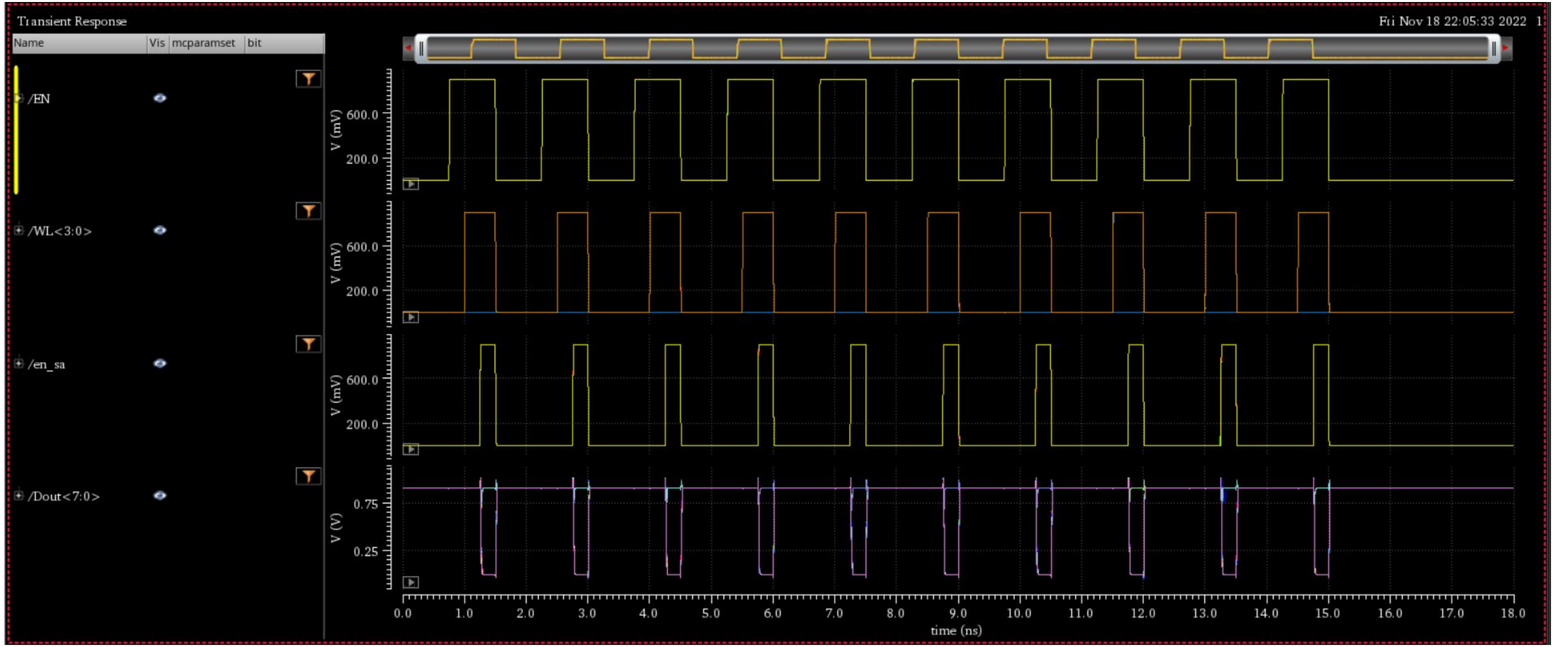
Simulations (20 Monte Carlo ALL WL ON)



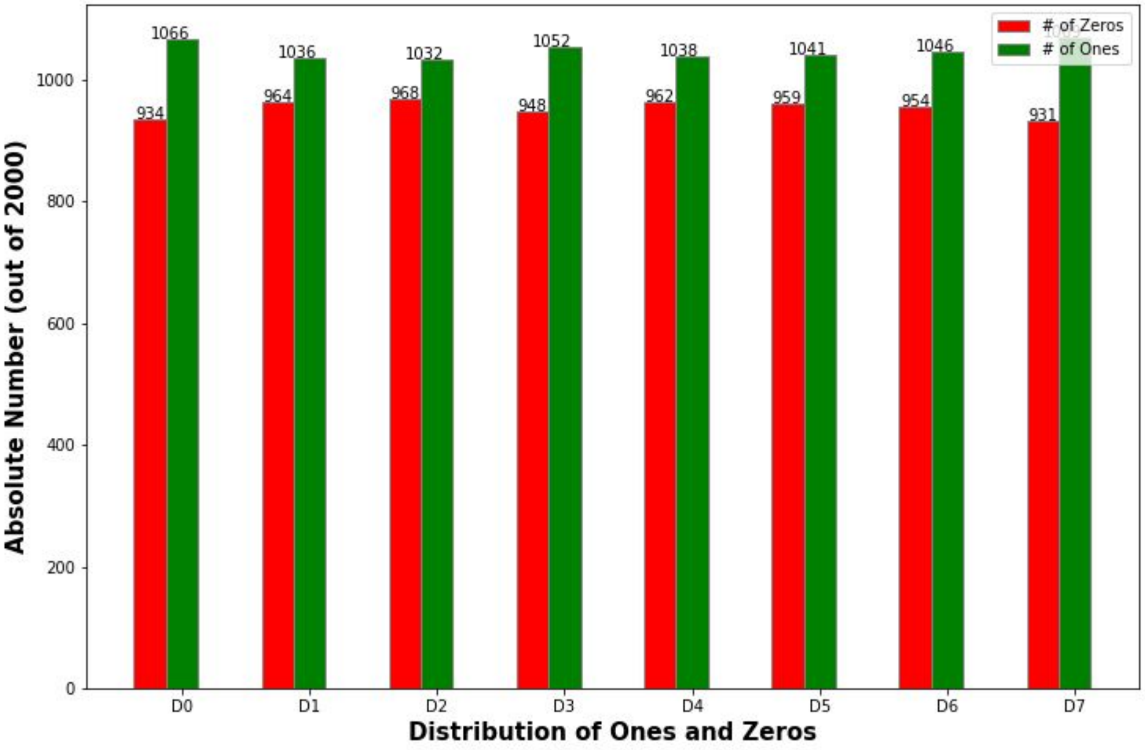
Simulations (1 WL ON)



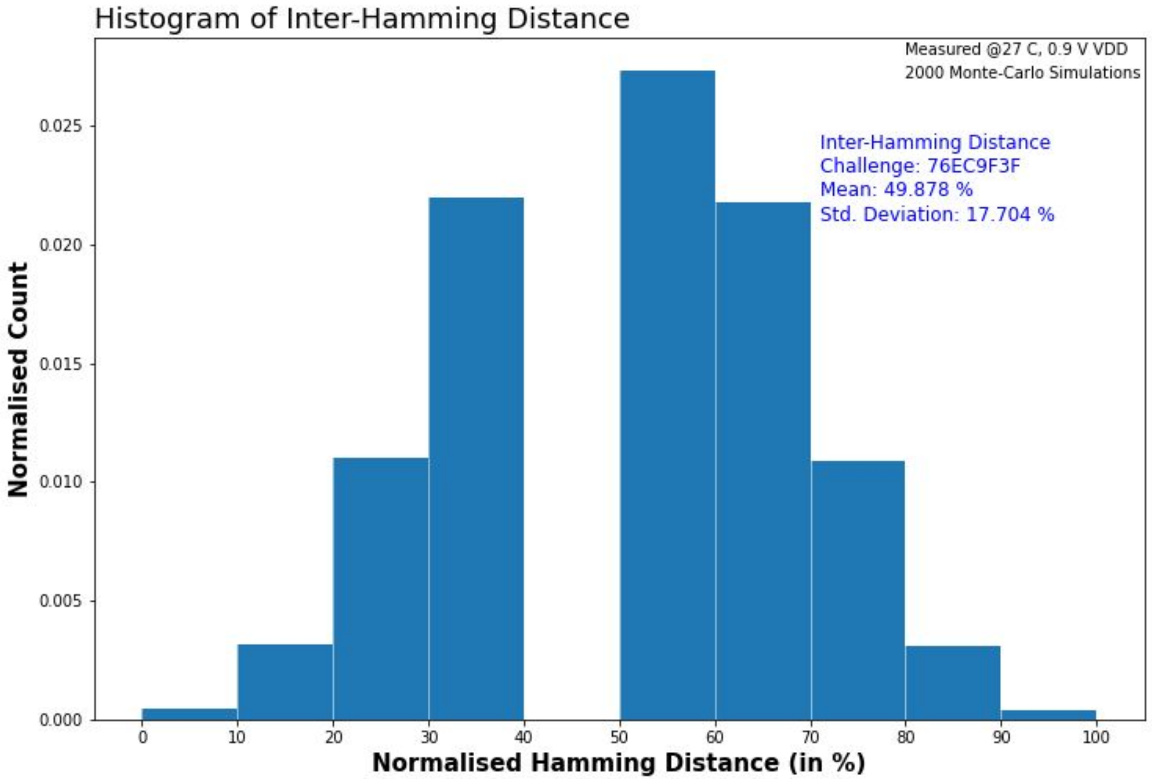
Simulations (20 Monte Carlo 1 WL ON)



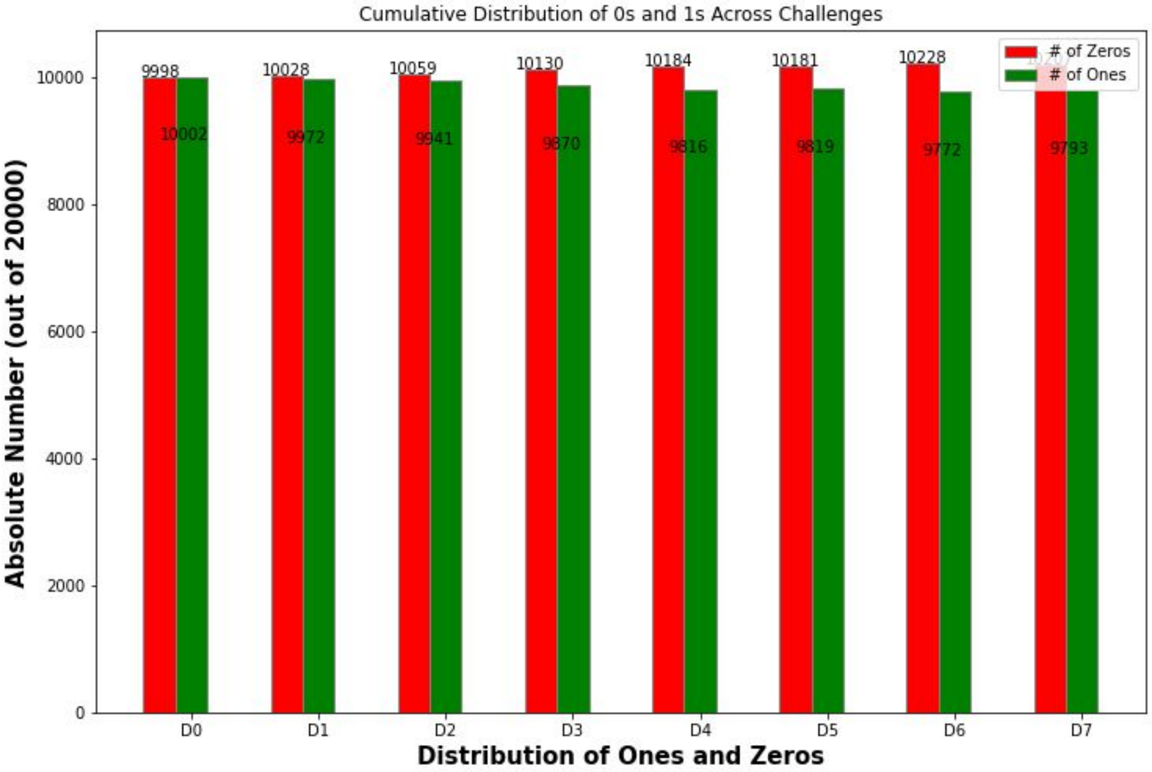
Results (Hamming Weight for One Challenge)



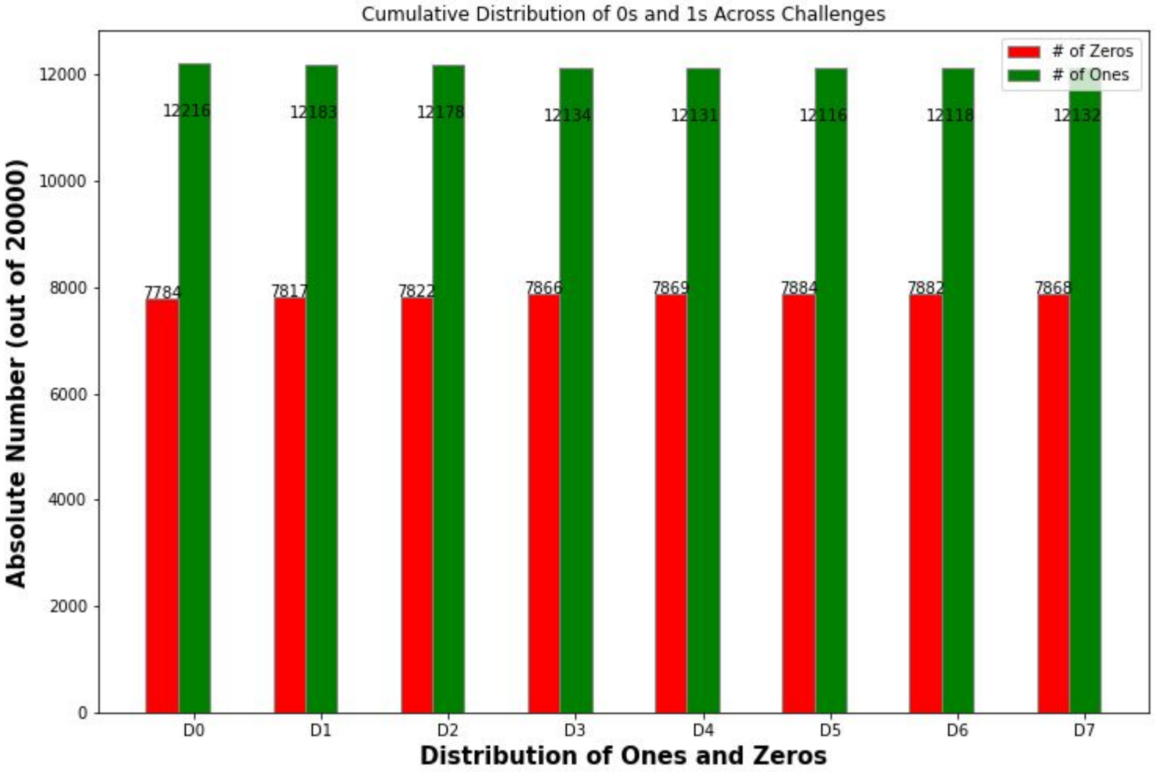
Results (Inter-Hamming Distance for One Challenge)



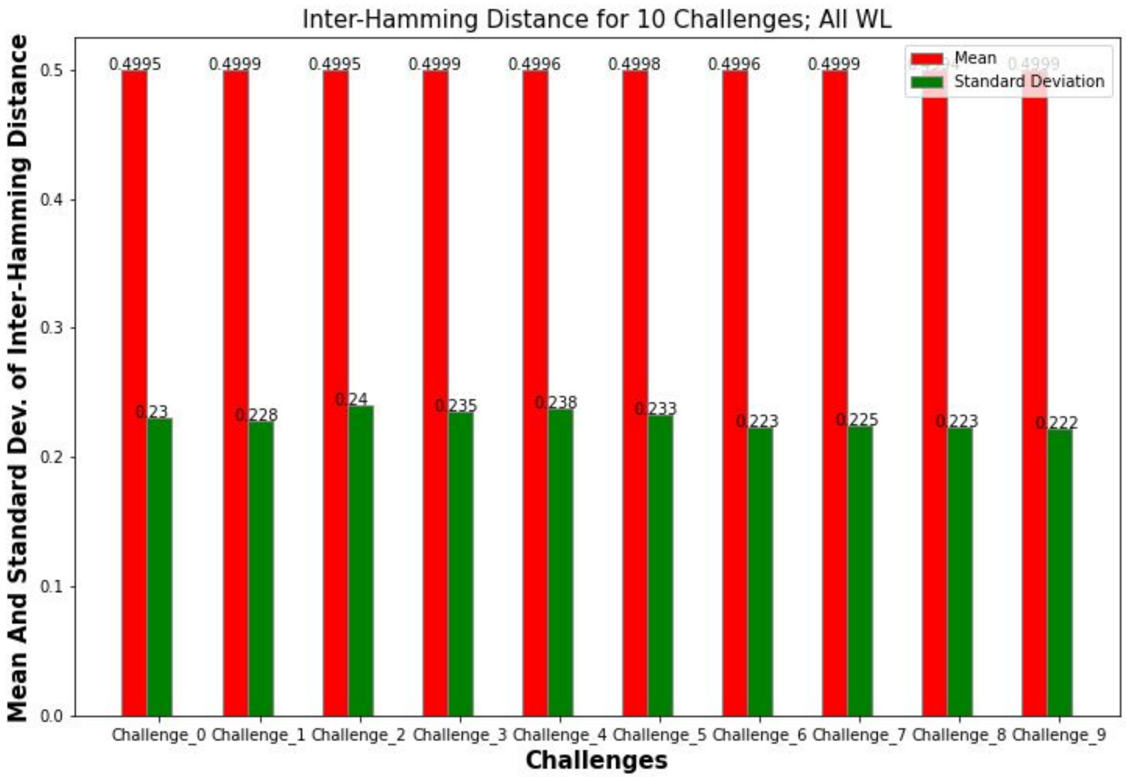
Results (Hamming Weight with all WL ON)



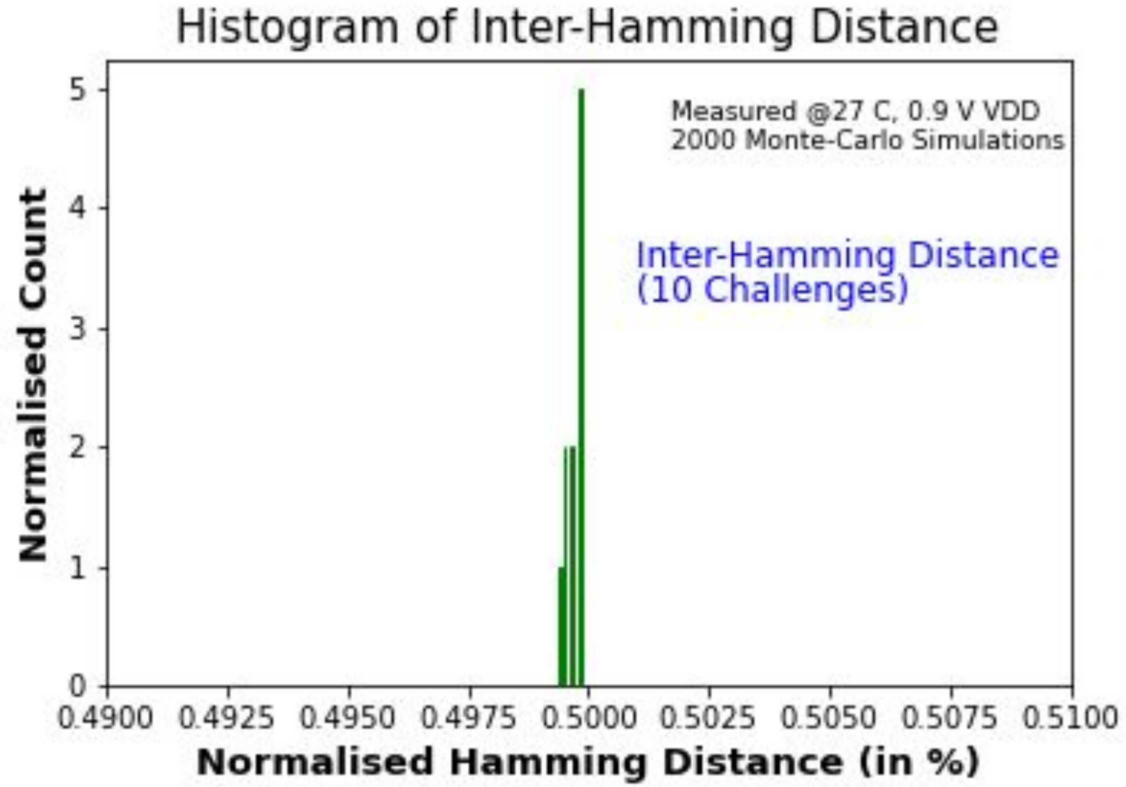
Results (Hamming Weight with one WL ON)



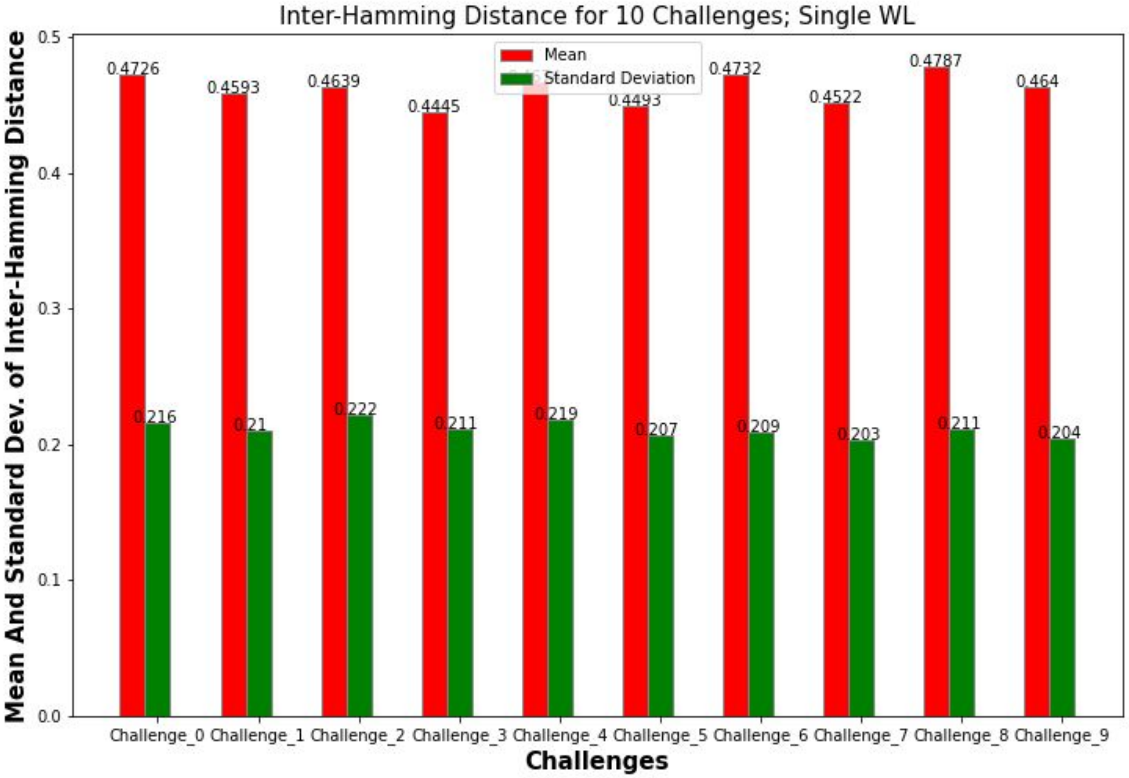
Results (Inter-Hamming Distance with all WL ON)



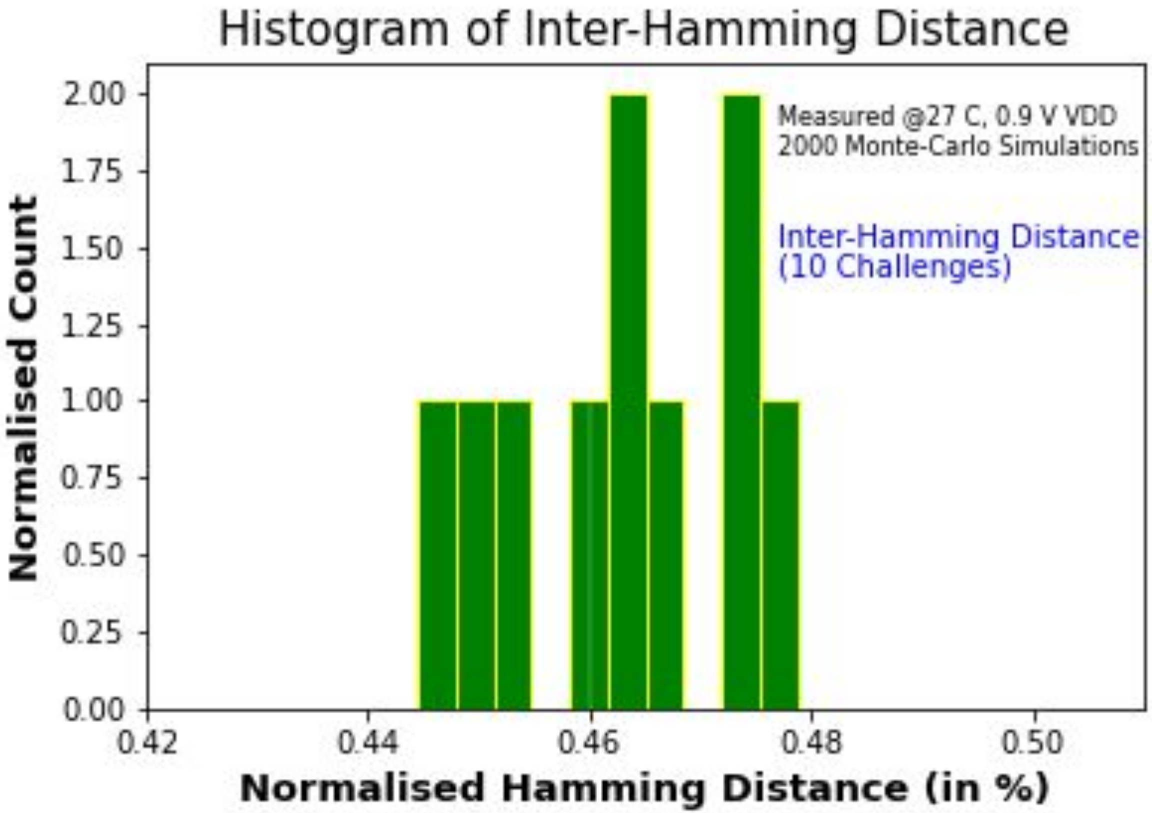
Results (Inter-Hamming Distance with all WL ON)



Results (Inter-Hamming Distance with one WL ON)



Results (Inter-Hamming Distance with one WL ON)



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

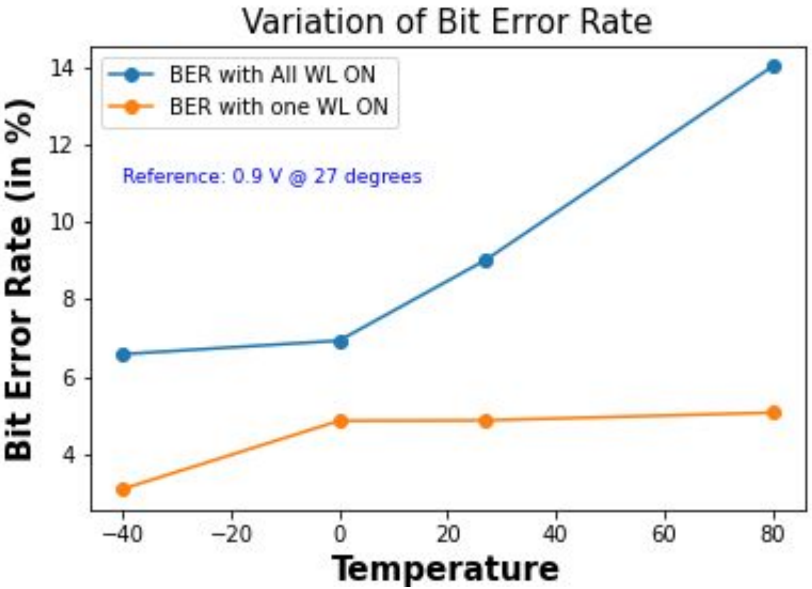
11 Out of 15 Tests Passed !

Results (BER)

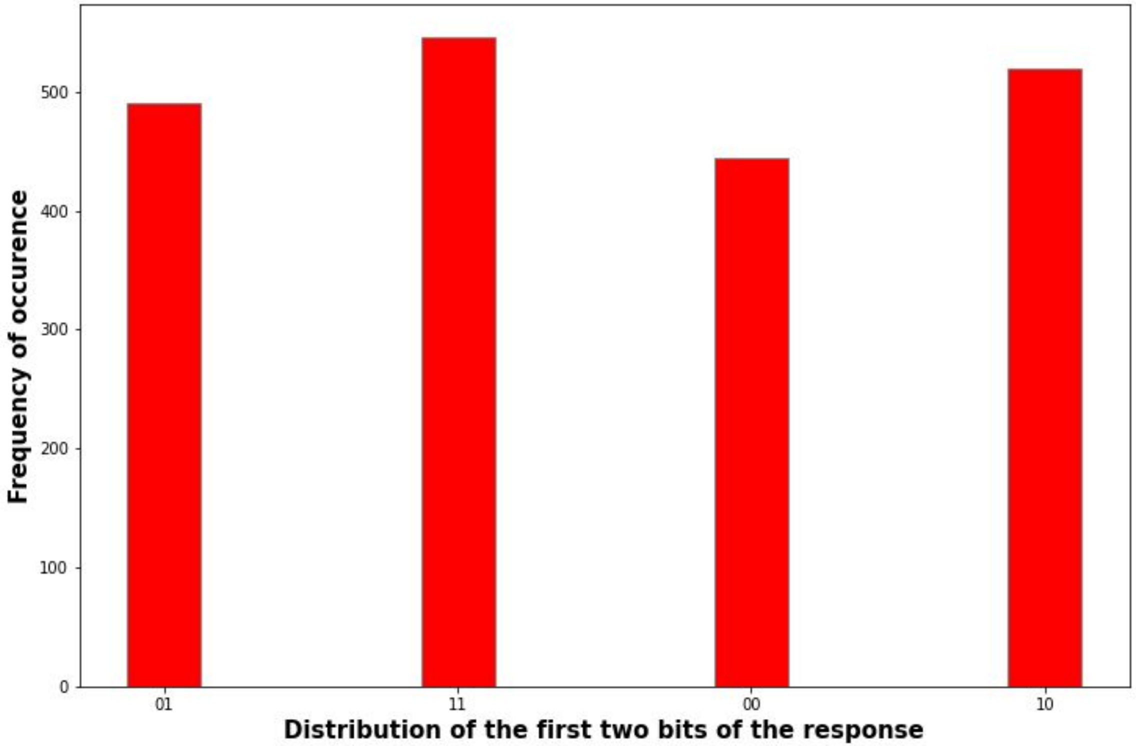
- The worst case bit error was calculated when the supply voltage was increased by 10 %, that is, made 99 mV and temperature was made 80^o C.

- Challenge was kept the same when calculating BER.

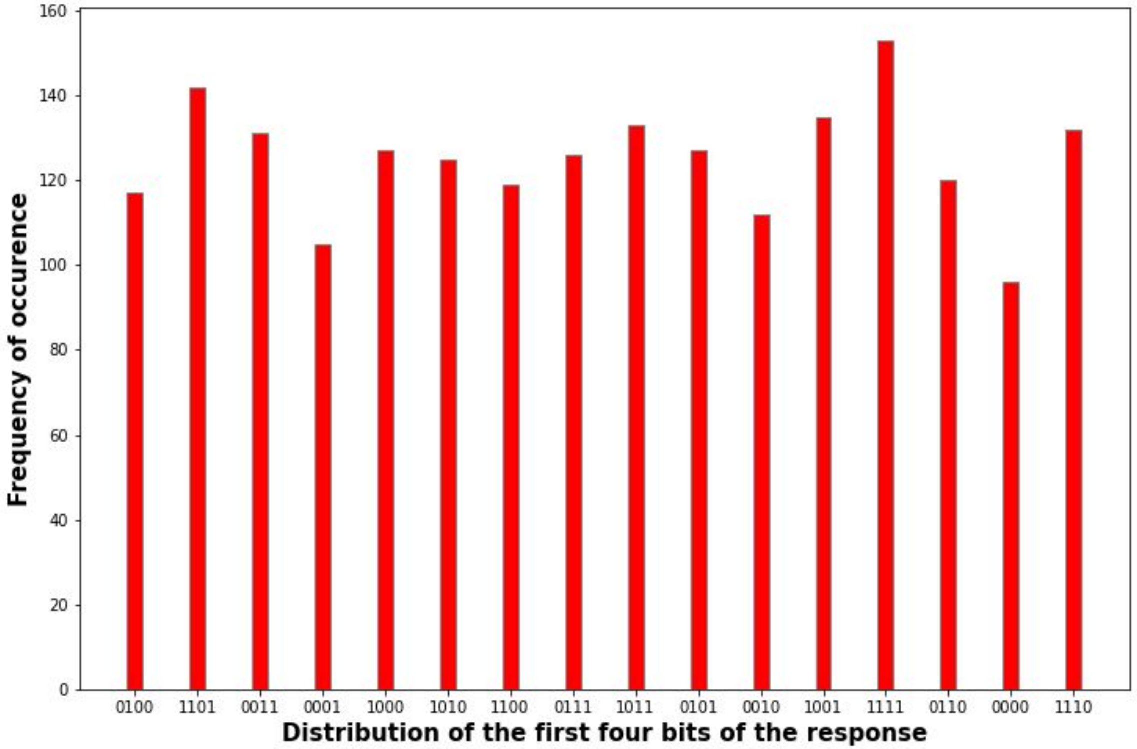
- The worst case BER in this case is found to be 14.01% when all WL are ON and 5.07% when only one WL is ON ! (Reported: 13.7 %)



Test of Uniformity (Data Visualization)



Test of Uniformity (Data Visualization)



Thank You!

Any Questions?

Source : Google Images