SoC Security: A Logic Level Methodology to Prevent Differential Power Analysis

- Hemanth Sabbella
- Diljyot Singh

Motivation

Researchers demonstrated a new side channel attack which allow them to steal encryption keys by simply touching a laptop.

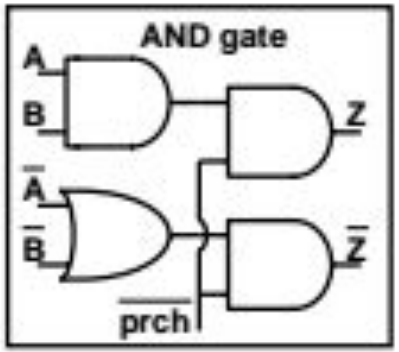
-Workshop on Cryptographic Hardware and Embedded Systems 2014 (CHES 2014) in Korea, on September 23th

Showed that the “ground” electric potential deviates in a computation-dependent way.

They further showed that the signal can also be measured at remote ends of ethernet, USB and VGA cables.

Proposed Methodology

- SDDL(Simple Dynamic Differential Logic)



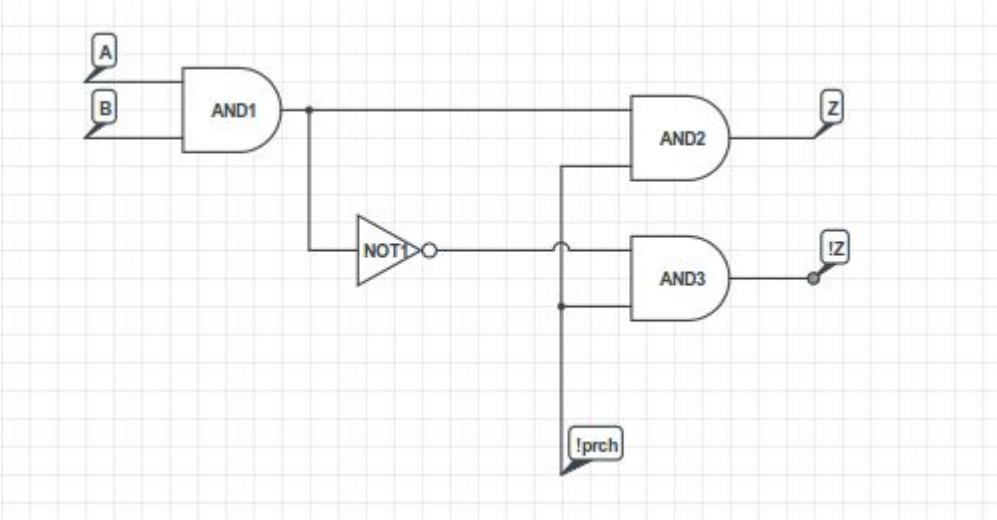
$(A.B).\overline{prch} \leftrightarrow (\bar{A}+\bar{B}).prch$

A	B	$\bar{A}$	$\bar{B}$	prch	Z	$\bar{Z}$
0	0	1	1	0	0	1
0	1	1	0	0	0	1
1	0	0	1	0	0	1
1	1	0	0	0	1	0
X	X	X	X	1	0	0

Source[1]

Modified Methodology

- IDL(Inversion Dynamic Logic)

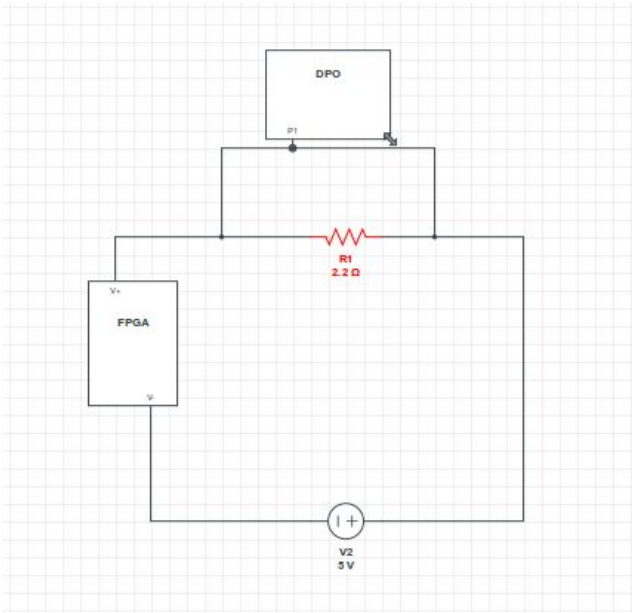


FPGA Implementation

- The power consumption of the device/hardware changes for every logic transition since the amount of current consumption changes.
- The power consumption can be measured by the doing the side channel attack or connecting a resistor in series with the power supply of the FPGA and probing the voltage across the resistor using a DPO/DSO since power is directly proportional to V series.

FPGA Implementation

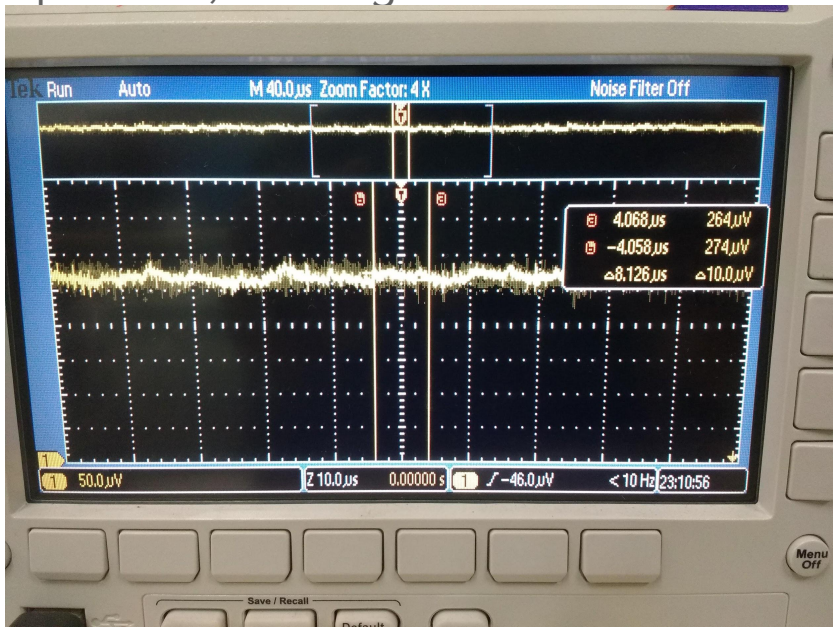
- Side channel attack on FPGA:



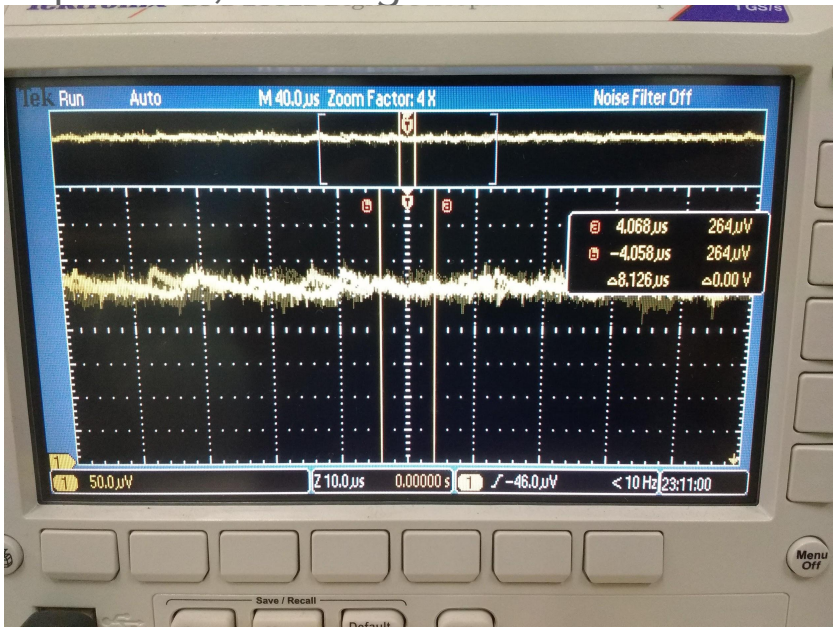
Results

Proposed Methodology:

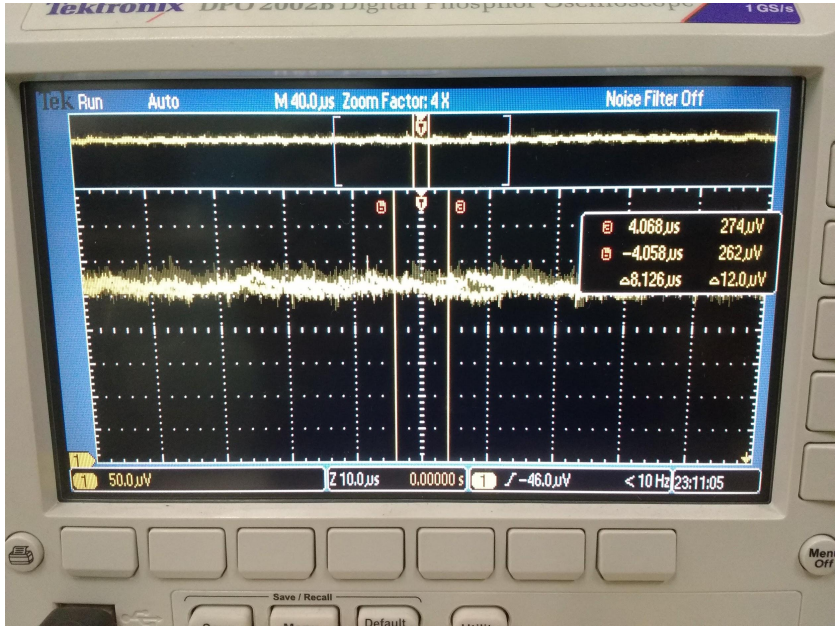
Inputs: 00, Preharge: 0



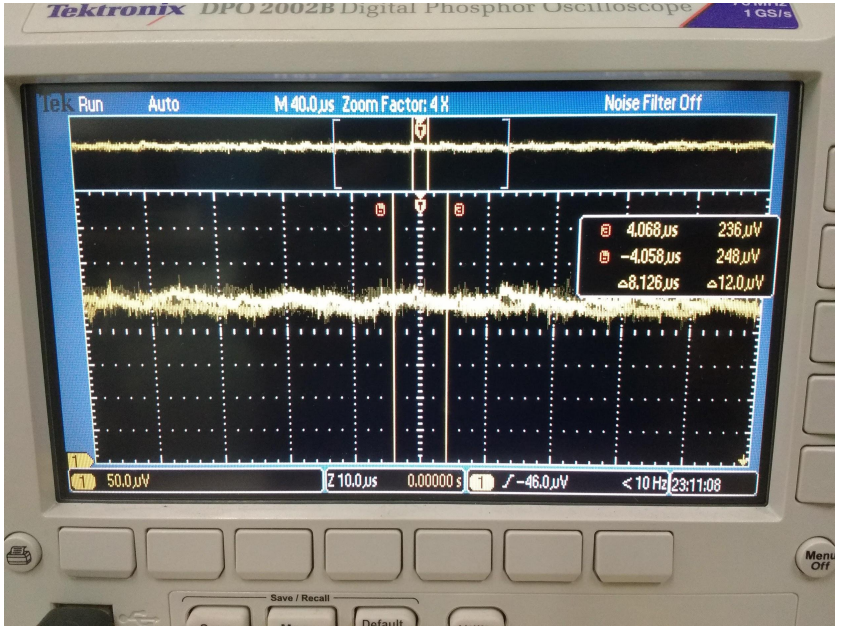
Inputs: 01, Preharge: 0



Inputs: 11, Precharge: 0

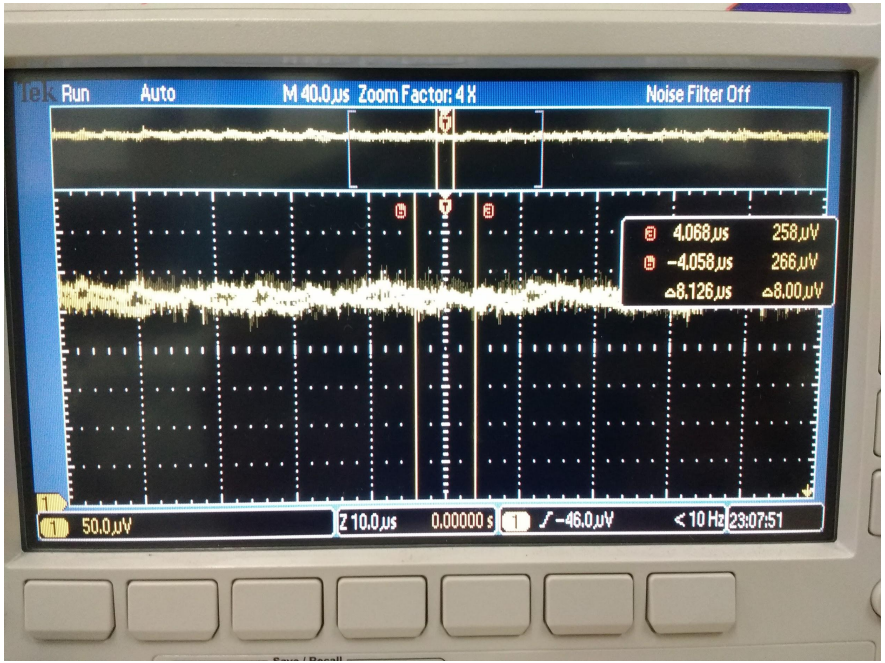


Inputs: 11, Precharge: 1

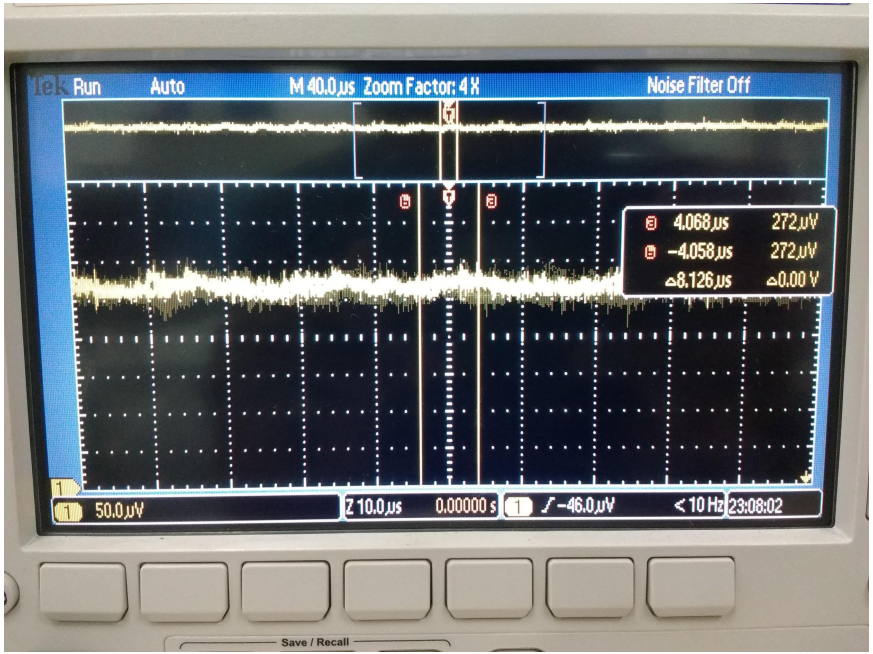


Modified Methodology:

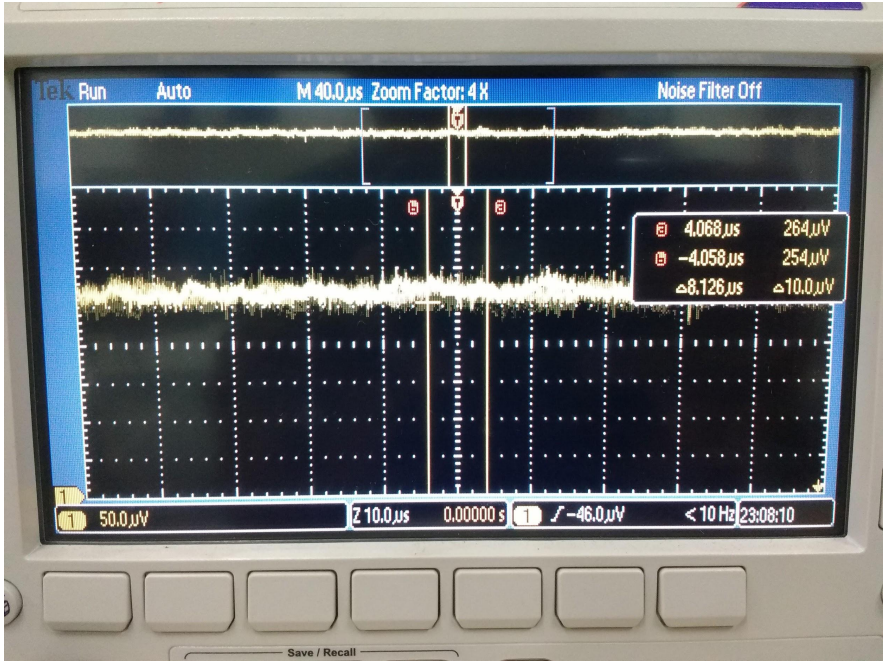
Inputs: 00, Precharge: 0



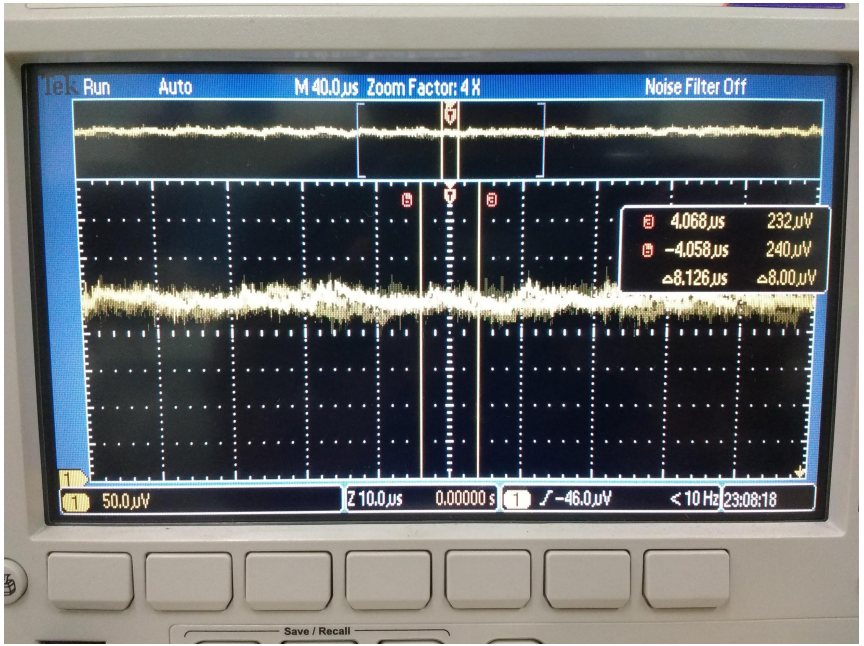
Inputs: 01, Precharge: 0



Inputs: 11, Precharge: 0



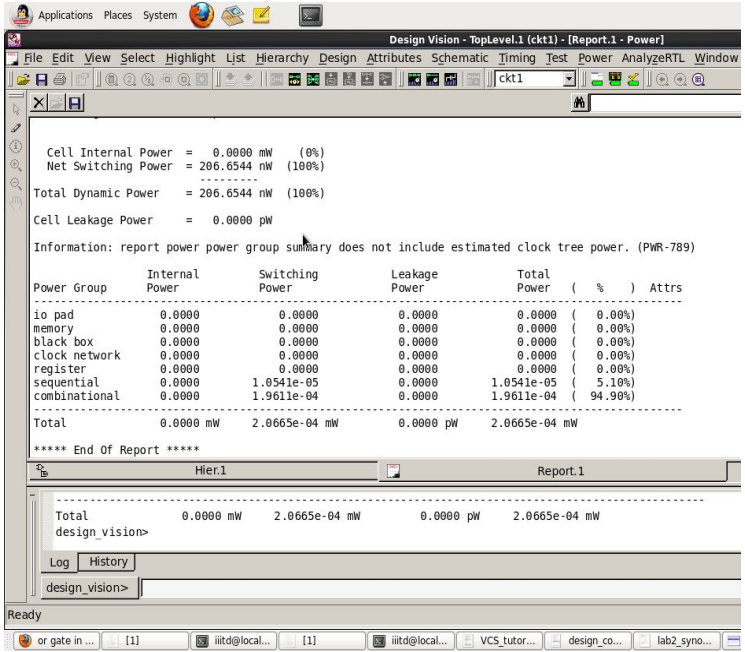
Inputs: 11, Precharge: 1



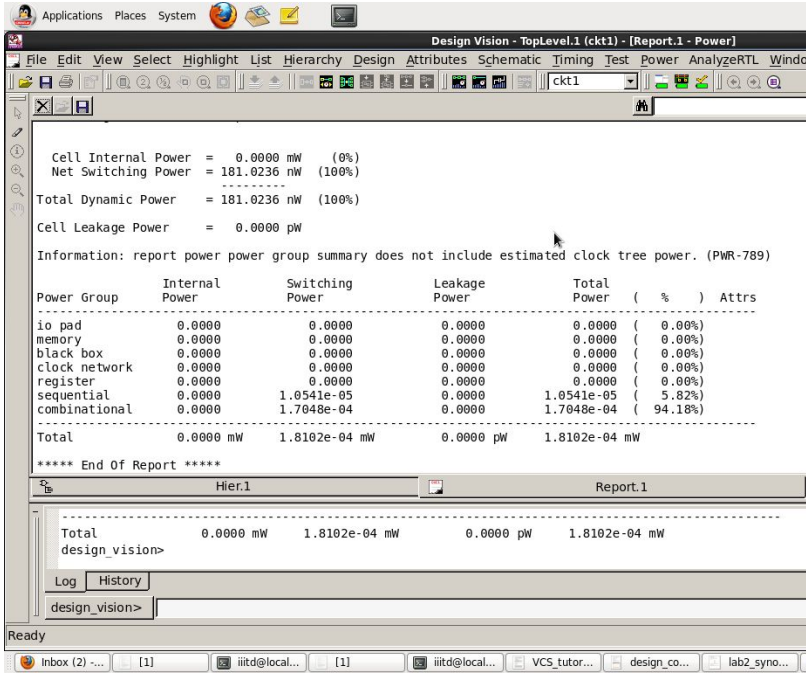
Evaluation

Power:

Proposed Methodology:

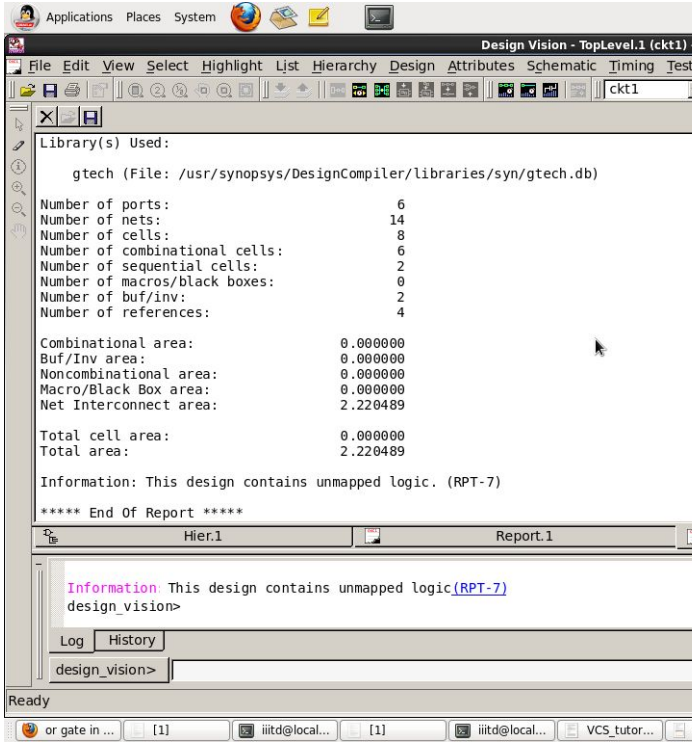


Modified Methodology:

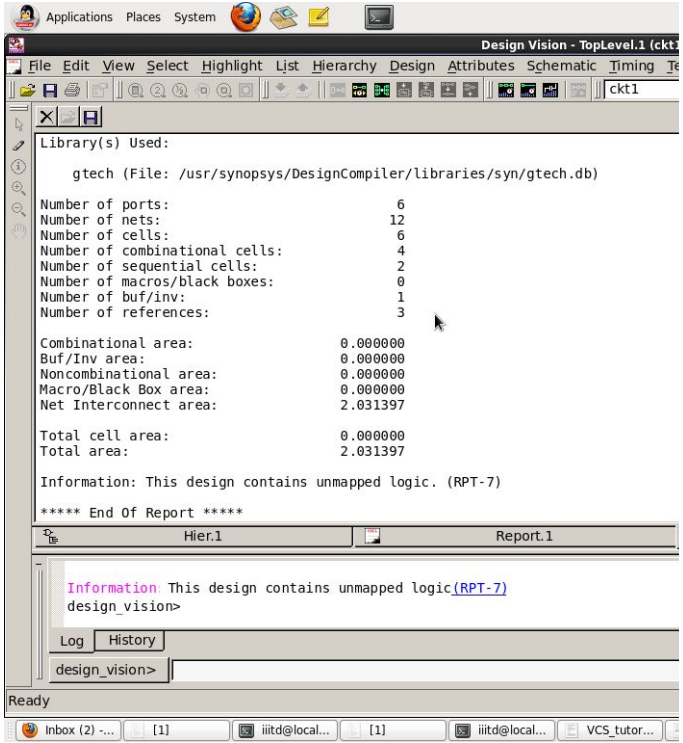


Area:

Proposed Methodology:



Modified Methodology:



Conclusion

- Implemented SDDL methodology.
- Optimized the methodology using the inversion logic.
- Implemented the above methodologies on FPGA and did a side channel attack to know the power consumption.
- Evaluated both the designs using Synopsys for power and area consumption.
- Future work:
    - This may be extended to implement on a larger environment and see how performance varies.

References

[1] A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation Kris Tiri and Ingrid Verbauwhede UCLA Electrical Engineering Department, 7440B Boelter Hall, P.O. Box 951594, Los Angeles, CA 90095-1594

Thank you!