ENSC 450
Final Project: SoC Integration

Daimon Gill
Siavash Rezghi
Zi Zhou (John) Qu

For Dr. Anita Tino and Sheida Alan

Final Project Purpose

- Perform an full hierarchical P&R system design
- Amend chosen core to interface with given bus design
- Create testbenches for given IPs and overall system
- Perform front end design including synthesis using DC shell for overall system
  - Chose operating frequency
  - Obtain design reference Verilog file
- Perform back end design including P&R using Cadence Innovus
  - Chose core density
  - Obtain design final Verilog file
- Test final Verilog file to match behavioral VHDL file in system testbench

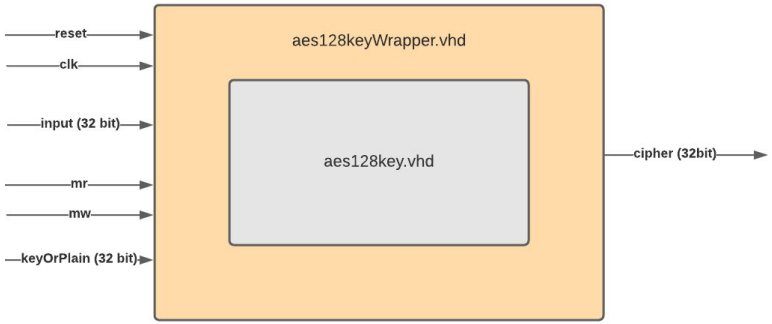
AES-128 Encryption Core

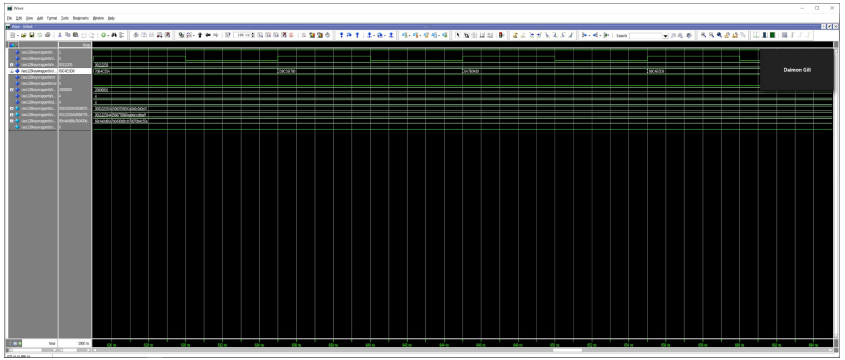
- Takes 2 128-bit vectors as inputs
  - a vector as plaintext data
  - a vector as encryption key
- Performs AES-128 encryption on plaintext based on FIPS 197 standard
  - Performs 10 rounds of substitution and permutation operations to obtain final ciphertext
- Output a 128-bit encrypted codeword

AES-128 **Amended** Encryption Core

- 128-bit IO reduced to 32-bit IO
  - Input and output conducted over 4 clock cycles (32-bit * 4 = 128-bit)
- Interface with MR and MW control signals
  - Read when MR = 1, write when MW = 1
- Interface with 32-bit BUS:
  - Key or plain accumulate within buffers (4 cycles), assert load signal
  - Pass 128-bit buffers to aes128key, reset counters and load
  - After computation, cipher accumulated in output buffer
  - Output buffer sent to bus in 4 cycles

```
-- Instantiate the Unit Under Test (UUT)
uut: aes128key PORT MAP (
        reset => nreset,
        clock => clock,
        empty => empty,
        load => load,
        key => keyBuffer,
        plain => plainBuffer,
        ready => ready,
        cipher => cipherBuffer
        );
nreset <= not reset;
```





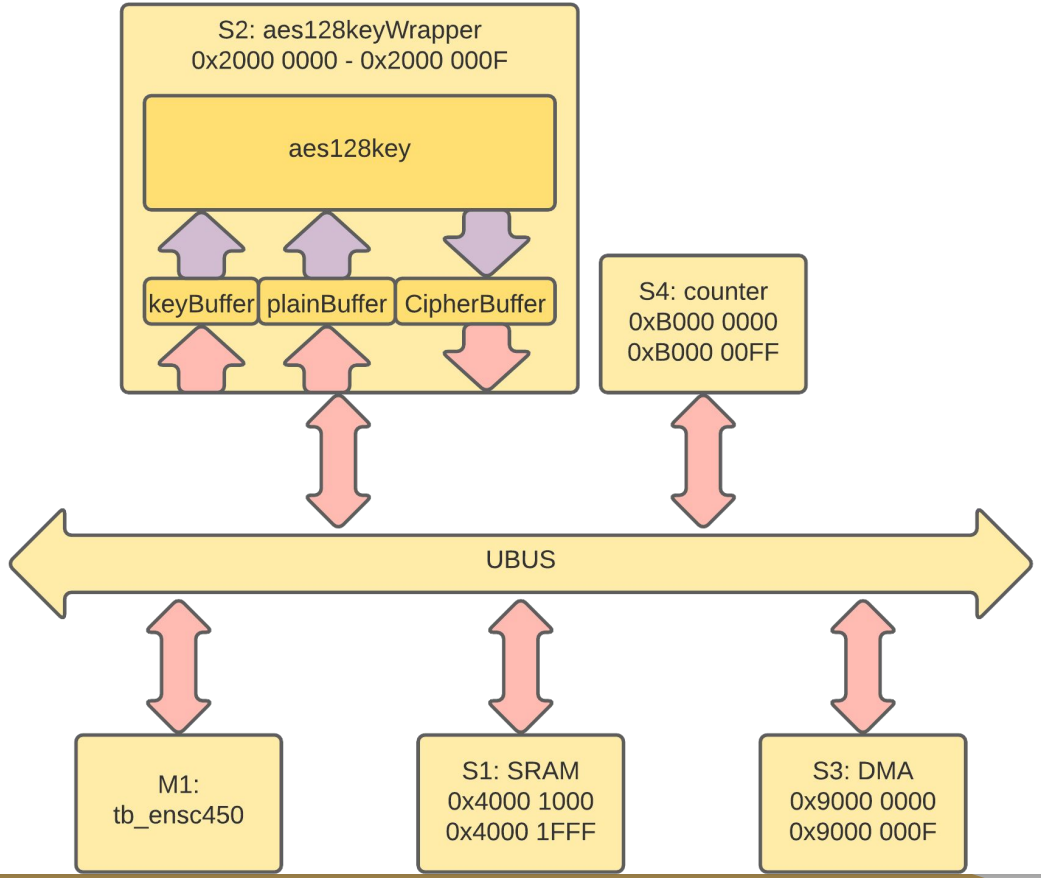
Soc System and Integrated Core

- DMA gets the data from the testbench into the SRAM
- Data from the SRAM goes towards the core
- Computation takes place in the core
- Computed data will sent back to the SRAM

Testbench Scenarios:

1. EXT port → bus → read and write to/from core
2. CPU writes to SRAM → core reads data from SRAM → computation → write back to SRAM (manually)
3. CPU writes to SRAM → core reads data from SRAM → computation → write back to SRAM (using DMA)

System Diagram



Core Synthesis Front-End Results

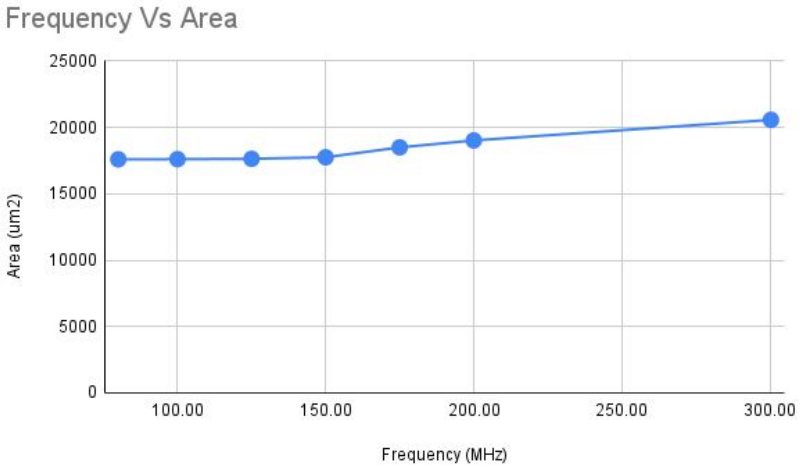
- Increasing area has frequency increased
- Power increased substantially as frequency increased
- **Target Frequency**: 175 MHz
  - 0.17 ns slack

```
Startpoint: keyOrPlain[23]
            (input port clocked by clock)
Endpoint: plainCount_reg[6]
          (rising edge-triggered flip-flop clocked by clock)
Path Group: clock
Path Type: max

Des/Clust/Port     Wire Load Model       Library
------------------------------------------------
aes128keyWrapper   SK_hvratio_1_1        NangateOpenCellLibrary

Point                                  Cap      Trans      Incr       Path
-----------------------------------------------------------------------------
clock clock (rise edge)                                    0.00       0.00
clock network delay (ideal)                                0.00       0.00
input external delay                                       0.80       0.80 f
keyOrPlain[23] (in)                 1.79       1.00       0.00       0.80 f
U5368/ZN (INV_X1)                   1.98       0.17       0.32       1.12 r
U5468/ZN (AND2_X2)                  1.92       0.03       0.14       1.26 r
U5467/ZN (AND2_X2)                  1.92       0.02       0.09       1.35 r
U5506/ZN (NAND2_X1)                 1.80       0.05       0.05       1.40 f
U5470/ZN (NOR2_X1)                  1.26       0.05       0.12       1.52 r
U5469/ZN (AND2_X1)                  1.92       0.03       0.11       1.63 r
U5491/ZN (AND2_X2)                  1.98       0.02       0.09       1.72 r
U5463/ZN (AND2_X2)                  1.88       0.02       0.09       1.82 r
U5462/ZN (NAND2_X1)                 1.82       0.04       0.04       1.86 f
C5482/ZN (OR2_X2)                   1.17       0.07       0.19       2.05 f
U5353/ZN (OR2_X1)                   1.17       0.07       0.21       2.26 f
U5352/ZN (OR2_X1)                   1.80       0.07       0.22       2.48 f
U5360/ZN (NOR2_X1)                  1.92       0.21       0.14       2.62 r
U5516/ZN (NAND2_X1)                 1.80       0.05       0.09       2.71 f
U5510/ZN (NOR2_X1)                  1.25       0.19       0.12       2.83 r
U5509/ZN (AND2_X1)                  1.98       0.03       0.16       3.00 r
U5511/ZN (AND2_X2)                  1.92       0.03       0.10       3.09 r
U5512/ZN (NAND2_X1)                 1.17       0.04       0.05       3.14 f
U5355/ZN (OR2_X1)                   1.17       0.07       0.20       3.34 f
U5354/ZN (OR2_X1)                   1.82       0.07       0.22       3.56 f
C5493/ZN (OR2_X2)                   3.72       0.07       0.21       3.77 f
U5513/ZN (OR2_X2)                   3.12       0.03       0.21       3.98 f
I_7/ZN (INV_X2)                     3.33       0.02       0.07       4.05 r
U5517/ZN (AND3_X4)                 29.06       0.07       0.18       4.23 r
U5514/ZN (INV_X16)                268.30       0.04       0.28       4.51 f
U74/ZN (NAND2_X1)                   1.95       0.04       0.11       4.62 r
U5443/ZN (INV_X1)                   3.12       0.02       0.05       4.66 f
U5444/ZN (INV_X2)                  84.01       0.35       0.40       5.06 r
U253/Z (MUX2_X1)                    1.34       0.03       0.30       5.36 f
plainCount_reg[6]/D (DFF_X1)                   0.03       0.01       5.37 f
data arrival time                                                    5.37

clock clock (rise edge)                                    5.70       5.70
clock network delay (ideal)                                0.00       5.70
plainCount_reg[6]/CK (DFF_X1)                              0.00       5.70 r
library setup time                                        -0.17       5.53
data required time                                                   5.53
-----------------------------------------------------------------------------
data required time                                                   5.53
data arrival time                                                   -5.37
-----------------------------------------------------------------------------
slack (MET)                                                          0.17
```



Core Synthesis Back-End Results

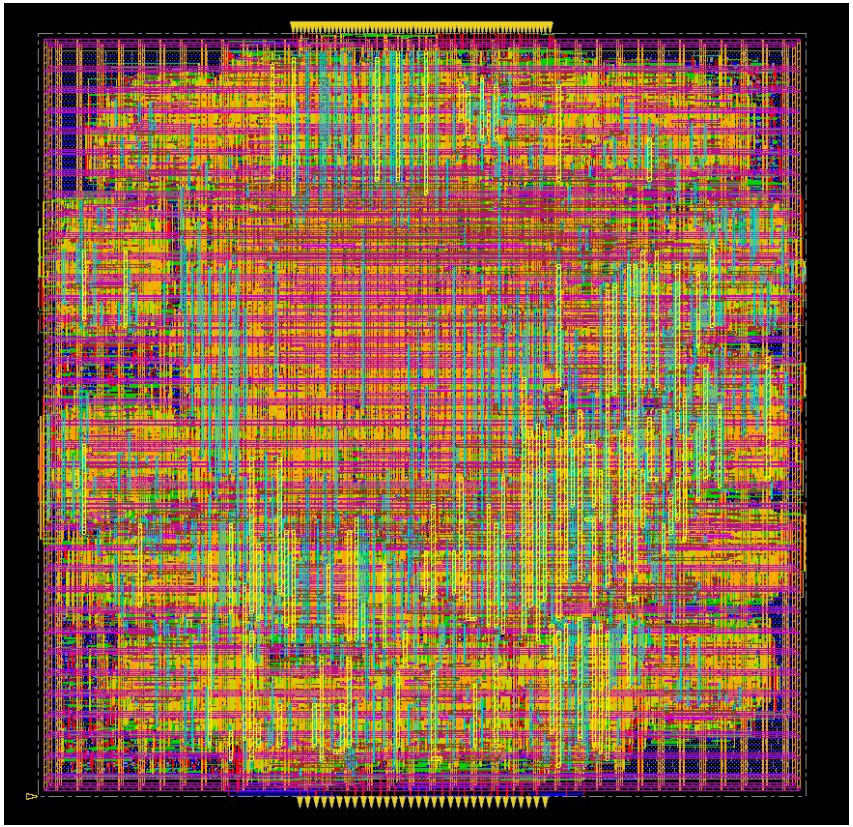
- Densities > 0.7 possessed slack violations
- Densities > 0.7 contained Max Tran and Max Cap violations
- Area decreased as density increased
- **Target Density**: 0.6
- **Target Frequency**: 175 MHz
  - 0.159 ns slack
  - No max tran or max cap violations
  - No timing violations
- Master Script run length: 5.7 minutes
- Critical path contained 71 cells, starts at a control signal port and ends at a internal counter register

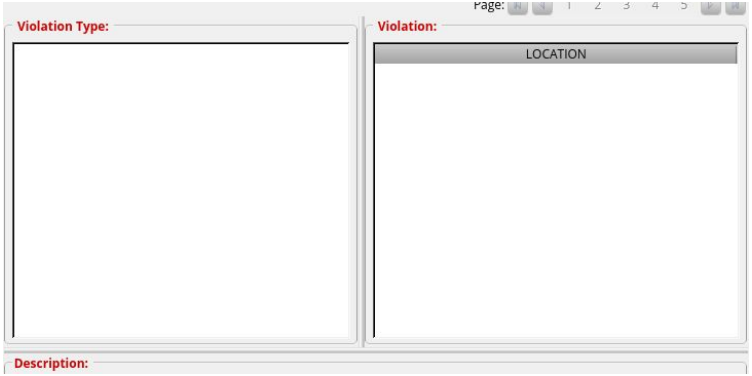
Density	Violations
0.4	None
0.5	None
0.6	None
0/7	Max tran, max cap

Core - Clock Tree

Max Skew	Latency	Number of Levels	Number of Clock Buffers	Number of Sinks
700.6ps	700.6ps - 700.6ps = 0ps	0	3	647

Core - Place and Route





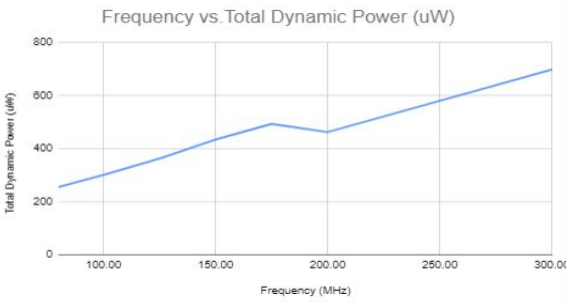
Core Design Specifications

Stage	Area (um2)	Area (KGates)	Frequency (MHz)	Slack (ns)	Power (Avg.) (mW)	Power (VCD) (mW)
Front End	18498.97	23122.5	175.00	0.17	0.8569	1.3582
Back End	30856.00	38570.0	175.00	0.159	3.807	1.2807

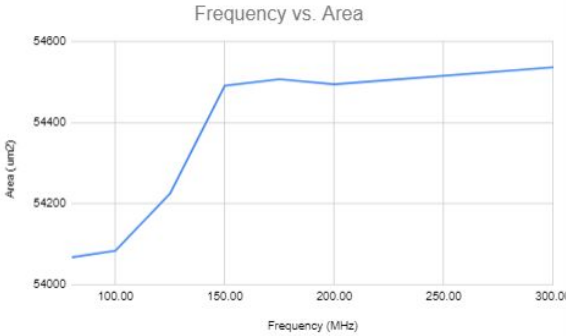
- Simulation was performed after both FE and BE processes to ensure behavior is preserved
- BE implementation is free of violations (DRC, max tran, max cap, timing)
- Degradation in area and power in backend

SoC Integration - Front End

- VHDL and post-synthesis simulations match
- Frequencies > 125 MHz possessed slack violations
- Minimal changes in area due to macros
- Power increased substantially as frequency increased
- **Target Frequency**: 100 MHz
    - 0.24 ns slack

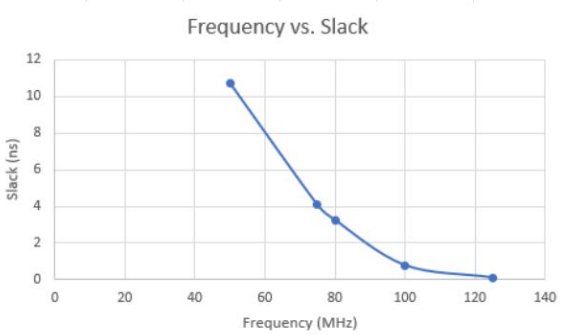


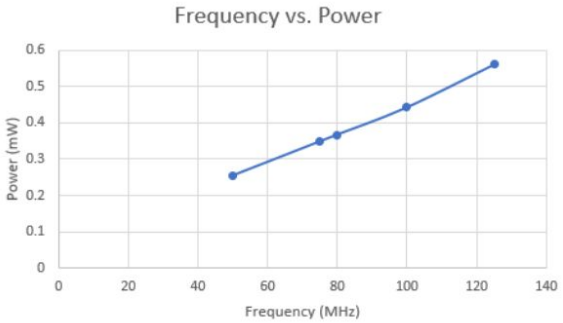
Reference	Library	Unit Area	Count	Total Area	Attributes
DMA_1_32_32		2464.489976	1	2464.489976	h, n
INV_X1	NangateOpenCellLibrary	0.532000	5	2.660000	
INV_X2	NangateOpenCellLibrary	0.798000	2	1.596000	
INV_X4	NangateOpenCellLibrary	1.330000	1	1.330000	
SRAM	SRAM	14884.000000	1	14884.000000	b, d
aes128keyWrapper	aes128keyWrapper	33818.601562	1	33818.601562	d
counter_32_4_1		2235.198009	1	2235.198009	h, n
ubus_32_32_40001000_400017ff_20000000_2000000f_a0000000_a000000f_b0000000_b00000ff		676.437997	1	676.437997	h, n
Total 8 references				54084.313545	



Soc Integration - Back End

- Area remained constant due to macros
- Macros accounted for 17% of core area
- At higher frequencies instances increased, due to clock buffers
- Remained the same otherwise
- Power increased substantially as frequency increased
- **Target Frequency**: 100 MHz
  - 0.768 ns slack
  - No max tran or max cap violations
- Master Script run length: 2.8 minutes



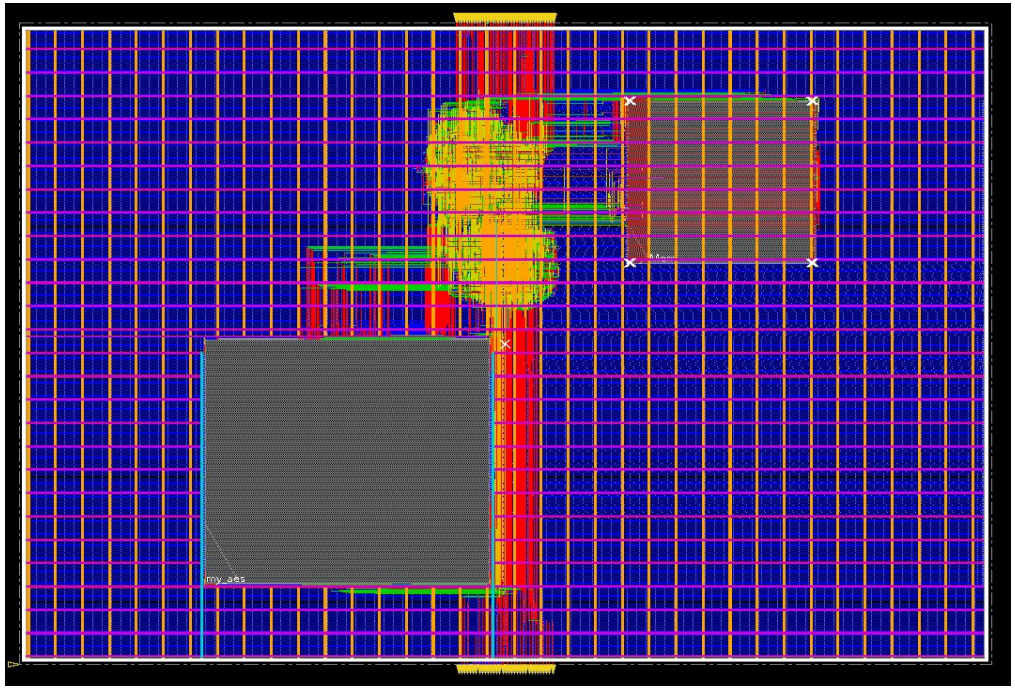


SoC - Clock Tree

Max Skew	Latency	Number of Levels	Number of Clock Buffers	Number of Sinks
1117.6ps	1117.6ps - 1117.6 ps = 0ps	0	3	409

Note: Critical path of the SoC contains the critical path of the core

SoC - Place and Route



Page: 1 2 3 4 5

Violation Type:

- Verify (10/10)
  - Connectivity (10/10)
    - Open (2/2)
    - UnConnPin (8/8)
      - metal10(10) (8/8)

Violation:

LAYER	OBJECT1	LOCATION
	VDD	(3.340, 3.440) (6...
	VSS	(2.240, 2.340) (6...
metal10(...	VDD	(512.990, 421.20...
metal10(...	VDD	(512.990, 300.00...
metal10(...	VDD	(396.380, 421.20...
metal10(...	VDD	(396.380, 300.00...
metal10(...	VSS	(514.590, 421.20...
metal10(...	VSS	(514.590, 300.00...
metal10(...	VSS	(394.780, 421.20...
metal10(...	VSS	(394.780, 300.00...

Description:

Verify: no. = 10, bbox = (2.240, 2.340) (627.800, 476.740)

SoC Integration - Front End vs Back End

Front End Critical Path:

Cells: 43

Operation: DMA operation from the core

Back End Critical Path:

Cells: 80

Operation: DMA Operation from the core

Stage	Area (um^2)	Area (kilogates)	Slack (ns)	Frequency (MHz)	Average Power (uW)	VCD Power (uW)
Front End	54,084.3	67,605	0.24	100.0	301.6	355.6
Back End	291,462.8	364,328.5	0.768	100.0	442.5	182.9216

- Degradation in area, power, and timing

SoC Performance - Test Cases

Stage	Test Case 1	Test Case 2	Test Case 3
VHDL	0x41	0x58	0x80
VHDL + Hard Macro	0x41	0x58	0x80
Front End	0x41	0x58	0x80
Back End	0x41	0x58	0x80

- Test Case 1: read and write raw data to core manually
- Test Case 2: read and write from SRAM to core manually
- Test Case 3: read and write from SRAM to core using DMA

P&R Considerations

- Both place and route scripts are not completely automated
- Failed to automate importing design, automated once design is imported
- Scripts report time of running P&R scripts

aes128keyWrapper Macro:

- Decreased input transition time to 0.01

ENSC450 System:

- Decreased input transition time to 0.1

Timing and DRC Violations

aes128keyWrapper Core Macro:

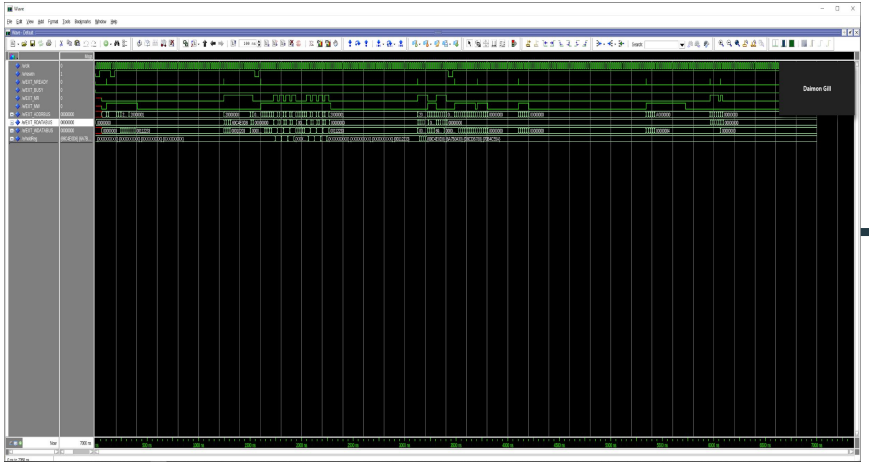
- DRC Violation free
- Timing Violation free
  - Hold and Setup conditions met
  - Max Tran and Max Cap conditions met

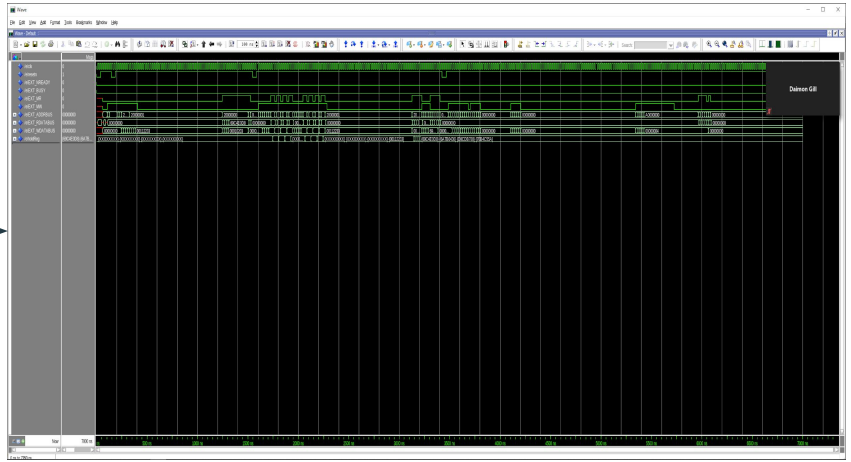
ENSC450 System:

- Contains DRC Violations
  - Unconnected pin violations with SRAM macro
  - Pins not connected to VDD and VSS global net
- Timing Violation free
  - Hold and Setup conditions met
  - Max Tran and Max Cap conditions met

Simulations

- Simulations conducted throughout to ensure correct functionality
- Two testbenches created: aes128keyWrapperTB and tb_ensc450
    - Before and after synthesis of amended core (within system and standalone)
    - After PR of core macro (within system and standalone)
    - After synthesizing system with macros
    - After place and route of the entire system
- All simulation waveforms can be viewed in submission folder





Thanks for watching!