COL215 Hardware Assignment 3

Arinjay Singhal 2023CS10041
Vihaan Luhariwala 2023CS10151

November 2024

1 Introduction

The objective of the assignment is: implementation of AES decryption operation. The components involved are memory elements (RAM, ROM and registers), FSM and control unit.

2 Design

The design of the AES decryption operation is as follows:

- main control unit: it takes clk and reset as input and performs aes decryption on the input data from the memory.
- memory: it stores the input data, round keys and sbox values.
- main FSM: it controls the flow of the decryption operation.

3 Logic

We use memory elements to load the ciphertext, round keys, and the inverse S-box matrix. The ciphertext is processed through a series of steps: Add Round Key, Inverse Mix Columns, Inverse Shift Rows, and Inverse Sub Bytes, with each step controlled by an FSM. The final plaintext is then displayed on an FPGA board, one column at a time, using a segment display process. Each process has its own FSM, and an additional FSM manages transitions between these processes, all synchronized to a clock.

3.1 main control unit

It has following fsm's:

- cycle_process : it updates the current fsm to the next fsm.
- whole_state_update : it updates the current 128 bit state by reading from the memory.
- main_proc : it does the aes decryption operation on current 128 bit state.
- seg_display : it displays the current 128 bit state.

3.2 memory

We generated 3 memories:

- sbox: it stores the sbox values.
- round_keys: it stores the round keys.
- input: it stores the input data.

We used block memory generator from IP catalog to generate the memories. The width of memories is 8 bit and depth is 256 for sbox and 160 for round keys and 32 for input. We then load the memories with the COE files and fill empty spaces with 0.

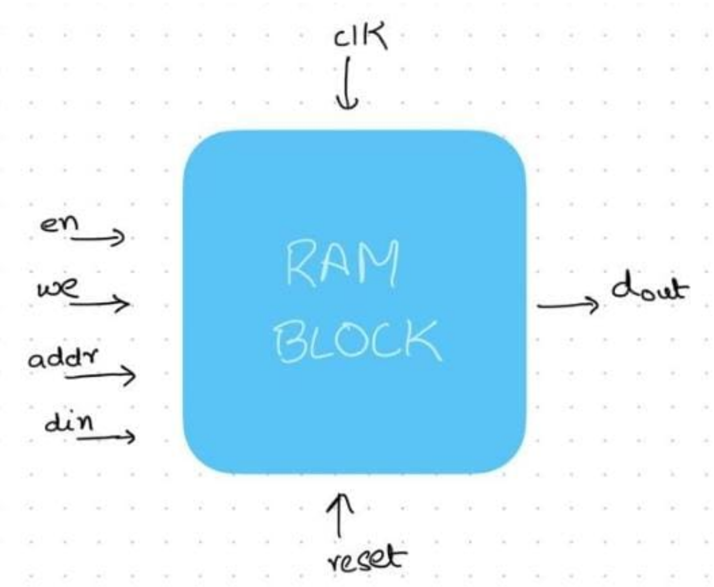


Figure 1: Block diagram of memory

3.3 main FSM

Main fsm controls the flow of the decryption operation. It is divided into round_counter, process_counter, intermediate_counter and step_counter. The delay to switch between states is 10 clock cycles. Round_counter is used to keep track of the current round (10 rounds in total). Process_counter is used to keep track of the current process (4 processes of AES decryption). Intermediate_counter tracks the current intermediate state (4 (in case of row operation) or 16 (in case of byte operation)). Step_counter is used to keep track of the current step (depends on the process).

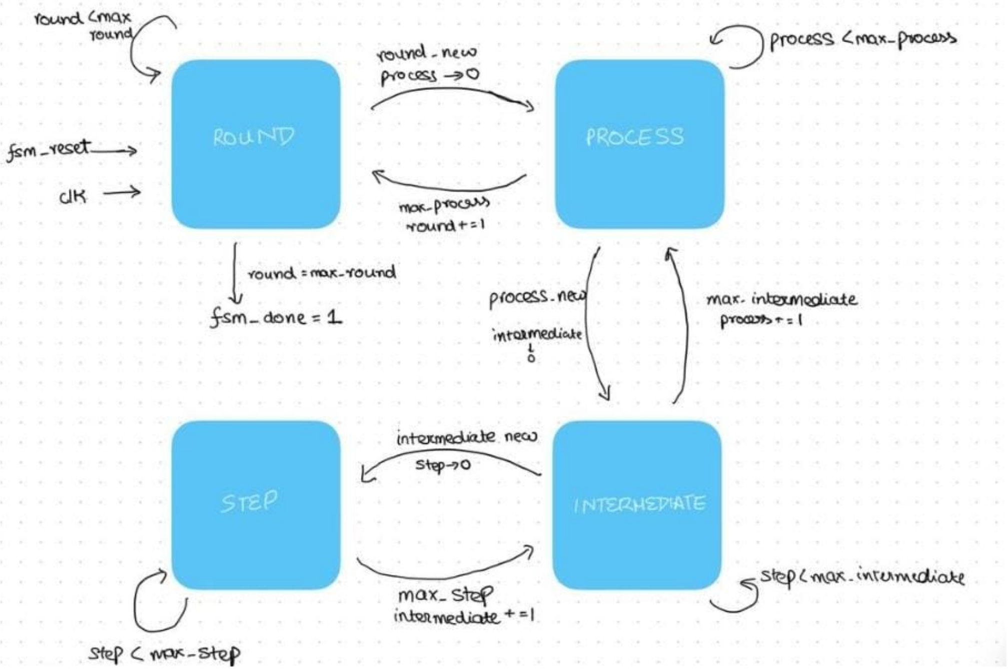


Figure 2: Block diagram of FSM

3.4 whole_state_update

It reads the 128 bit state from the memory and updates the current state signal (128 bit) with the read value. It has 2 steps indicating read and update. These have delay of 10 clock cycles.

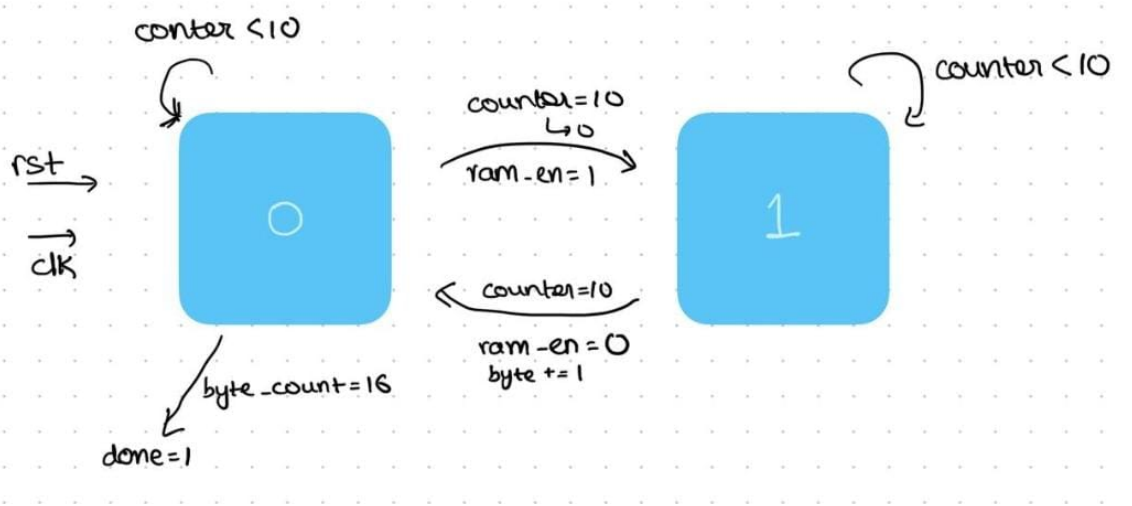


Figure 3: Block diagram of whole_state_update

3.5 main_proc

It performs the AES decryption operation on the current state. It takes its states from main FSM and performs the operations according to the signals.

3.6 seg_display

It displays the current state on the 7 segment display. We define 4 output columns before calling this state. It switches between the columns after 2^{28} clock cycles.

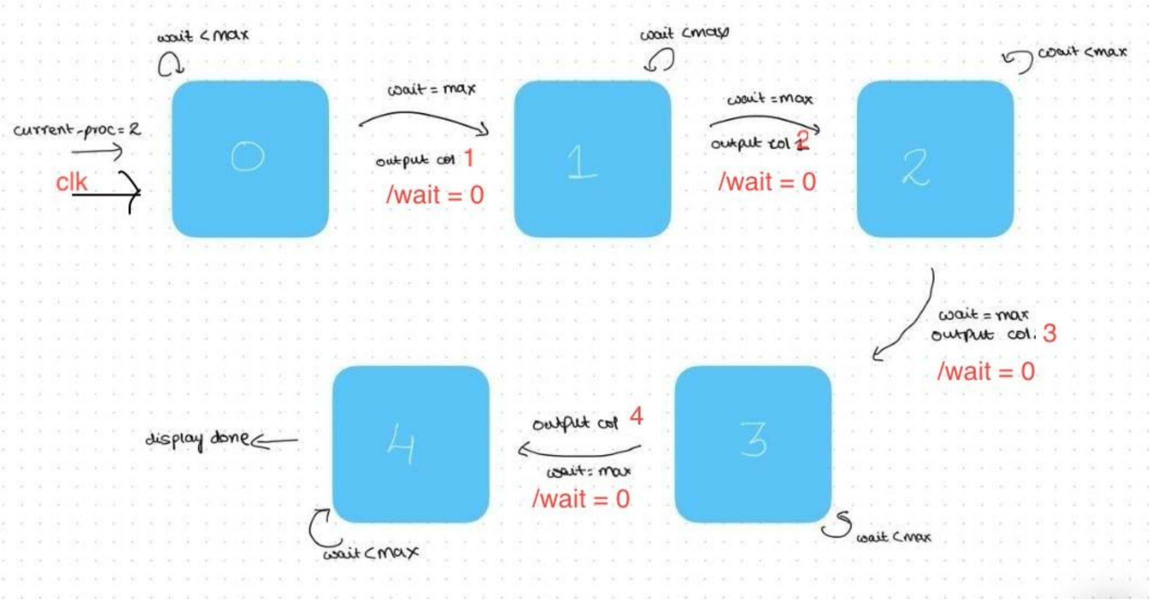


Figure 4: Block diagram of seg_display

3.7 cycle_process

It updates the current fsm to the next fsm based on the done signal from the current fsm.

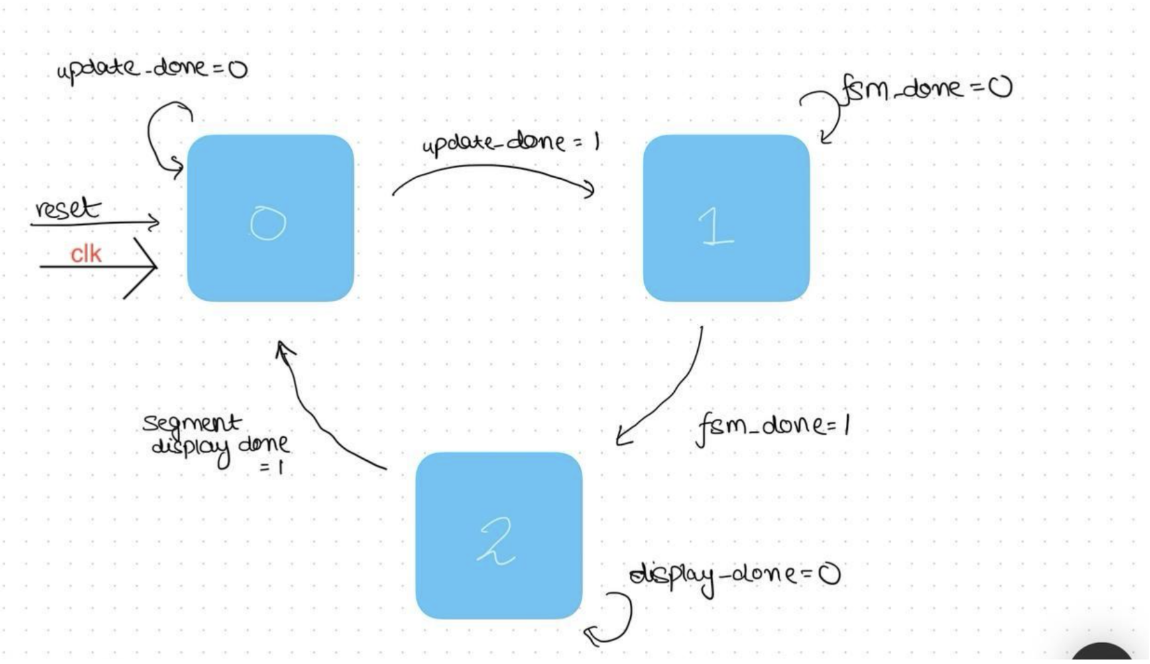


Figure 5: Block diagram of cycle_process

4 Simulation

4.1 Main FSM

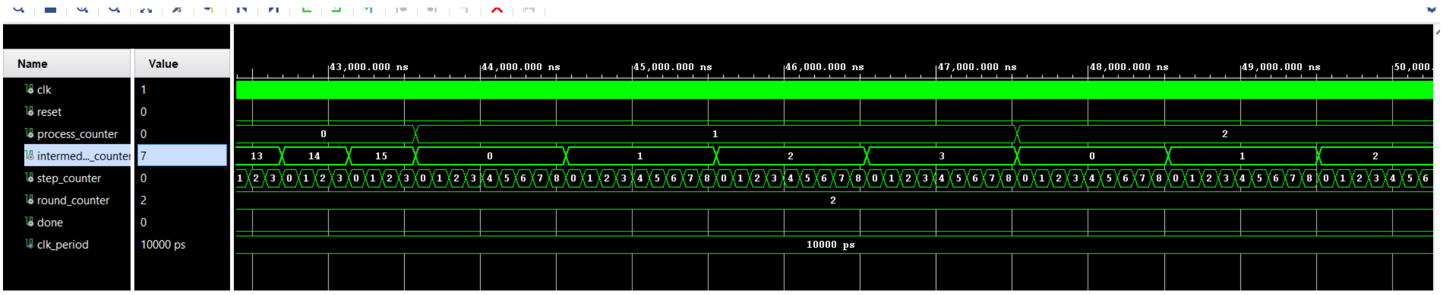


Figure 6: Simulation of FSM

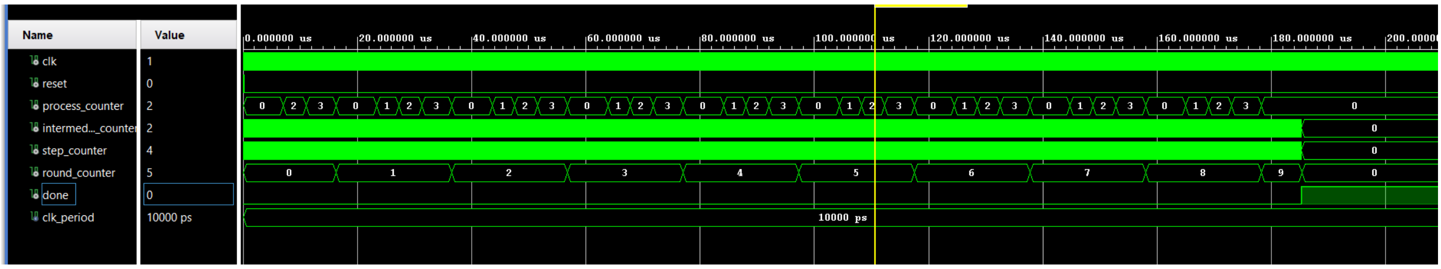


Figure 7: Simulation of FSM

4.2 Main control unit

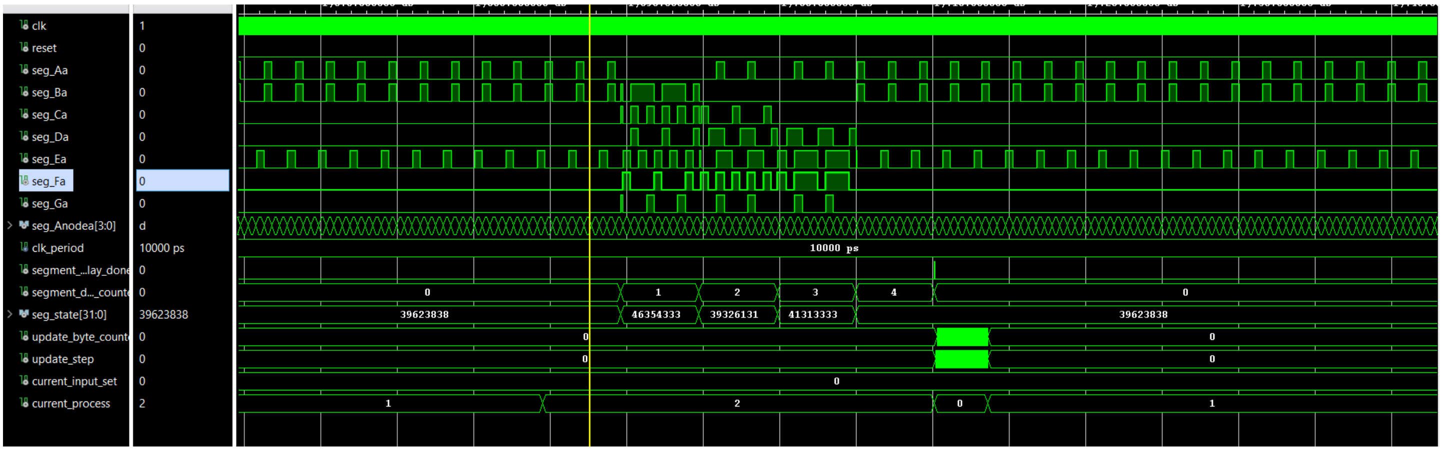
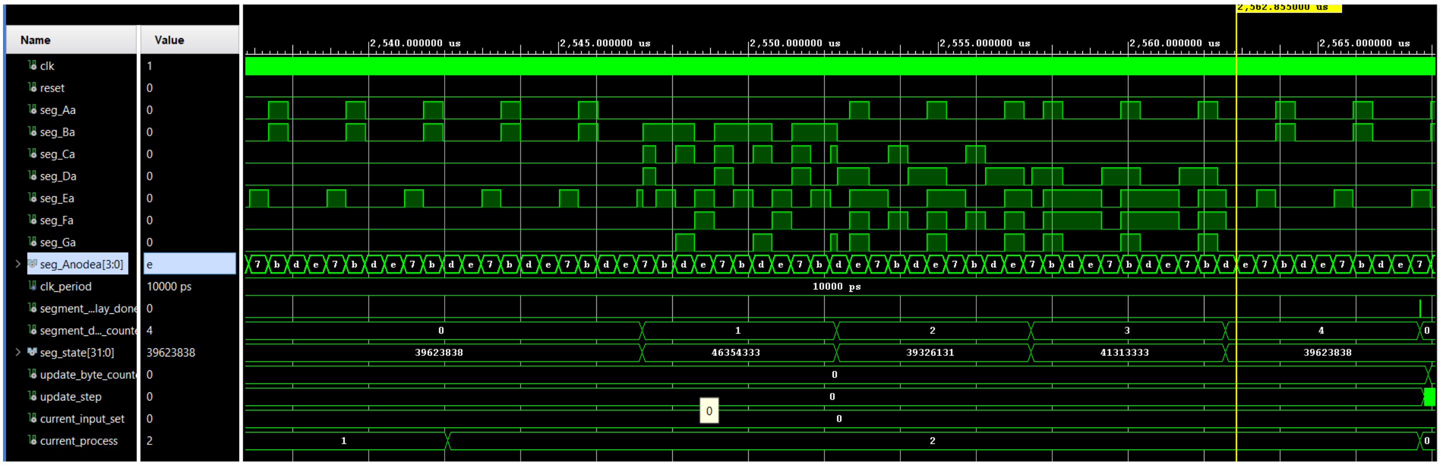
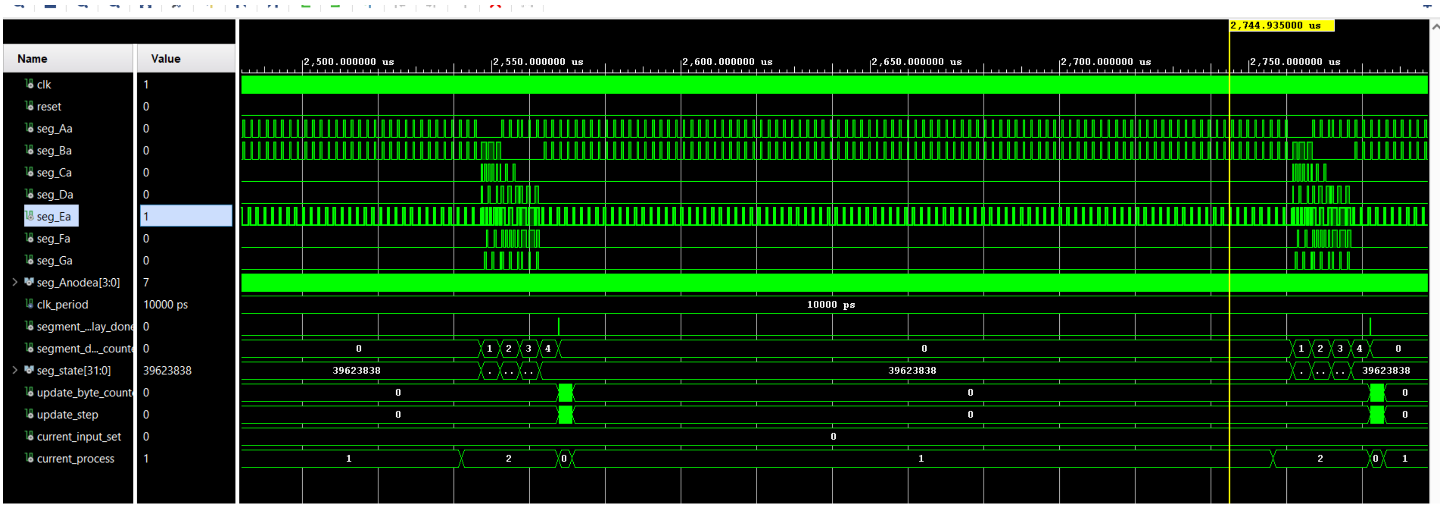


Figure 8: Simulation of main control unit



Name	Value
clk	1
reset	0
seg_Aa	0
seg_Ba	0
seg_Ca	0
seg_Da	0
seg_Ea	0
seg_Fa	0
seg_Ga	0
seg_Anodea[3:0]	e
clk_period	10000 ps
segment_...lay_done	0
segment_d..._count	4
seg_state[31:0]	39623838
update_byte_count	0
update_step	0
current_input_set	0
current_process	2

Figure 9: Simulation of main control unit



Name	Value
clk	1
reset	0
seg_Aa	0
seg_Ba	0
seg_Ca	0
seg_Da	0
seg_Ea	1
seg_Fa	0
seg_Ga	0
seg_Anodea[3:0]	7
clk_period	10000 ps
segment_...lay_done	0
segment_d..._count	0
seg_state[31:0]	39623838
update_byte_count	0
update_step	0
current_input_set	0
current_process	1

Figure 10: Simulation of main control unit

4.3 RTL Schematic

4.3.1 Main FSM

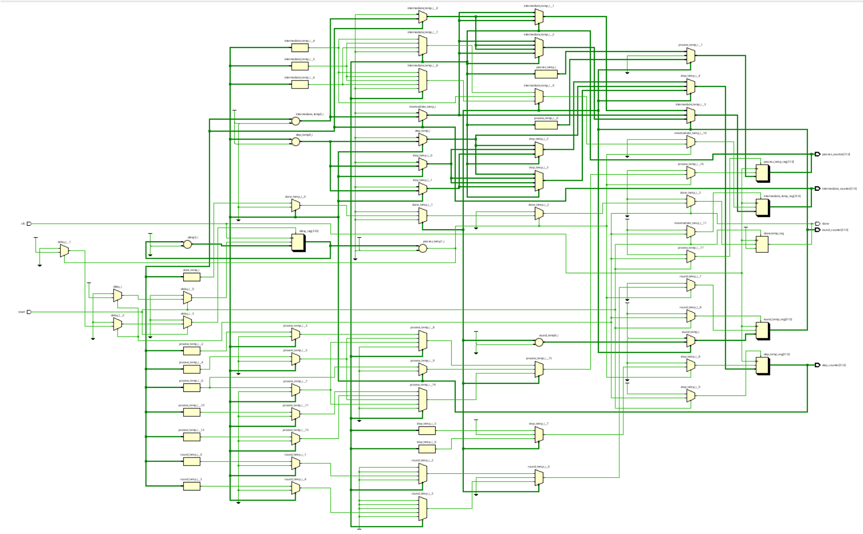


Figure 11: RTL Schematic

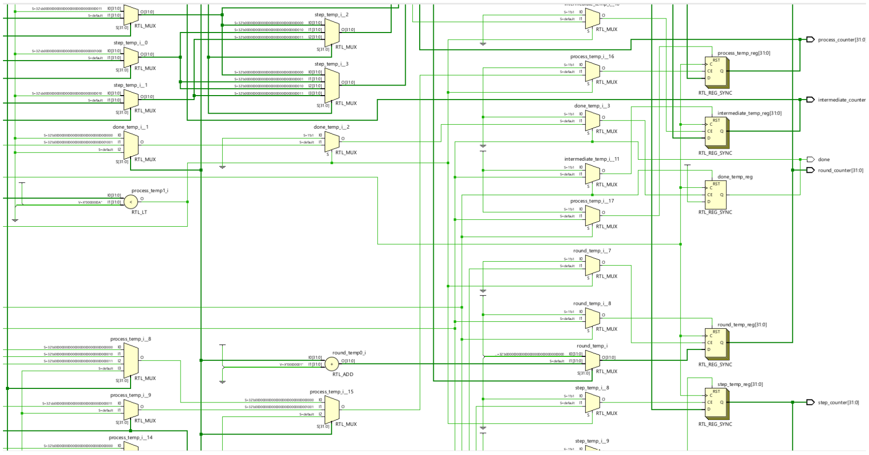


Figure 12: RTL Schematic

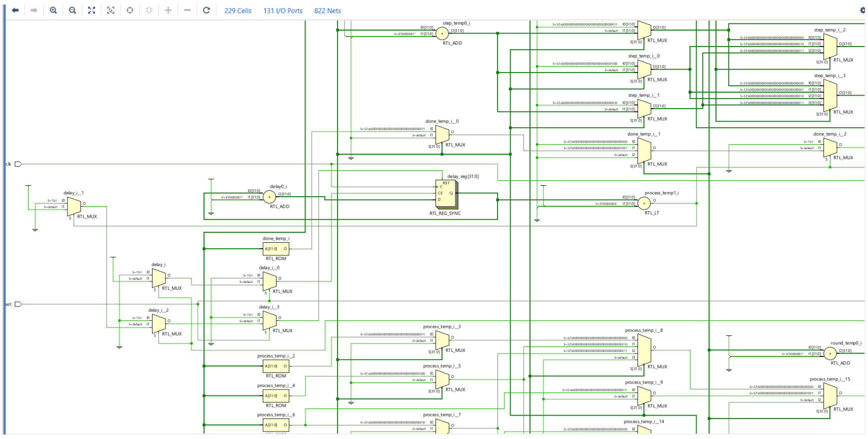


Figure 13: RTL Schematic

4.3.2 Main control unit

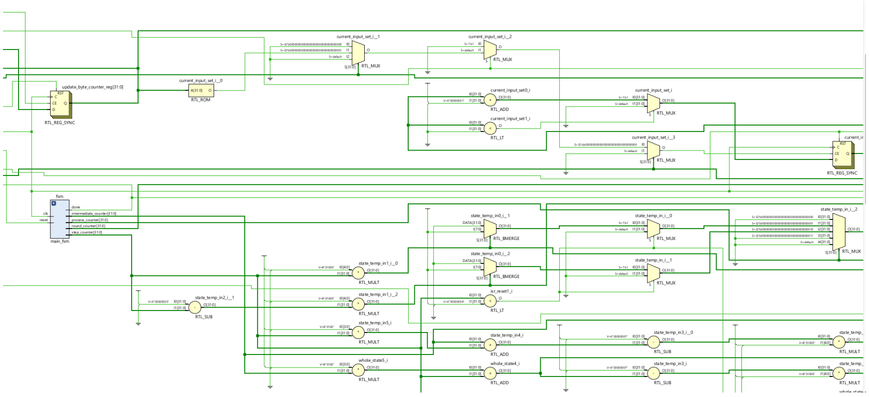


Figure 14: RTL Schematic

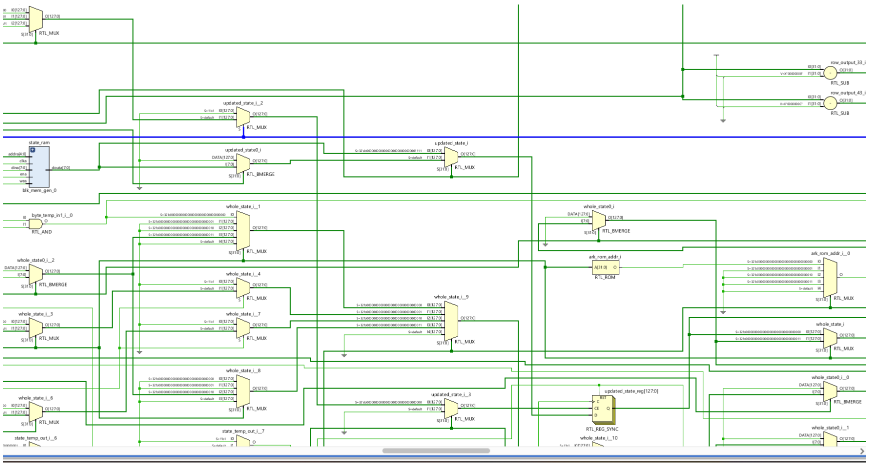


Figure 15: RTL Schematic

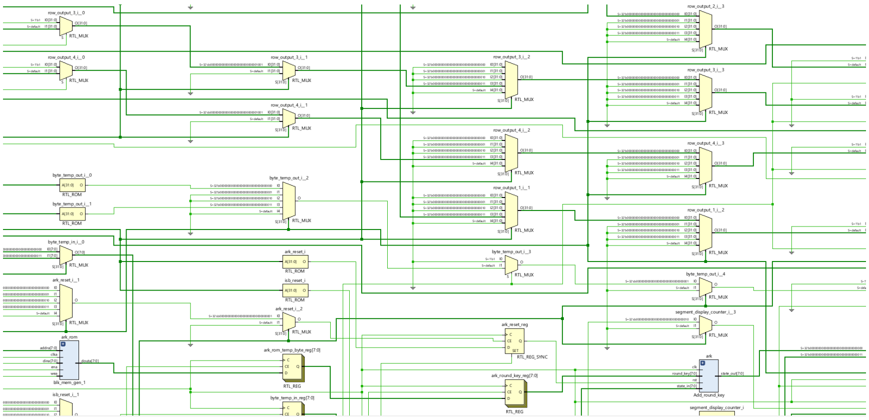


Figure 16: RTL Schematic

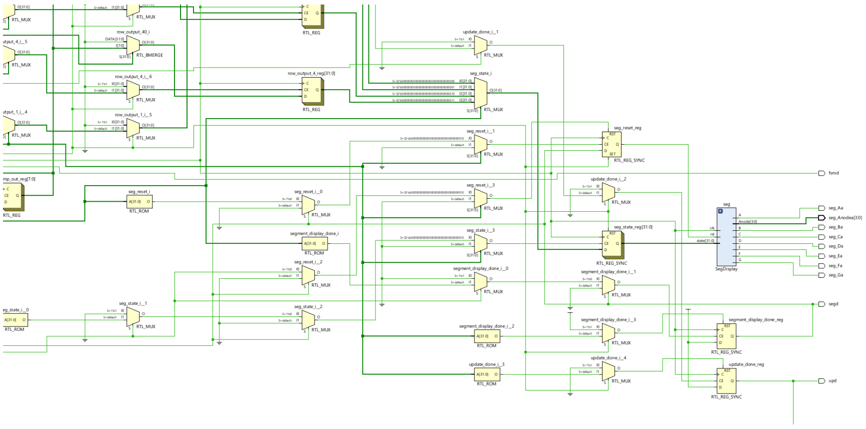
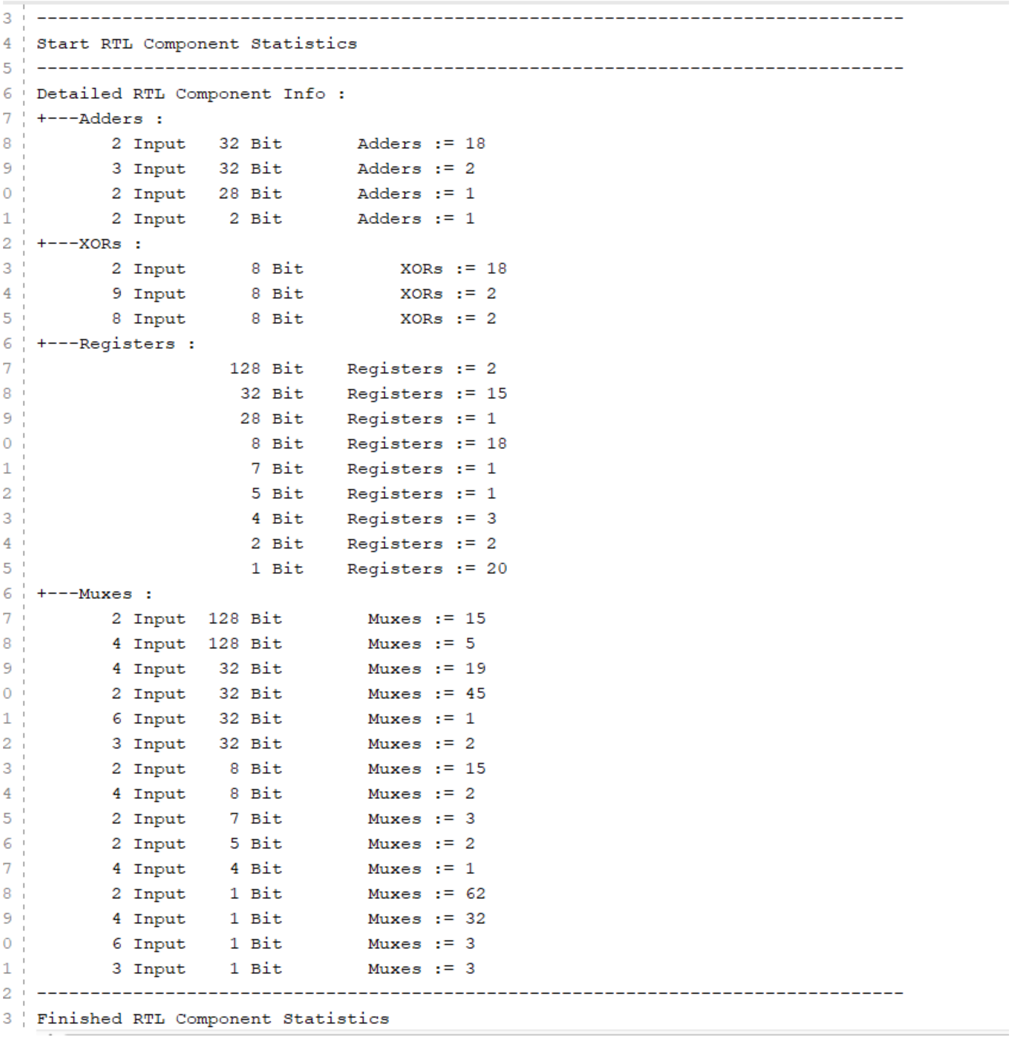


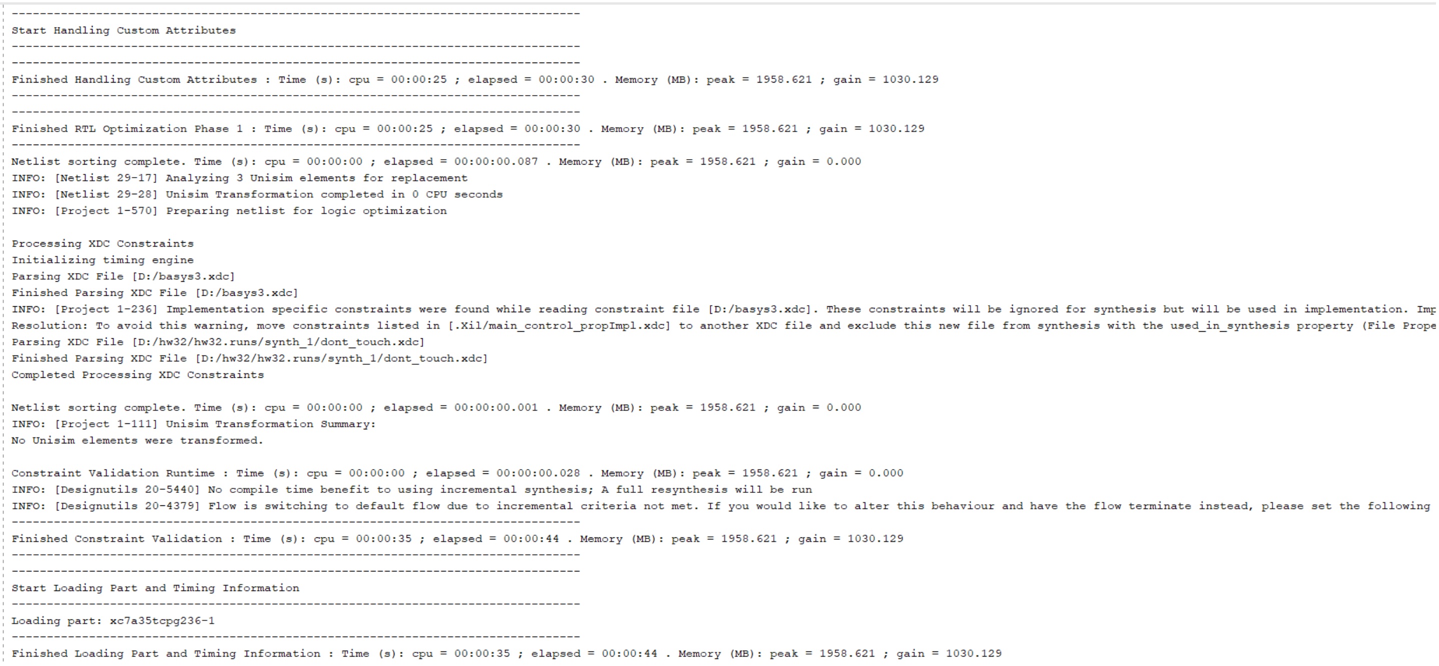
Figure 17: RTL Schematic

5 Synthesis Report



```
---------------------------------------------------------------------------------
Start RTL Component Statistics
---------------------------------------------------------------------------------
Detailed RTL Component Info :
+---Adders :
       2 Input   32 Bit       Adders := 18
       3 Input   32 Bit       Adders := 2
       2 Input   28 Bit       Adders := 1
       2 Input    2 Bit       Adders := 1
+---XORs :
       2 Input      8 Bit         XORs := 18
       9 Input      8 Bit         XORs := 2
       8 Input      8 Bit         XORs := 2
+---Registers :
                  128 Bit    Registers := 2
                   32 Bit    Registers := 15
                   28 Bit    Registers := 1
                    8 Bit    Registers := 18
                    7 Bit    Registers := 1
                    5 Bit    Registers := 1
                    4 Bit    Registers := 3
                    2 Bit    Registers := 2
                    1 Bit    Registers := 20
+---Muxes :
       2 Input  128 Bit        Muxes := 15
       4 Input  128 Bit        Muxes := 5
       4 Input   32 Bit        Muxes := 19
       2 Input   32 Bit        Muxes := 45
       6 Input   32 Bit        Muxes := 1
       3 Input   32 Bit        Muxes := 2
       2 Input    8 Bit        Muxes := 15
       4 Input    8 Bit        Muxes := 2
       2 Input    7 Bit        Muxes := 3
       2 Input    5 Bit        Muxes := 2
       4 Input    4 Bit        Muxes := 1
       2 Input    1 Bit        Muxes := 62
       4 Input    1 Bit        Muxes := 32
       6 Input    1 Bit        Muxes := 3
       3 Input    1 Bit        Muxes := 3
---------------------------------------------------------------------------------
Finished RTL Component Statistics
```

Figure 18: Synthesis Report



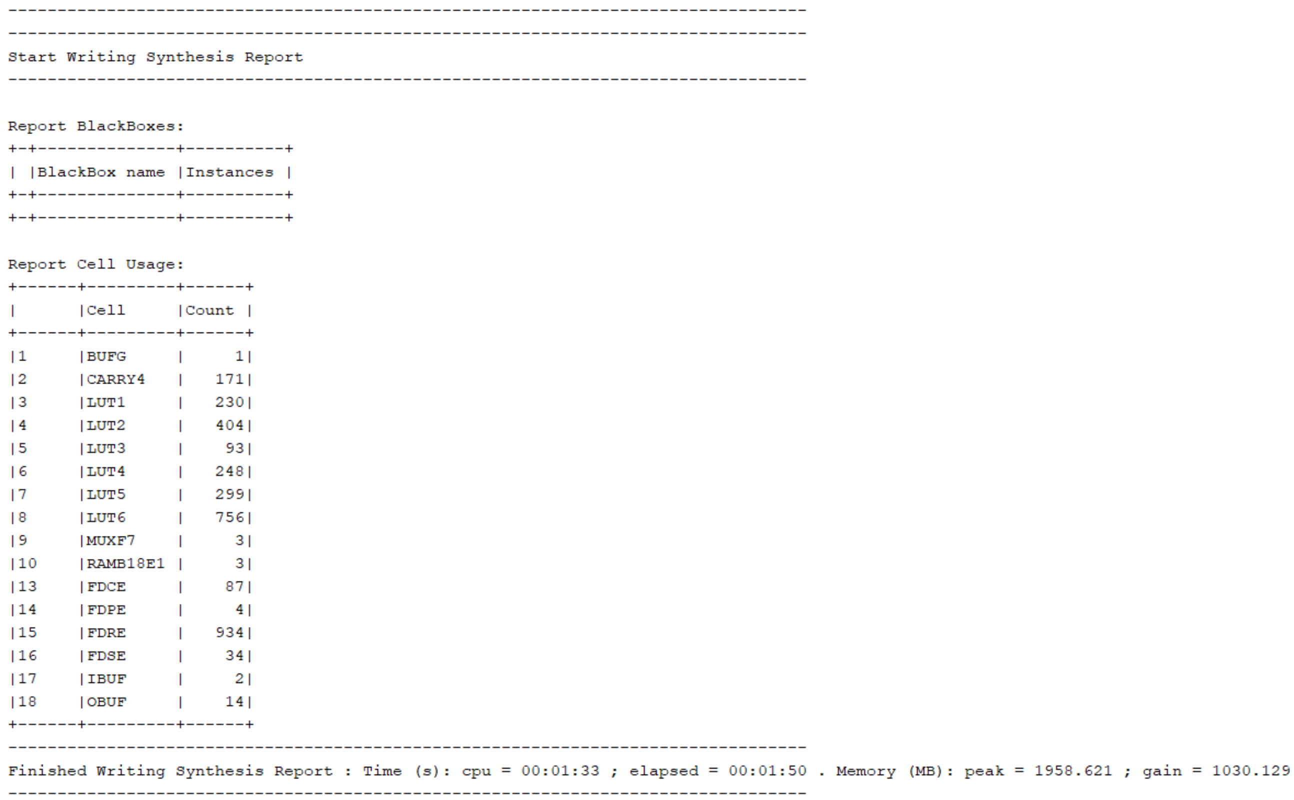
```
---------------------------------------------------------------------------------
Start Handling Custom Attributes
---------------------------------------------------------------------------------
---------------------------------------------------------------------------------
Finished Handling Custom Attributes : Time (s): cpu = 00:00:25 ; elapsed = 00:00:30 . Memory (MB): peak = 1958.621 ; gain = 1030.129
---------------------------------------------------------------------------------
---------------------------------------------------------------------------------
Finished RTL Optimization Phase 1 : Time (s): cpu = 00:00:25 ; elapsed = 00:00:30 . Memory (MB): peak = 1958.621 ; gain = 1030.129
---------------------------------------------------------------------------------
Netlist sorting complete. Time (s): cpu = 00:00:00 ; elapsed = 00:00:00.087 . Memory (MB): peak = 1958.621 ; gain = 0.000
INFO: [Netlist 29-17] Analyzing 3 Unisim elements for replacement
INFO: [Netlist 29-28] Unisim Transformation completed in 0 CPU seconds
INFO: [Project 1-570] Preparing netlist for logic optimization

Processing XDC Constraints
Initializing timing engine
Parsing XDC File [D:/basys3.xdc]
Finished Parsing XDC File [D:/basys3.xdc]
INFO: [Project 1-236] Implementation specific constraints were found while reading constraint file [D:/basys3.xdc]. These constraints will be ignored for synthesis but will be used in implementation. Imp
Resolution: To avoid this warning, move constraints listed in [.Xil/main_control_propImpl.xdc] to another XDC file and exclude this new file from synthesis with the used_in_synthesis property (File Prope
Parsing XDC File [D:/hw32/hw32.runs/synth_1/dont_touch.xdc]
Finished Parsing XDC File [D:/hw32/hw32.runs/synth_1/dont_touch.xdc]
Completed Processing XDC Constraints

Netlist sorting complete. Time (s): cpu = 00:00:00 ; elapsed = 00:00:00.001 . Memory (MB): peak = 1958.621 ; gain = 0.000
INFO: [Project 1-111] Unisim Transformation Summary:
No Unisim elements were transformed.

Constraint Validation Runtime : Time (s): cpu = 00:00:00 ; elapsed = 00:00:00.028 . Memory (MB): peak = 1958.621 ; gain = 0.000
INFO: [Designutils 20-5440] No compile time benefit to using incremental synthesis; A full resynthesis will be run
INFO: [Designutils 20-4379] Flow is switching to default flow due to incremental criteria not met. If you would like to alter this behaviour and have the flow terminate instead, please set the following
---------------------------------------------------------------------------------
Finished Constraint Validation : Time (s): cpu = 00:00:35 ; elapsed = 00:00:44 . Memory (MB): peak = 1958.621 ; gain = 1030.129
---------------------------------------------------------------------------------
---------------------------------------------------------------------------------
Start Loading Part and Timing Information
---------------------------------------------------------------------------------
Loading part: xc7a35tcpg236-1
---------------------------------------------------------------------------------
Finished Loading Part and Timing Information : Time (s): cpu = 00:00:35 ; elapsed = 00:00:44 . Memory (MB): peak = 1958.621 ; gain = 1030.129
```

Figure 19: Synthesis Report



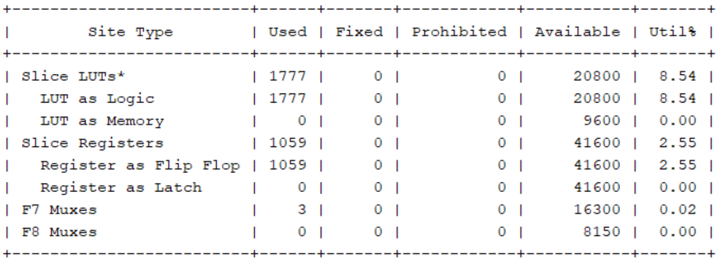
```
---------------------------------------------------------------------------------
---------------------------------------------------------------------------------
Start Writing Synthesis Report
---------------------------------------------------------------------------------

Report BlackBoxes:
+-+--------------+----------+
| |BlackBox name |Instances |
+-+--------------+----------+
+-+--------------+----------+

Report Cell Usage:
+------+---------+------+
|      |Cell     |Count |
+------+---------+------+
|1     |BUFG     |     1|
|2     |CARRY4   |   171|
|3     |LUT1     |   230|
|4     |LUT2     |   404|
|5     |LUT3     |    93|
|6     |LUT4     |   248|
|7     |LUT5     |   299|
|8     |LUT6     |   756|
|9     |MUXF7    |     3|
|10    |RAMB18E1 |     3|
|13    |FDCE     |    87|
|14    |FDPE     |     4|
|15    |FDRE     |   934|
|16    |FDSE     |    34|
|17    |IBUF     |     2|
|18    |OBUF     |    14|
+------+---------+------+
---------------------------------------------------------------------------------
Finished Writing Synthesis Report : Time (s): cpu = 00:01:33 ; elapsed = 00:01:50 . Memory (MB): peak = 1958.621 ; gain = 1030.129
---------------------------------------------------------------------------------
```

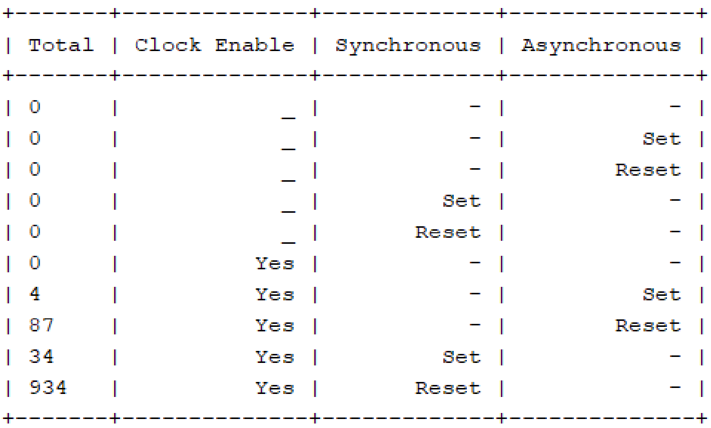
Figure 20: Synthesis Report

6 Utilization Report



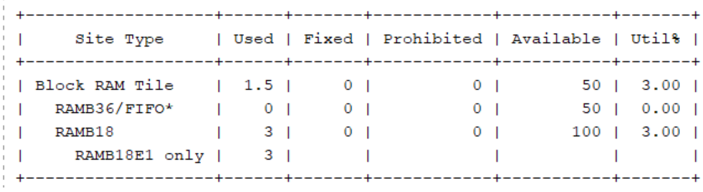
```
+-------------------------+------+-------+------------+-----------+-------+
|        Site Type        | Used | Fixed | Prohibited | Available | Util% |
+-------------------------+------+-------+------------+-----------+-------+
| Slice LUTs*             | 1777 |     0 |          0 |     20800 |  8.54 |
|   LUT as Logic          | 1777 |     0 |          0 |     20800 |  8.54 |
|   LUT as Memory         |    0 |     0 |          0 |      9600 |  0.00 |
| Slice Registers         | 1059 |     0 |          0 |     41600 |  2.55 |
|   Register as Flip Flop | 1059 |     0 |          0 |     41600 |  2.55 |
|   Register as Latch     |    0 |     0 |          0 |     41600 |  0.00 |
| F7 Muxes                |    3 |     0 |          0 |     16300 |  0.02 |
| F8 Muxes                |    0 |     0 |          0 |      8150 |  0.00 |
+-------------------------+------+-------+------------+-----------+-------+
```

Figure 21: Utilization Report



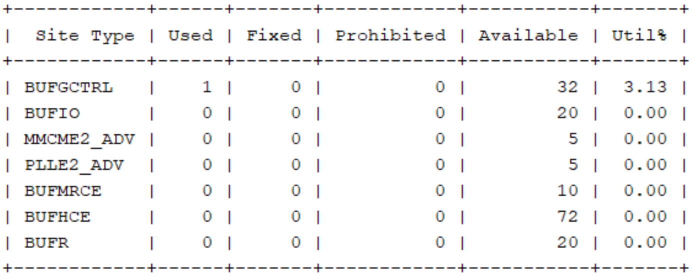
```
+-------+--------------+-------------+--------------+
| Total | Clock Enable | Synchronous | Asynchronous |
+-------+--------------+-------------+--------------+
| 0     |            _ |           - |            - |
| 0     |            _ |           - |          Set |
| 0     |            _ |           - |        Reset |
| 0     |            _ |         Set |            - |
| 0     |            _ |       Reset |            - |
| 0     |          Yes |           - |            - |
| 4     |          Yes |           - |          Set |
| 87    |          Yes |           - |        Reset |
| 34    |          Yes |         Set |            - |
| 934   |          Yes |       Reset |            - |
+-------+--------------+-------------+--------------+
```

Figure 22: Utilization Report



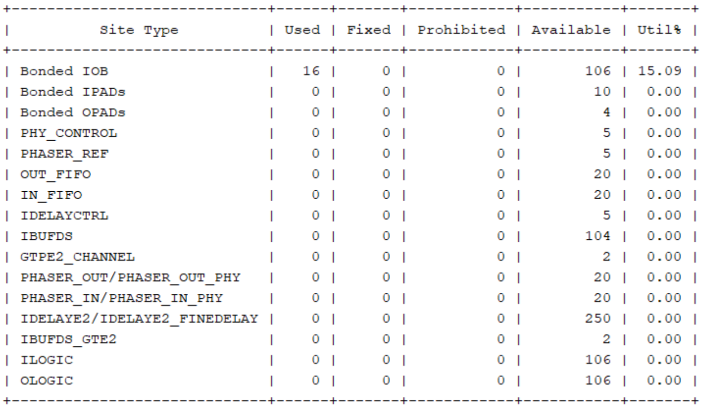
```
+-------------------+------+-------+------------+-----------+-------+
|     Site Type     | Used | Fixed | Prohibited | Available | Util% |
+-------------------+------+-------+------------+-----------+-------+
| Block RAM Tile    |  1.5 |     0 |          0 |        50 |  3.00 |
|   RAMB36/FIFO*    |    0 |     0 |          0 |        50 |  0.00 |
|   RAMB18          |    3 |     0 |          0 |       100 |  3.00 |
|     RAMB18E1 only |    3 |       |            |           |       |
+-------------------+------+-------+------------+-----------+-------+
```

Figure 23: Utilization Report



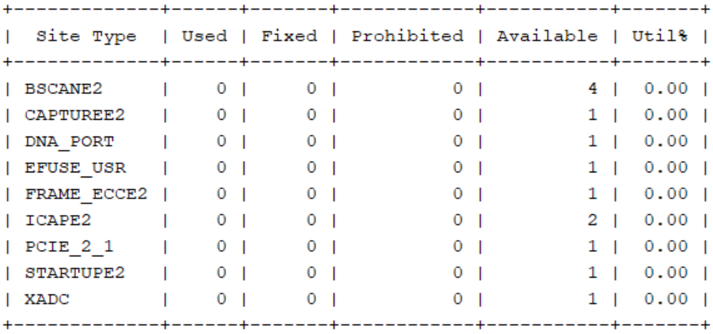
```
+------------+------+-------+------------+-----------+-------+
|  Site Type | Used | Fixed | Prohibited | Available | Util% |
+------------+------+-------+------------+-----------+-------+
| BUFGCTRL   |    1 |     0 |          0 |        32 |  3.13 |
| BUFIO      |    0 |     0 |          0 |        20 |  0.00 |
| MMCME2_ADV |    0 |     0 |          0 |         5 |  0.00 |
| PLLE2_ADV  |    0 |     0 |          0 |         5 |  0.00 |
| BUFMRCE    |    0 |     0 |          0 |        10 |  0.00 |
| BUFHCE     |    0 |     0 |          0 |        72 |  0.00 |
| BUFR       |    0 |     0 |          0 |        20 |  0.00 |
+------------+------+-------+------------+-----------+-------+
```

Figure 24: Utilization Report



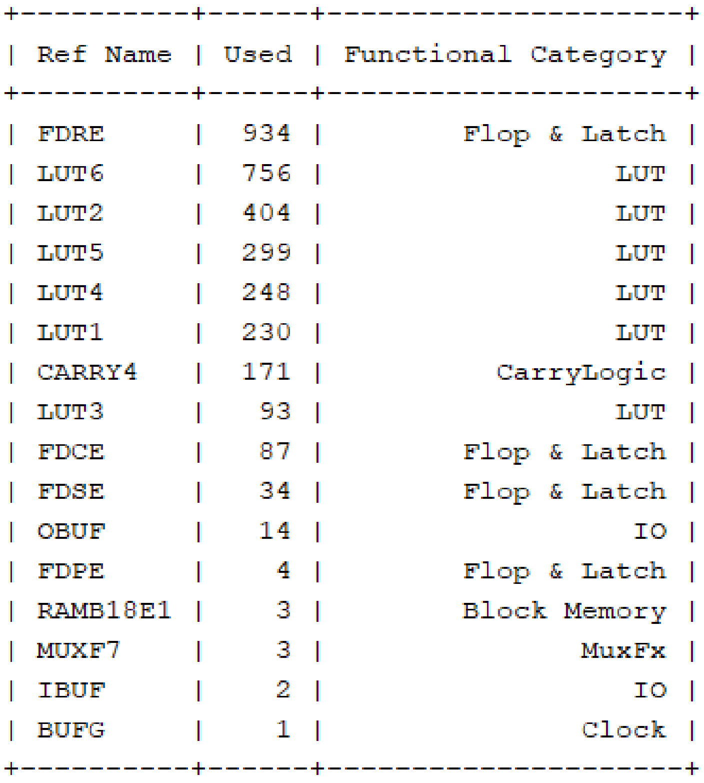
```
+-----------------------------+------+-------+------------+-----------+-------+
|          Site Type          | Used | Fixed | Prohibited | Available | Util% |
+-----------------------------+------+-------+------------+-----------+-------+
| Bonded IOB                  |   16 |     0 |          0 |       106 | 15.09 |
| Bonded IPADs                |    0 |     0 |          0 |        10 |  0.00 |
| Bonded OPADs                |    0 |     0 |          0 |         4 |  0.00 |
| PHY_CONTROL                 |    0 |     0 |          0 |         5 |  0.00 |
| PHASER_REF                  |    0 |     0 |          0 |         5 |  0.00 |
| OUT_FIFO                    |    0 |     0 |          0 |        20 |  0.00 |
| IN_FIFO                     |    0 |     0 |          0 |        20 |  0.00 |
| IDELAYCTRL                  |    0 |     0 |          0 |         5 |  0.00 |
| IBUFDS                      |    0 |     0 |          0 |       104 |  0.00 |
| GTPE2_CHANNEL               |    0 |     0 |          0 |         2 |  0.00 |
| PHASER_OUT/PHASER_OUT_PHY   |    0 |     0 |          0 |        20 |  0.00 |
| PHASER_IN/PHASER_IN_PHY     |    0 |     0 |          0 |        20 |  0.00 |
| IDELAYE2/IDELAYE2_FINEDELAY |    0 |     0 |          0 |       250 |  0.00 |
| IBUFDS_GTE2                 |    0 |     0 |          0 |         2 |  0.00 |
| ILOGIC                      |    0 |     0 |          0 |       106 |  0.00 |
| OLOGIC                      |    0 |     0 |          0 |       106 |  0.00 |
+-----------------------------+------+-------+------------+-----------+-------+
```

Figure 25: Utilization Report



```
+-------------+------+-------+------------+-----------+-------+
|  Site Type  | Used | Fixed | Prohibited | Available | Util% |
+-------------+------+-------+------------+-----------+-------+
| BSCANE2     |    0 |     0 |          0 |         4 |  0.00 |
| CAPTUREE2   |    0 |     0 |          0 |         1 |  0.00 |
| DNA_PORT    |    0 |     0 |          0 |         1 |  0.00 |
| EFUSE_USR   |    0 |     0 |          0 |         1 |  0.00 |
| FRAME_ECCE2 |    0 |     0 |          0 |         1 |  0.00 |
| ICAPE2      |    0 |     0 |          0 |         2 |  0.00 |
| PCIE_2_1    |    0 |     0 |          0 |         1 |  0.00 |
| STARTUPE2   |    0 |     0 |          0 |         1 |  0.00 |
| XADC        |    0 |     0 |          0 |         1 |  0.00 |
+-------------+------+-------+------------+-----------+-------+
```

Figure 26: Utilization Report



```
+-----------+------+---------------------+
| Ref Name  | Used | Functional Category |
+-----------+------+---------------------+
| FDRE      |  934 |        Flop & Latch |
| LUT6      |  756 |                 LUT |
| LUT2      |  404 |                 LUT |
| LUT5      |  299 |                 LUT |
| LUT4      |  248 |                 LUT |
| LUT1      |  230 |                 LUT |
| CARRY4    |  171 |          CarryLogic |
| LUT3      |   93 |                 LUT |
| FDCE      |   87 |        Flop & Latch |
| FDSE      |   34 |        Flop & Latch |
| OBUF      |   14 |                  IO |
| FDPE      |    4 |        Flop & Latch |
| RAMB18E1  |    3 |        Block Memory |
| MUXF7     |    3 |               MuxFx |
| IBUF      |    2 |                  IO |
| BUFG      |    1 |               Clock |
+-----------+------+---------------------+
```

Figure 27: Utilization Report

7 Final result

We ran our module on the FPGA after loading the memories with the 128 bit COE file from moodle. The output was as expected and the 7 segment display showed the correct output.

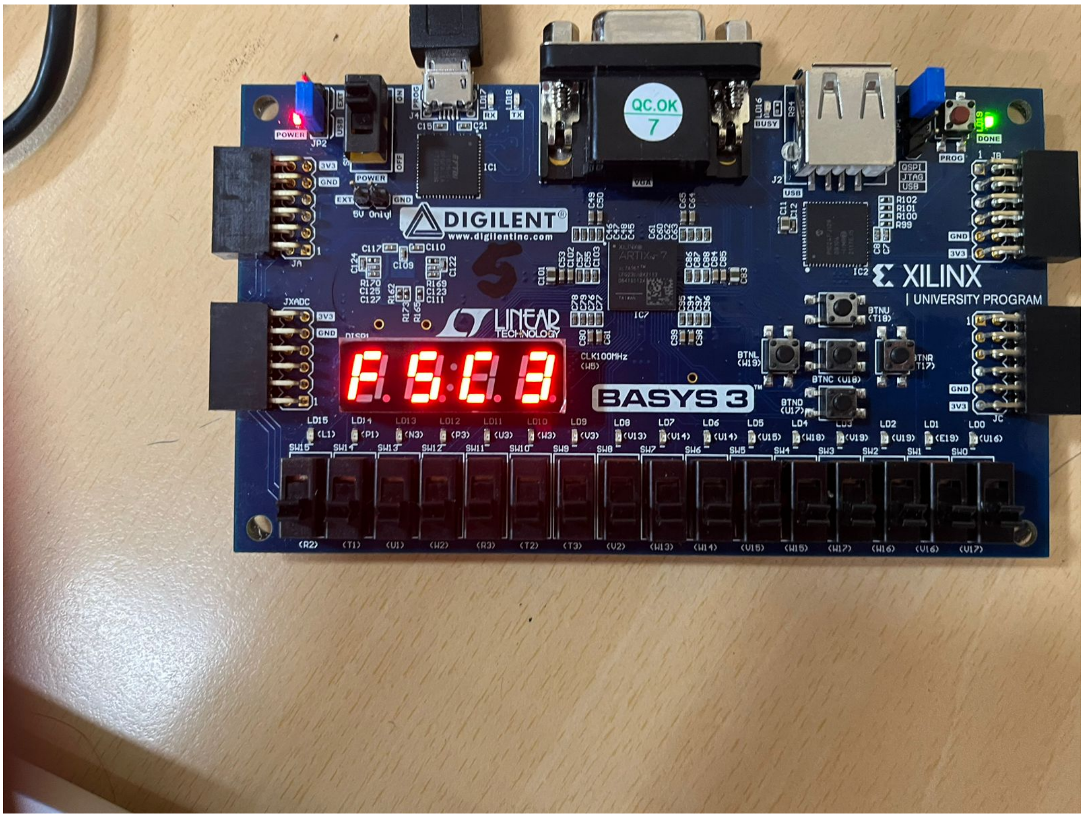


Figure 28: output column 1 : F5C3

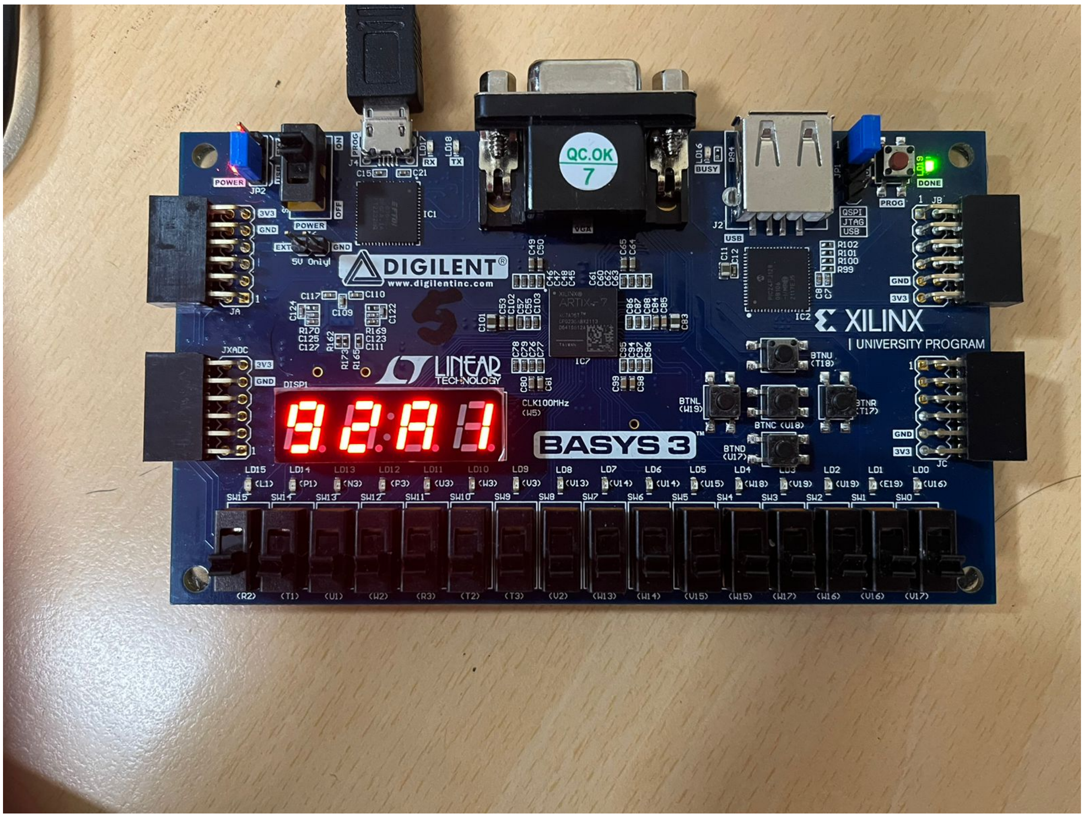


Figure 29: output column 2 : 92A1

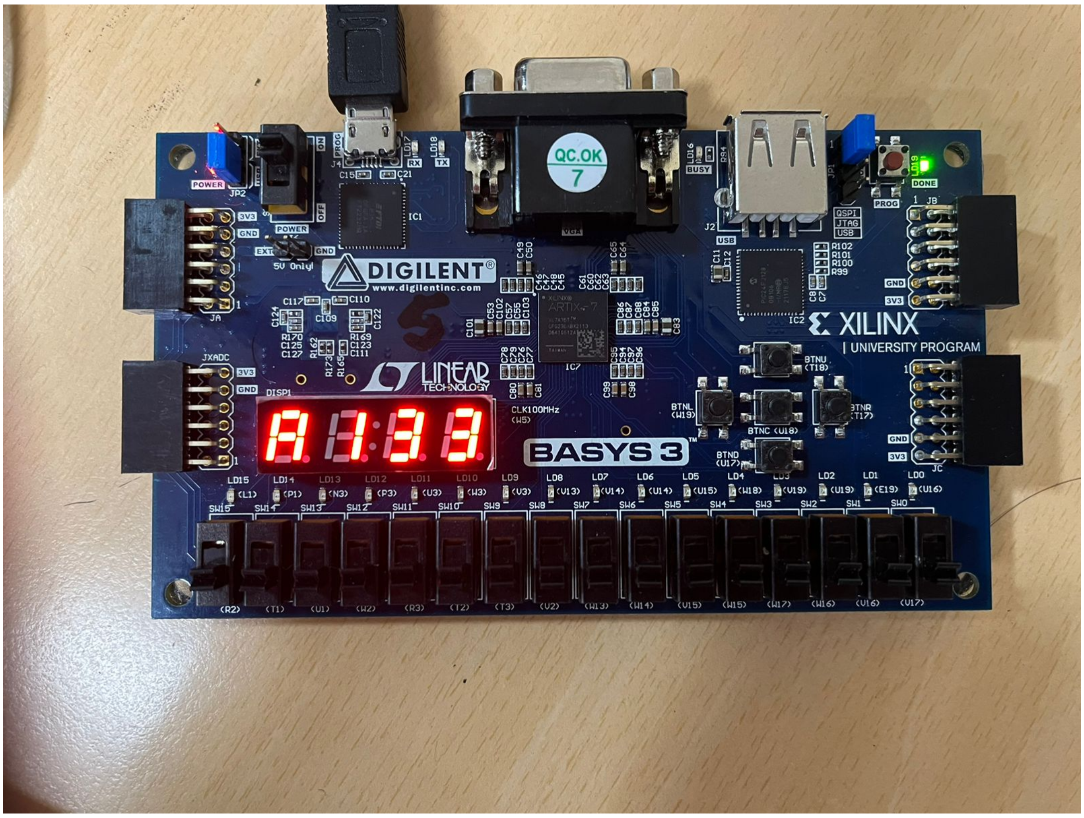


Figure 30: output column 3 : A133

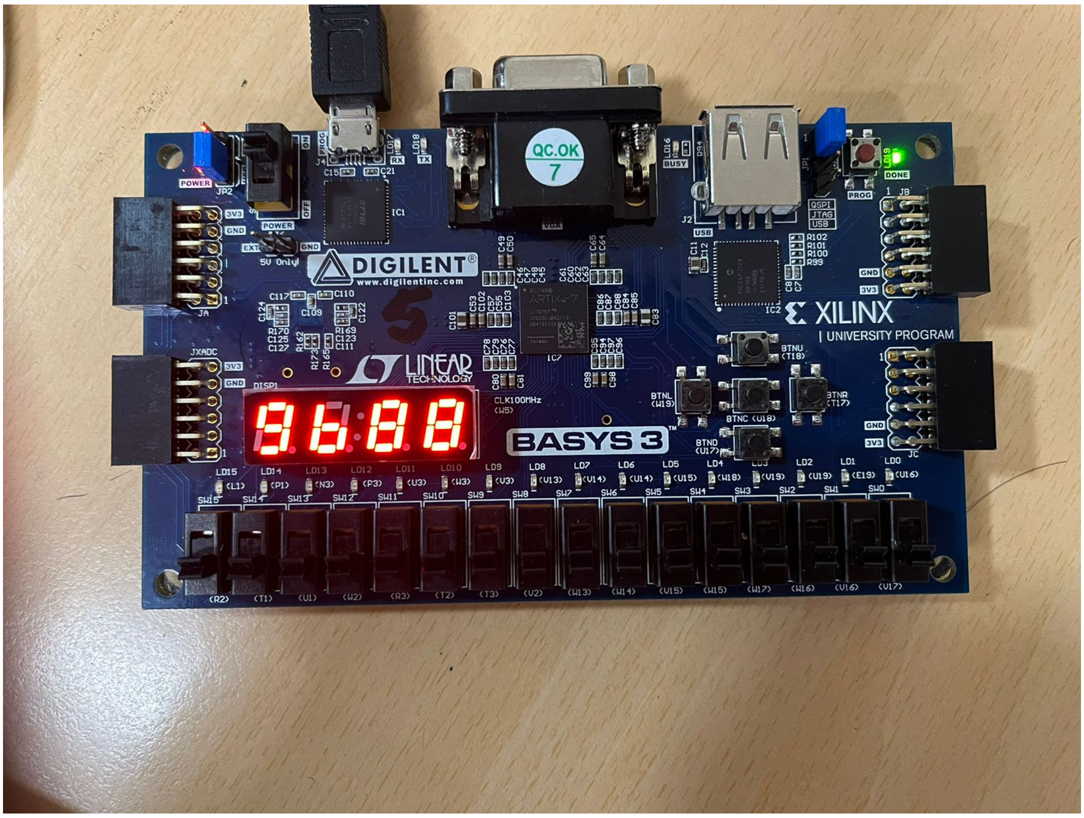


Figure 31: output column 4 : 9b88