Elliptic Curve Cryptography with Triple DES Encryption

Final Report

Team 3 Members: Nico Bellante, Lucas Dahl, Manish Gupta, Xiong-Yao Zha

Class: ECE 337

Lab Section: Wednesday 11:30

May 7, 2015

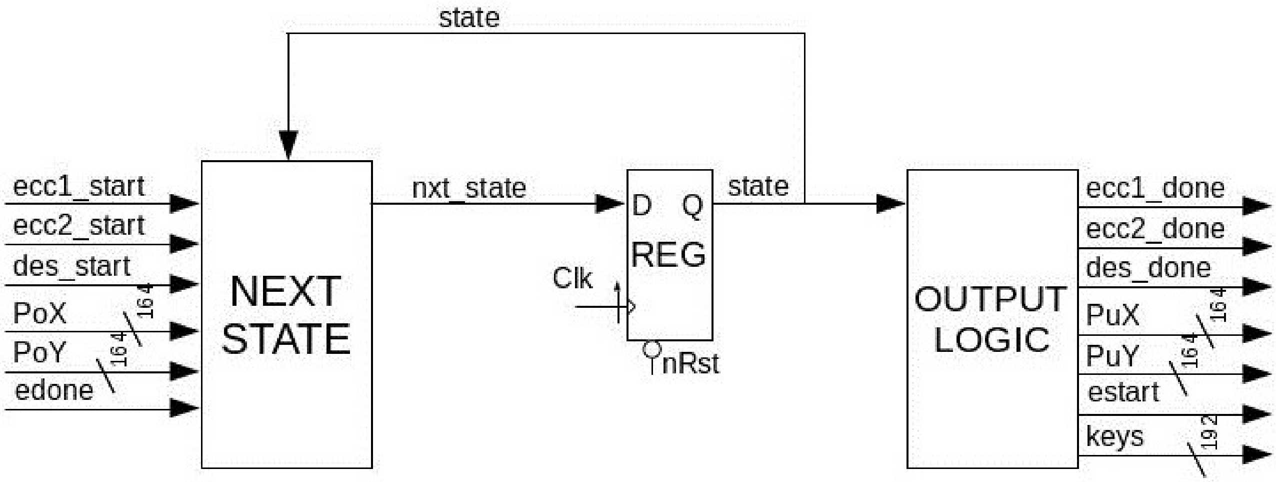
Teaching Assistant: Yunus Akhtar

SIGNATURES GO HERE

Executive Summary

We have designed a chip that does secure encryption of data using Elliptical Curve Cryptography and Triple DES encryption. The chip uses an Elliptical Curve Cryptography implementation of the Diffie-Hellman Key Exchange Protocol to generate the public and session keys that will be used for encrypting data. The actual encryption is done using Triple DES EEE encryption. Our chip will generate our own public key using our implementation of Elliptical Curve Cryptography upon reset. Following generating the public key, it will receive a public key from another party and use our ECC algorithm to generate a session key that will be used to create the round keys for Triple DES. Finally, upon receiving raw data it will encrypt the data using Triple DES encryption using the round keys generated from the generated session keys, and store it in SRAM. That is encrypting the data three times using three parts of the generated session keys. In this day and age computer security and security of encrypted data is extremely important, and the chip we have designed allows for an efficient and very secure method to encrypt data. Furthermore, our algorithm allows for the same amount of security using a much smaller key size than other algorithms used for encryption. Our design is unique from the current encryption chips because all three keys for Triple DES encryption are created using ECC making it extremely secure. Our design is more efficient as an ASIC implementation, because we can do calculations in parallel. The rest of this report will cover the design specifications of our chip, the finalized system diagrams, and the results of our chip.

Operational Characteristics



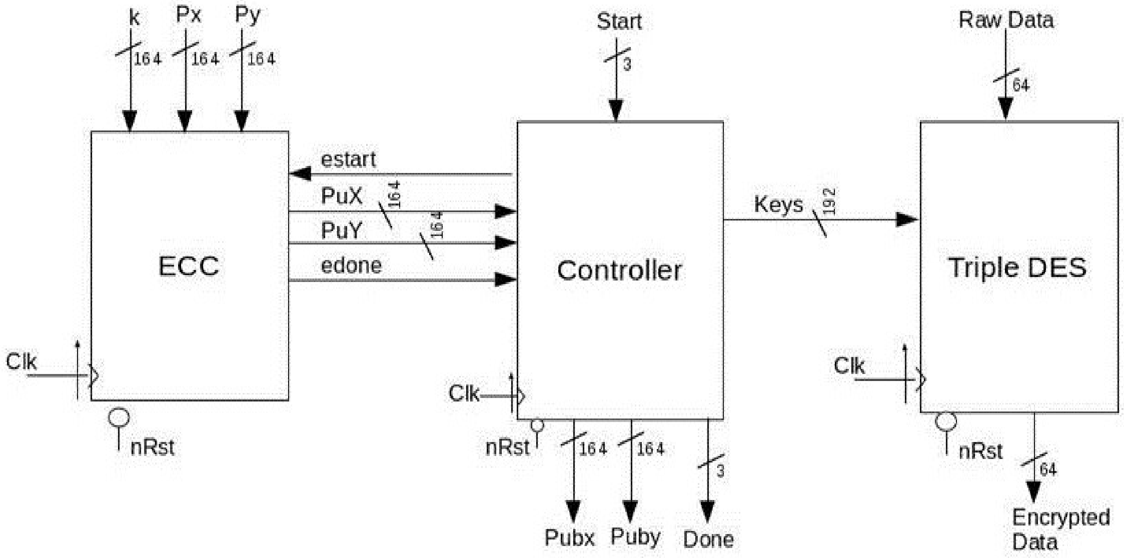
Signal Name	Type	Number of bits	Description
CLK	IN	1	The System Clock.
nRST	IN	1	This is an asynchronous, active-low system reset. When this line is low(logic ‘0’) all registers/ flip-flops

			in the device must reset to their initial values
ecc1_Start	IN	1	An active-high signal that indicates that ECC should be run to generate the public key
ecc2_start	IN	1	An active-high signal that indicates that ECC should be run to generate the session key
des_start	IN	1	An active-high signal that indicates that DES should be run.
PoX	IN	164	The x value of our generated key from the ECC module
PoY	IN	164	The y value of our generated key from the ECC module
estart	OUT	1	The signal sent to the ECC module to tell it to begin key generation
ecc1_done	OUT	1	A signal to indicate that the public key has been generated.
ecc2_done	OUT	1	A signal to indicate that the session key has been generated.
des_done	OUT	1	A signal to indicate that the all the data has been encrypted
PuX	OUT	164	The x value of our generated Public key
PuY	OUT	164	The y value of our generated Public key
Keys	OUT	192	The keys being sent to the Triple DES module to be used for encryption

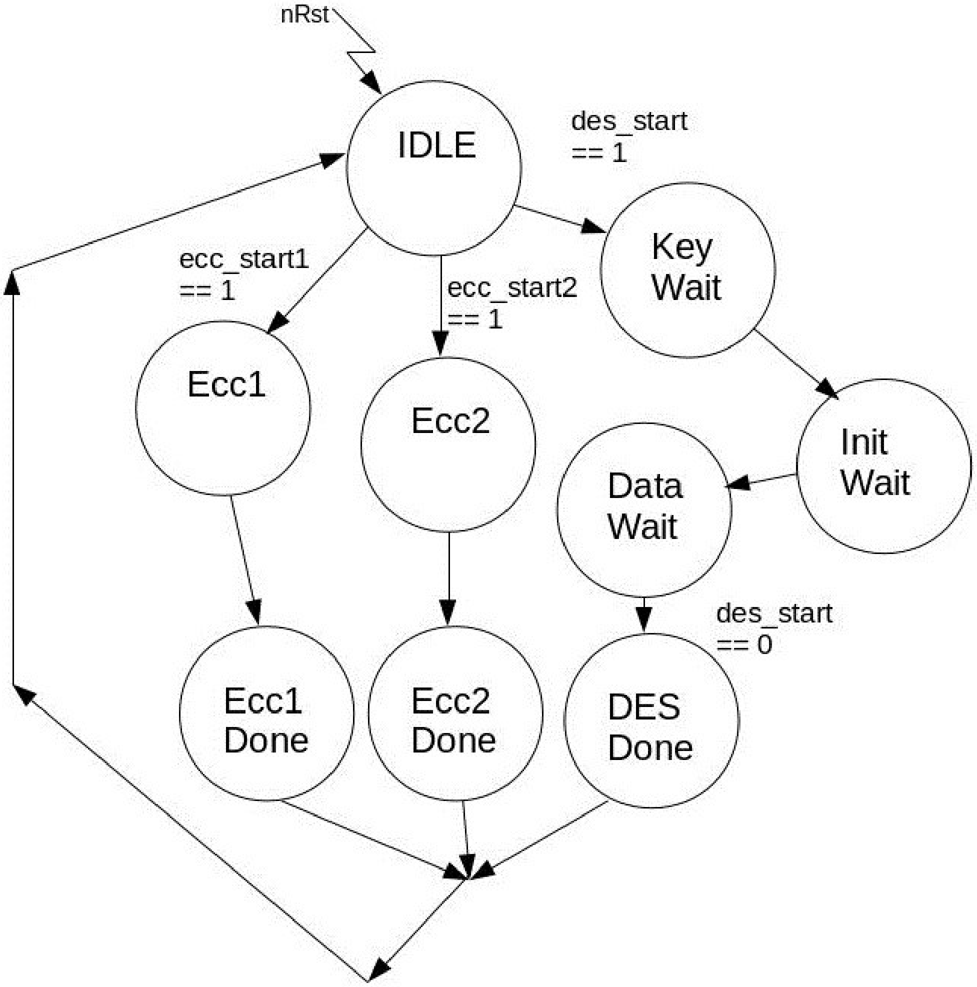
Requirements

In our project we prioritized on secure and quick encryption of data. In order to make it secure we are using an Elliptical Curve Cryptography implementation of the Diffie-Hellman key exchange protocol. This implementation allows for two parties to generate the same session key without ever having to put the key on the wire. This makes it almost impossible for someone to guess the session key. This chip is designed to be used as a slave, where the master will control getting the public key from the party of which you intend to communicate, as well as sending data to SRAM for our chip to encrypt. We intended for our chip to be interfaced with a master using an Avalon Bus module. We optimized our chip for speed by doing computations in parallel, minimizing the number of states on our state machines, and minimizing the size of the combinational blocks. Doing operations in parallel is one of the main advantages of implementing our design in ASIC. Additionally, there were states in the controller and ECC modules that we managed to combine to reduce the overall number of states. We used Moore state machines for all modules that used a state machine. Our ECC algorithm is very computationally complex and when done in software, but when it is implemented in hardware it is much faster because a lot of the logic can be done with shifts and xors. Our chip runs at 200 MHz with 8 bytes of encrypted data being written to SRAM every clock cycle after an initial delay. Our final design had an area under 70 mm^2.

Design Architecture

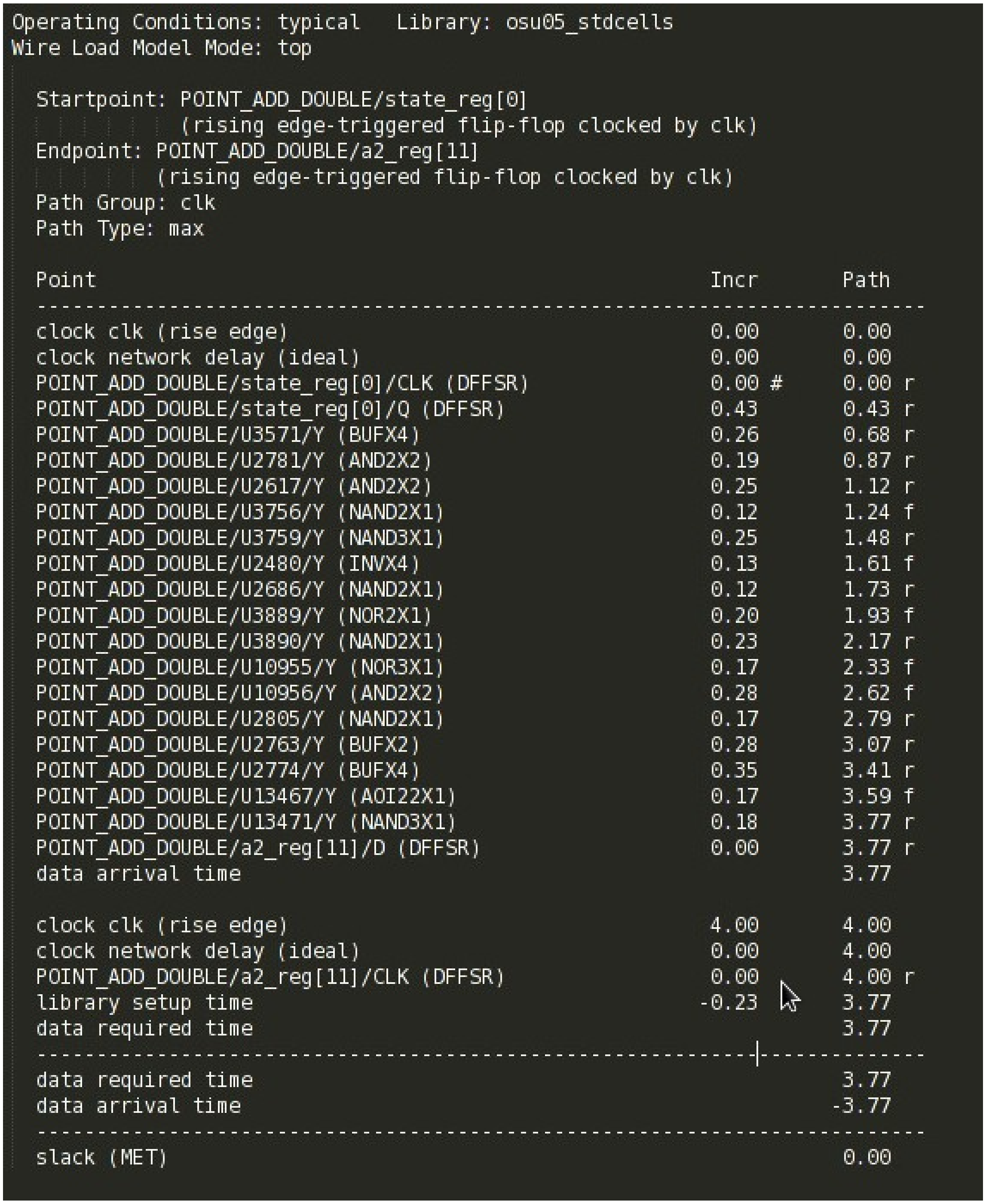


Functional Block Diagrams

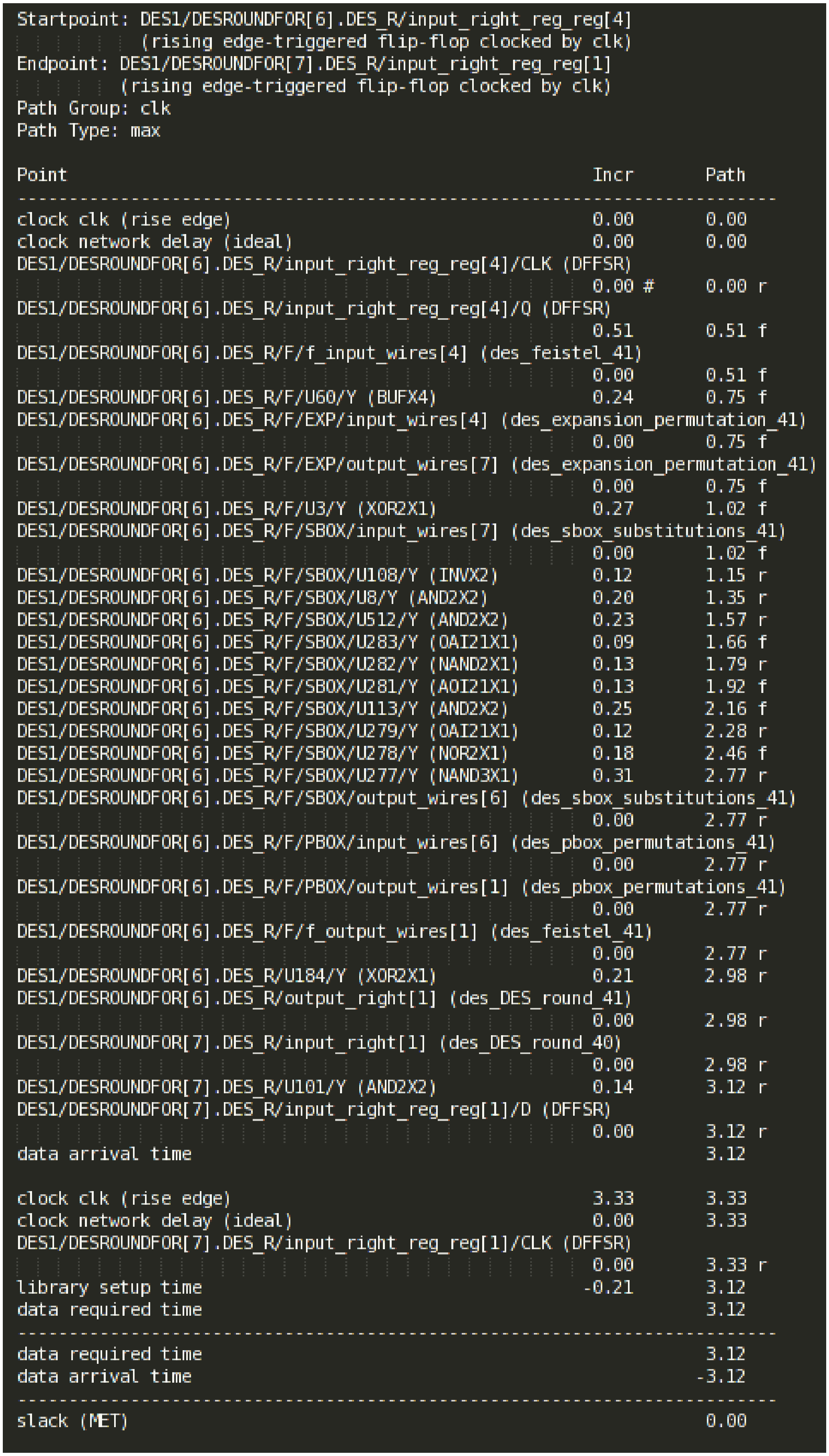


Timing and Area Budgets

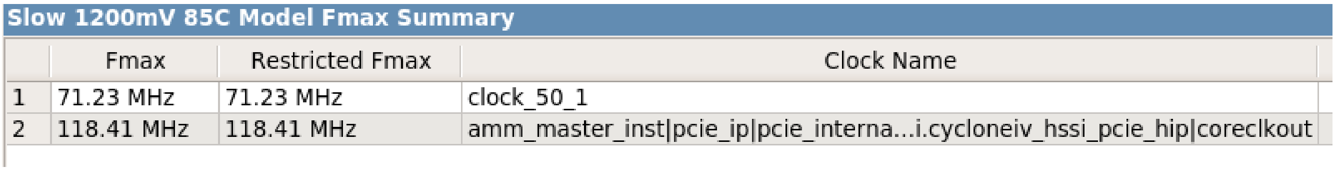
Module	Start location	End location	Delay	Area?
			200MHz	150 mm^2
Point_add_double	State_reg[0]	A2_reg[11]	3.77 ns	
DES/DESRound	Input_right_reg[4]	Input_right_reg[1]	3.12 ns	



```
Operating Conditions: typical   Library: osu05_stdcells
Wire Load Model Mode: top

  Startpoint: POINT_ADD_DOUBLE/state_reg[0]
              (rising edge-triggered flip-flop clocked by clk)
  Endpoint: POINT_ADD_DOUBLE/a2_reg[11]
            (rising edge-triggered flip-flop clocked by clk)
  Path Group: clk
  Path Type: max

  Point                                                   Incr       Path
  --------------------------------------------------------------------------
  clock clk (rise edge)                                   0.00       0.00
  clock network delay (ideal)                             0.00       0.00
  POINT_ADD_DOUBLE/state_reg[0]/CLK (DFFSR)               0.00 #     0.00 r
  POINT_ADD_DOUBLE/state_reg[0]/Q (DFFSR)                 0.43       0.43 r
  POINT_ADD_DOUBLE/U3571/Y (BUFX4)                        0.26       0.68 r
  POINT_ADD_DOUBLE/U2781/Y (AND2X2)                       0.19       0.87 r
  POINT_ADD_DOUBLE/U2617/Y (AND2X2)                       0.25       1.12 r
  POINT_ADD_DOUBLE/U3756/Y (NAND2X1)                      0.12       1.24 f
  POINT_ADD_DOUBLE/U3759/Y (NAND3X1)                      0.25       1.48 r
  POINT_ADD_DOUBLE/U2480/Y (INVX4)                        0.13       1.61 f
  POINT_ADD_DOUBLE/U2686/Y (NAND2X1)                      0.12       1.73 r
  POINT_ADD_DOUBLE/U3889/Y (NOR2X1)                       0.20       1.93 f
  POINT_ADD_DOUBLE/U3890/Y (NAND2X1)                      0.23       2.17 r
  POINT_ADD_DOUBLE/U10955/Y (NOR3X1)                      0.17       2.33 f
  POINT_ADD_DOUBLE/U10956/Y (AND2X2)                      0.28       2.62 f
  POINT_ADD_DOUBLE/U2805/Y (NAND2X1)                      0.17       2.79 r
  POINT_ADD_DOUBLE/U2763/Y (BUFX2)                        0.28       3.07 r
  POINT_ADD_DOUBLE/U2774/Y (BUFX4)                        0.35       3.41 r
  POINT_ADD_DOUBLE/U13467/Y (AOI22X1)                     0.17       3.59 f
  POINT_ADD_DOUBLE/U13471/Y (NAND3X1)                     0.18       3.77 r
  POINT_ADD_DOUBLE/a2_reg[11]/D (DFFSR)                   0.00       3.77 r
  data arrival time                                                  3.77

  clock clk (rise edge)                                   4.00       4.00
  clock network delay (ideal)                             0.00       4.00
  POINT_ADD_DOUBLE/a2_reg[11]/CLK (DFFSR)                 0.00       4.00 r
  library setup time                                     -0.23       3.77
  data required time                                                 3.77
  --------------------------------------------------------------------------
  data required time                                                 3.77
  data arrival time                                                 -3.77
  --------------------------------------------------------------------------
  slack (MET)                                                        0.00
```



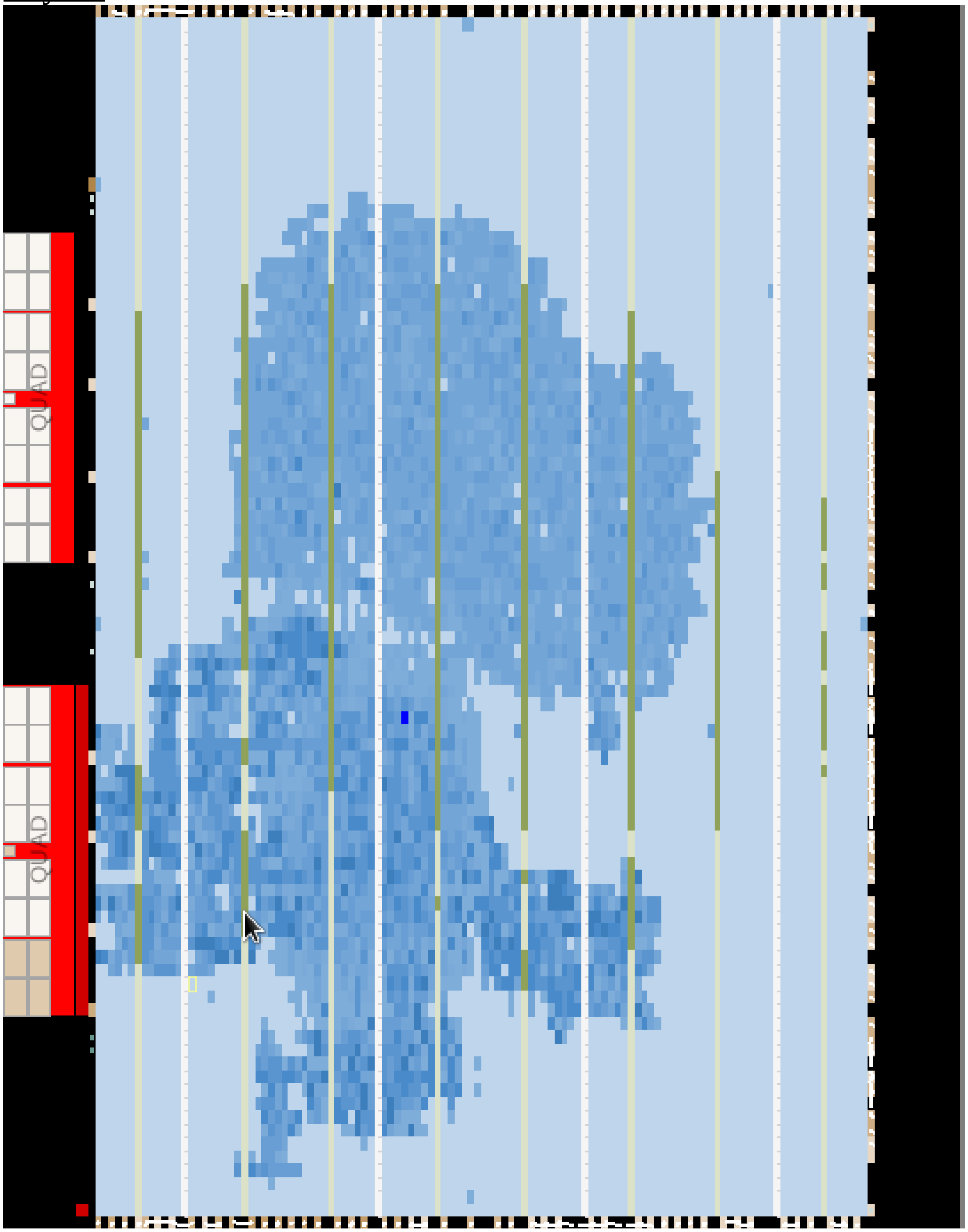
```
Startpoint: DES1/DESROUNDFOR[6].DES_R/input_right_reg_reg[4]
            (rising edge-triggered flip-flop clocked by clk)
Endpoint: DES1/DESROUNDFOR[7].DES_R/input_right_reg_reg[1]
          (rising edge-triggered flip-flop clocked by clk)
Path Group: clk
Path Type: max

Point                                                   Incr       Path
--------------------------------------------------------------------------
clock clk (rise edge)                                   0.00       0.00
clock network delay (ideal)                             0.00       0.00
DES1/DESROUNDFOR[6].DES_R/input_right_reg_reg[4]/CLK (DFFSR)
                                                        0.00 #     0.00 r
DES1/DESROUNDFOR[6].DES_R/input_right_reg_reg[4]/Q (DFFSR)
                                                        0.51       0.51 f
DES1/DESROUNDFOR[6].DES_R/F/f_input_wires[4] (des_feistel_41)
                                                        0.00       0.51 f
DES1/DESROUNDFOR[6].DES_R/F/U60/Y (BUFX4)               0.24       0.75 f
DES1/DESROUNDFOR[6].DES_R/F/EXP/input_wires[4] (des_expansion_permutation_41)
                                                        0.00       0.75 f
DES1/DESROUNDFOR[6].DES_R/F/EXP/output_wires[7] (des_expansion_permutation_41)
                                                        0.00       0.75 f
DES1/DESROUNDFOR[6].DES_R/F/U3/Y (XOR2X1)               0.27       1.02 f
DES1/DESROUNDFOR[6].DES_R/F/SBOX/input_wires[7] (des_sbox_substitutions_41)
                                                        0.00       1.02 f
DES1/DESROUNDFOR[6].DES_R/F/SBOX/U108/Y (INVX2)         0.12       1.15 r
DES1/DESROUNDFOR[6].DES_R/F/SBOX/U8/Y (AND2X2)          0.20       1.35 r
DES1/DESROUNDFOR[6].DES_R/F/SBOX/U512/Y (AND2X2)        0.23       1.57 r
DES1/DESROUNDFOR[6].DES_R/F/SBOX/U283/Y (OAI21X1)       0.09       1.66 f
DES1/DESROUNDFOR[6].DES_R/F/SBOX/U282/Y (NAND2X1)       0.13       1.79 r
DES1/DESROUNDFOR[6].DES_R/F/SBOX/U281/Y (AOI21X1)       0.13       1.92 f
DES1/DESROUNDFOR[6].DES_R/F/SBOX/U113/Y (AND2X2)        0.25       2.16 f
DES1/DESROUNDFOR[6].DES_R/F/SBOX/U279/Y (OAI21X1)       0.12       2.28 r
DES1/DESROUNDFOR[6].DES_R/F/SBOX/U278/Y (NOR2X1)        0.18       2.46 f
DES1/DESROUNDFOR[6].DES_R/F/SBOX/U277/Y (NAND3X1)       0.31       2.77 r
DES1/DESROUNDFOR[6].DES_R/F/SBOX/output_wires[6] (des_sbox_substitutions_41)
                                                        0.00       2.77 r
DES1/DESROUNDFOR[6].DES_R/F/PBOX/input_wires[6] (des_pbox_permutations_41)
                                                        0.00       2.77 r
DES1/DESROUNDFOR[6].DES_R/F/PBOX/output_wires[1] (des_pbox_permutations_41)
                                                        0.00       2.77 r
DES1/DESROUNDFOR[6].DES_R/F/f_output_wires[1] (des_feistel_41)
                                                        0.00       2.77 r
DES1/DESROUNDFOR[6].DES_R/U184/Y (XOR2X1)               0.21       2.98 r
DES1/DESROUNDFOR[6].DES_R/output_right[1] (des_DES_round_41)
                                                        0.00       2.98 r
DES1/DESROUNDFOR[7].DES_R/input_right[1] (des_DES_round_40)
                                                        0.00       2.98 r
DES1/DESROUNDFOR[7].DES_R/U101/Y (AND2X2)               0.14       3.12 r
DES1/DESROUNDFOR[7].DES_R/input_right_reg_reg[1]/D (DFFSR)
                                                        0.00       3.12 r
data arrival time                                                  3.12

clock clk (rise edge)                                   3.33       3.33
clock network delay (ideal)                             0.00       3.33
DES1/DESROUNDFOR[7].DES_R/input_right_reg_reg[1]/CLK (DFFSR)
                                                        0.00       3.33 r
library setup time                                     -0.21       3.12
data required time                                                 3.12
--------------------------------------------------------------------------
data required time                                                 3.12
data arrival time                                                 -3.12
--------------------------------------------------------------------------
slack (MET)                                                        0.00
```

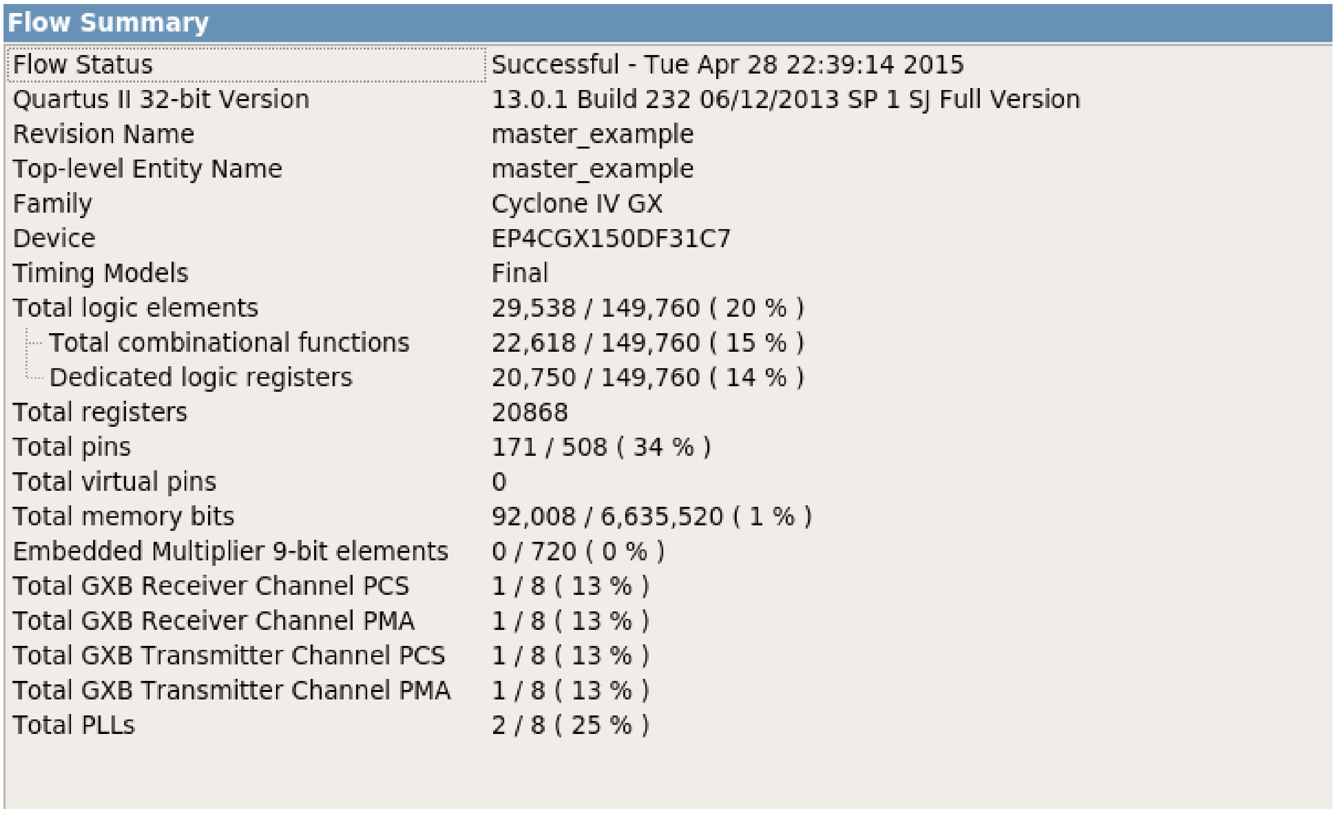


Slow 1200mV 85C Model Fmax Summary

	Fmax	Restricted Fmax	Clock Name
1	71.23 MHz	71.23 MHz	clock_50_1
2	118.41 MHz	118.41 MHz	amm_master_inst|pcie_ip|pcie_interna...i.cycloneiv_hssi_pcie_hip|coreclkout

Layout





Flow Summary

Flow Status	Successful - Tue Apr 28 22:39:14 2015
Quartus II 32-bit Version	13.0.1 Build 232 06/12/2013 SP 1 SJ Full Version
Revision Name	master_example
Top-level Entity Name	master_example
Family	Cyclone IV GX
Device	EP4CGX150DF31C7
Timing Models	Final
Total logic elements	29,538 / 149,760 (20 %)
Total combinational functions	22,618 / 149,760 (15 %)
Dedicated logic registers	20,750 / 149,760 (14 %)
Total registers	20868
Total pins	171 / 508 (34 %)
Total virtual pins	0
Total memory bits	92,008 / 6,635,520 (1 %)
Embedded Multiplier 9-bit elements	0 / 720 (0 %)
Total GXB Receiver Channel PCS	1 / 8 (13 %)
Total GXB Receiver Channel PMA	1 / 8 (13 %)
Total GXB Transmitter Channel PCS	1 / 8 (13 %)
Total GXB Transmitter Channel PMA	1 / 8 (13 %)
Total PLLs	2 / 8 (25 %)

Results

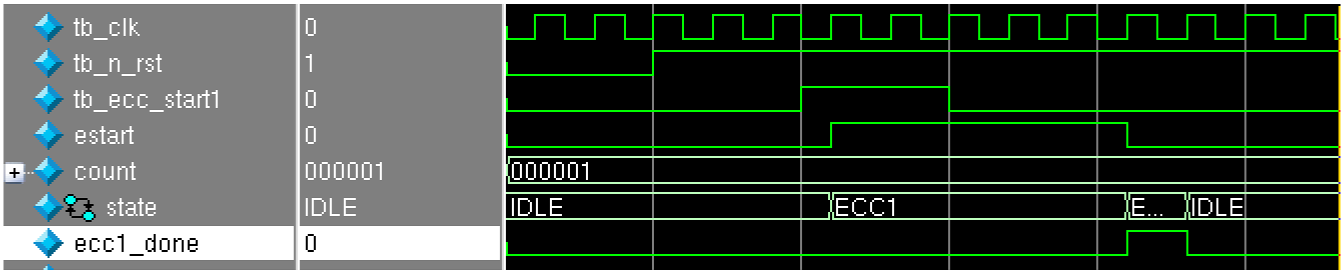
Fixed Success Criteria:

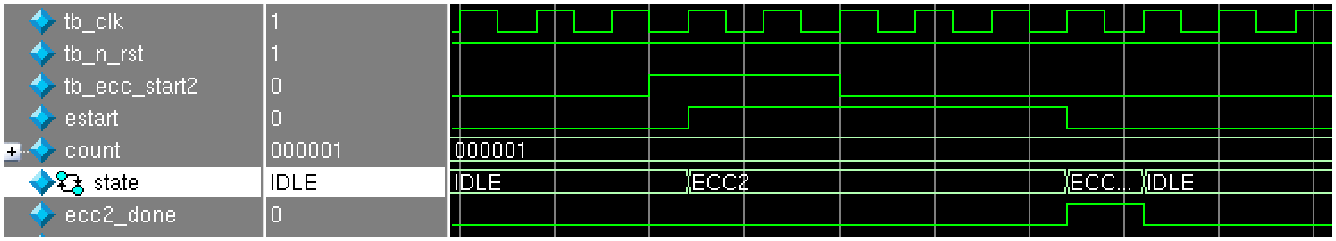
1. Test benches exist for all top level components and the entire design. The test benches for the entire design can be demonstrated or documented to cover all of the functional requirements given in the design specific success criteria.
   -Completed
2. Entire design synthesizes completely, without any inferred latches, timing arcs, and, sensitivity list warnings.
   -Completed
3. Source and mapped version of the complete design behave the same for all test cases. The mapped version simulates without timing errors except at time zero.
   -Completed
4. A complete IC layout is produced that passes all geometry and connectivity checks.
   -Completed
5. The entire design complies with targets for area, pin count, throughput(if applicable), and clock rate. The final targets for these parameters will be determined by the course staff based on your design review. Failure to reach any of the targets will result a score of 1 out of 2 provided that you are within 50% on area, 10% on pin count, and 25% on throughput. Doing worse in any category will result in a score of 0 out of 2.
   a) Area: 70mm^2
   -Completed
   b) Pin Count: 150
   -Completed
   c) Clock Period: 5.0 ns
   -Completed

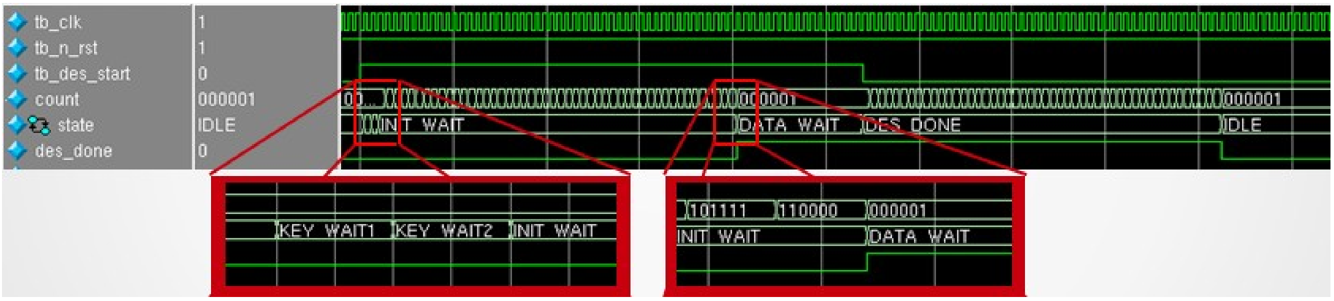
Design Specific Success Criteria (DSSC):

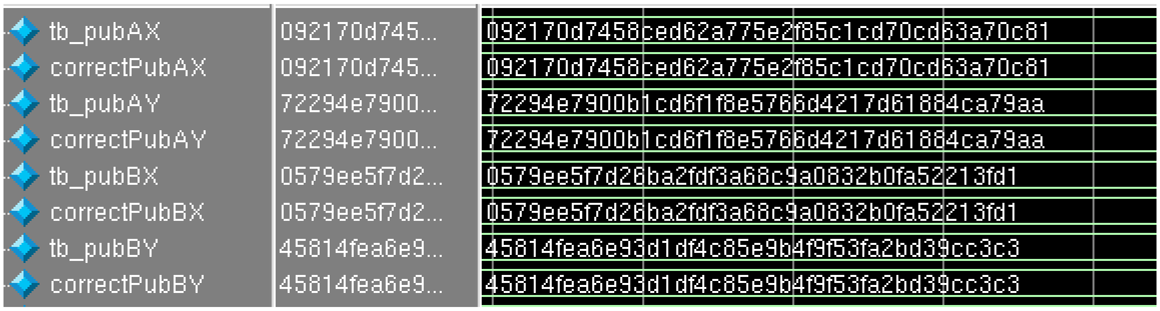
1. Demonstrate by simulation of a Verilog test bench that the public key of A that is generated is correct.
   -Completed
2. Demonstrate by simulation of a Verilog test bench that the values of Skx and Sky are both generated correctly.
   -Completed
3. Demonstrate by simulation of a Verilog test bench that given a key, the Triple DES encryption gives out the correct values.
   -Completed
4. Demonstrate by simulation of a Verilog test bench that the chip correctly responds to the input of keys, as well as raw data.
   -Completed
5. Demonstrate by simulation of a Verilog test bench that the controller correctly transitions through its states.
   -Completed

Appendix B

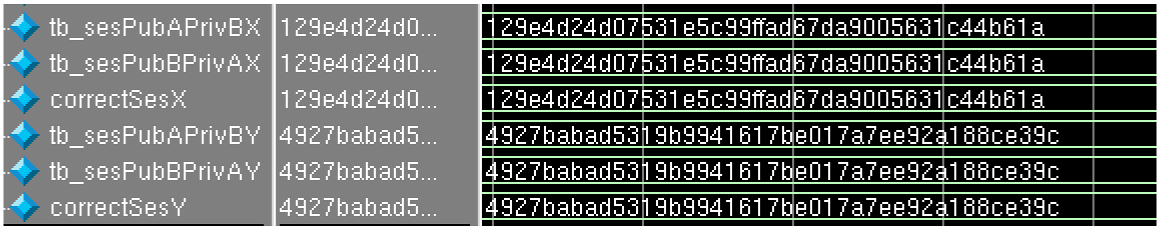




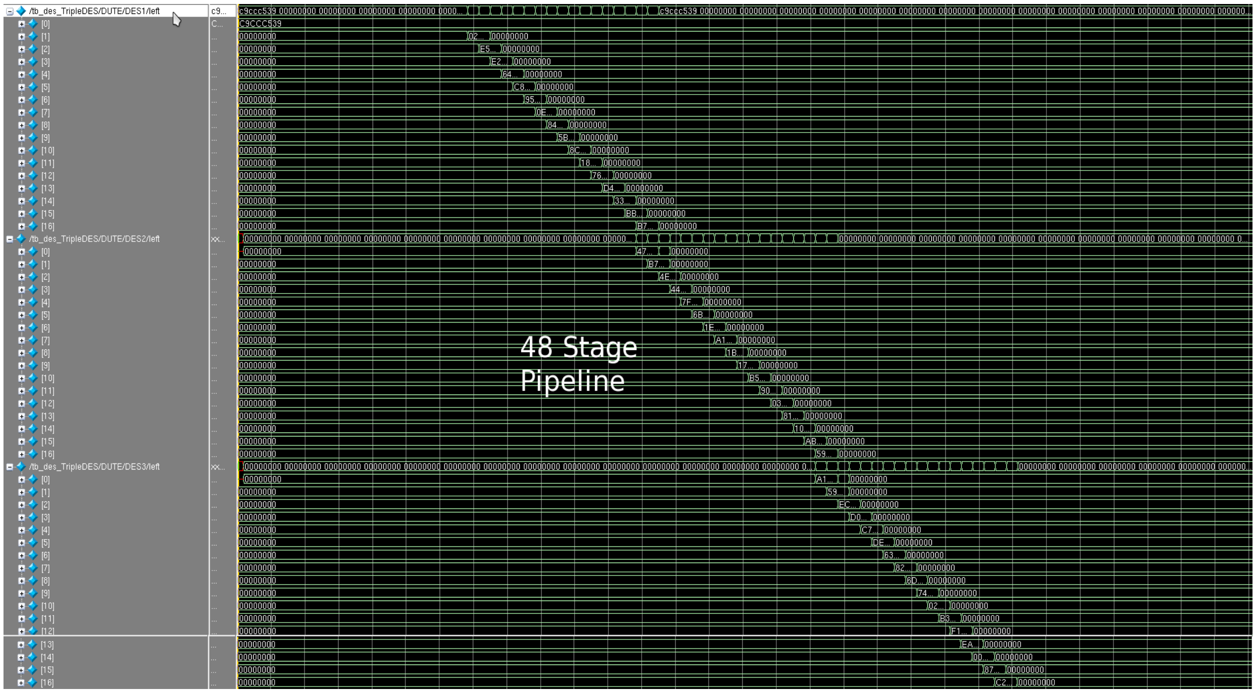


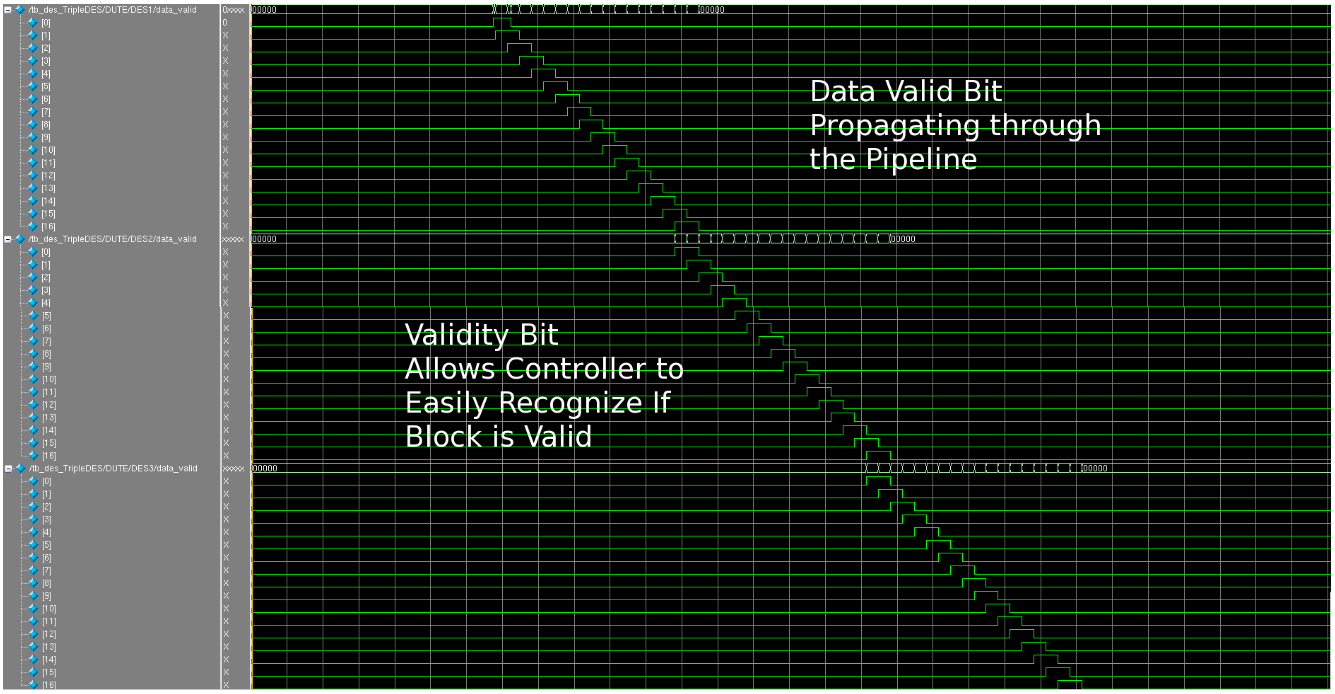


```
tb_pubAX        092170d745...  092170d7458ced62a775e2f85c1cd70cd63a70c81
correctPubAX    092170d745...  092170d7458ced62a775e2f85c1cd70cd63a70c81
tb_pubAY        72294e7900...  72294e7900b1cd6f1f8e5766d4217d61884ca79aa
correctPubAY    72294e7900...  72294e7900b1cd6f1f8e5766d4217d61884ca79aa
tb_pubBX        0579ee5f7d2... 0579ee5f7d26ba2fdf3a68c9a0832b0fa52213fd1
correctPubBX    0579ee5f7d2... 0579ee5f7d26ba2fdf3a68c9a0832b0fa52213fd1
tb_pubBY        45814fea6e9... 45814fea6e93d1df4c85e9b4f9f53fa2bd39cc3c3
correctPubBY    45814fea6e9... 45814fea6e93d1df4c85e9b4f9f53fa2bd39cc3c3
```



```
tb_sesPubAPrivBX  129e4d24d0...  129e4d24d07531e5c99ffad67da9005631c44b61a
tb_sesPubBPrivAX  129e4d24d0...  129e4d24d07531e5c99ffad67da9005631c44b61a
correctSesX       129e4d24d0...  129e4d24d07531e5c99ffad67da9005631c44b61a
tb_sesPubAPrivBY  4927babad5...  4927babad5319b9941617be017a7ee92a188ce39c
tb_sesPubBPrivAY  4927babad5...  4927babad5319b9941617be017a7ee92a188ce39c
correctSesY       4927babad5...  4927babad5319b9941617be017a7ee92a188ce39c
```


/tb_des_TripleDES/DUTE/DES1/left
/tb_des_TripleDES/DUTE/DES2/left
/tb_des_TripleDES/DUTE/DES3/left
48 Stage Pipeline


/tb_des_TripleDES/DUTE/DES1/data_valid
[0]
[1]
[2]
[3]
[4]
[5]
[6]
[7]
[8]
[9]
[10]
[11]
[12]
[13]
[14]
[15]
[16]
/tb_des_TripleDES/DUTE/DES2/data_valid
/tb_des_TripleDES/DUTE/DES3/data_valid
00000

Data Valid Bit
Propagating through
the Pipeline

Validity Bit
Allows Controller to
Easily Recognize If
Block is Valid