lab2 report

- Arcuitecture

  DE2_115

  | Rsa 256 Wrapper

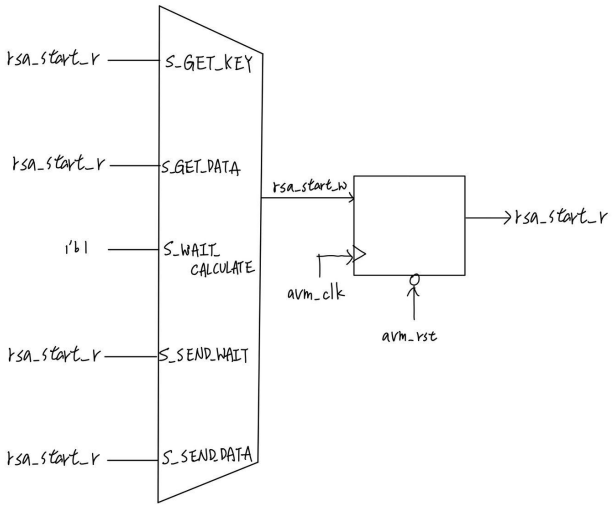
  | Rsa 256 Core

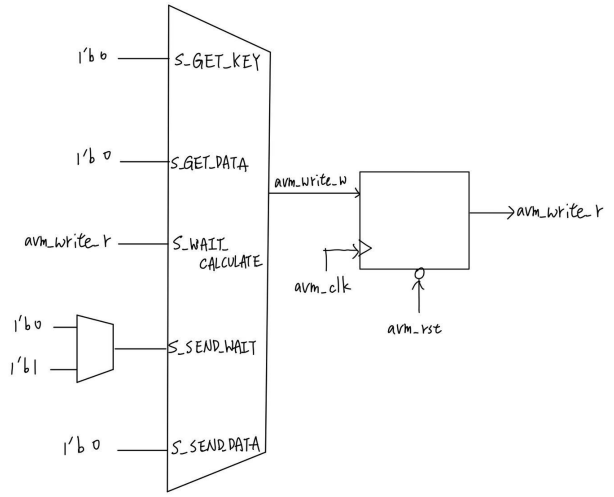
  | Modulo Product

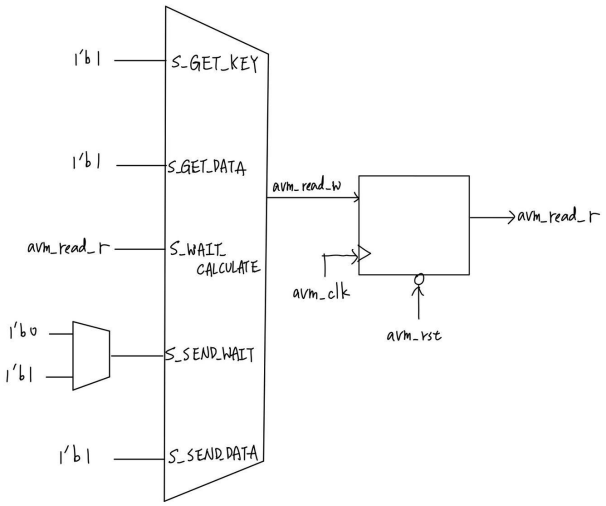
  | Montgemory Algorithm

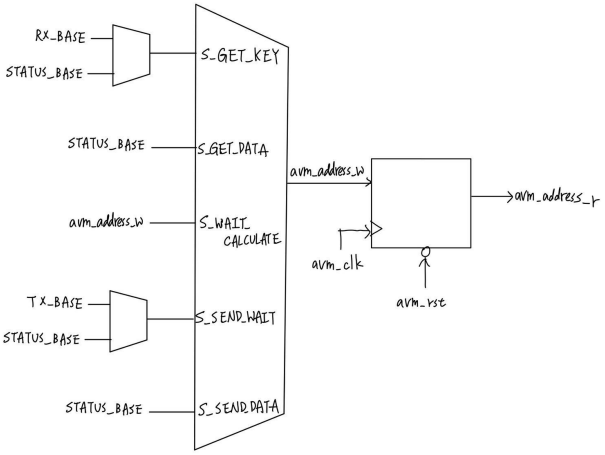
- block diagram

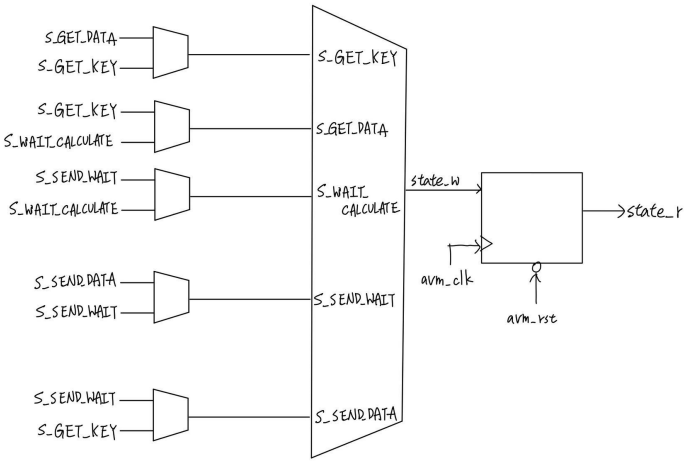
  1.wrapper

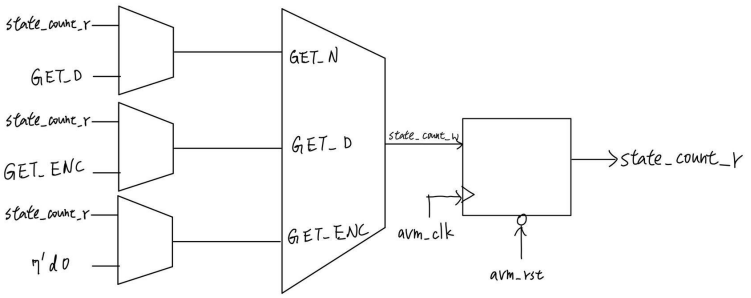


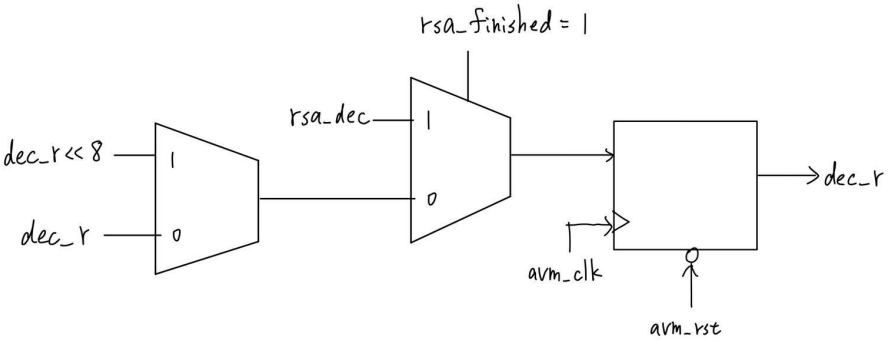


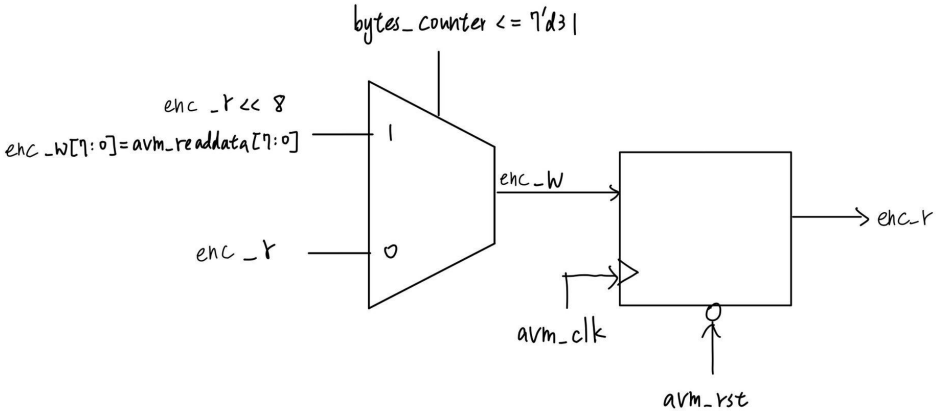

1'b1
S_GET_KEY
1'b1
S_GET_DATA
avm_read_r
S_WAIT_CALCULATE
1'b0
1'b1
S_SEND_WAIT
1'b1
S_SEND_DATA
avm_read_w
avm_read_r
avm_clk
avm_rst

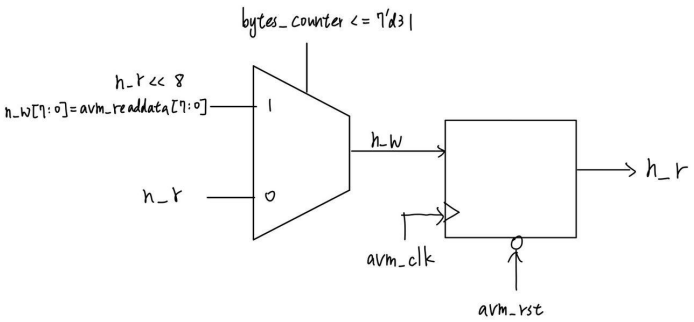

RX_BASE
STATUS_BASE
S_GET_KEY
STATUS_BASE
S_GET_DATA
avm_address_w
S_WAIT_CALCULATE
TX_BASE
STATUS_BASE
S_SEND_WAIT
STATUS_BASE
S_SEND_DATA
avm_address_w
avm_address_r
avm_clk
avm_rst

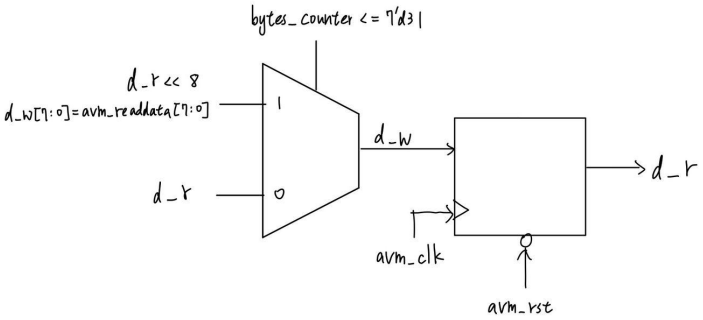

S_GET_DATA
S_GET_KEY
S_GET_KEY
S_WAIT_CALCULATE
S_SEND_WAIT
S_WAIT_CALCULATE
S_SEND_DATA
S_SEND_WAIT
S_SEND_WAIT
S_GET_KEY
S_GET_KEY
S_GET_DATA
S_WAIT_CALCULATE
S_SEND_WAIT
S_SEND_DATA
state_w
state_r
avm_clk
avm_rst

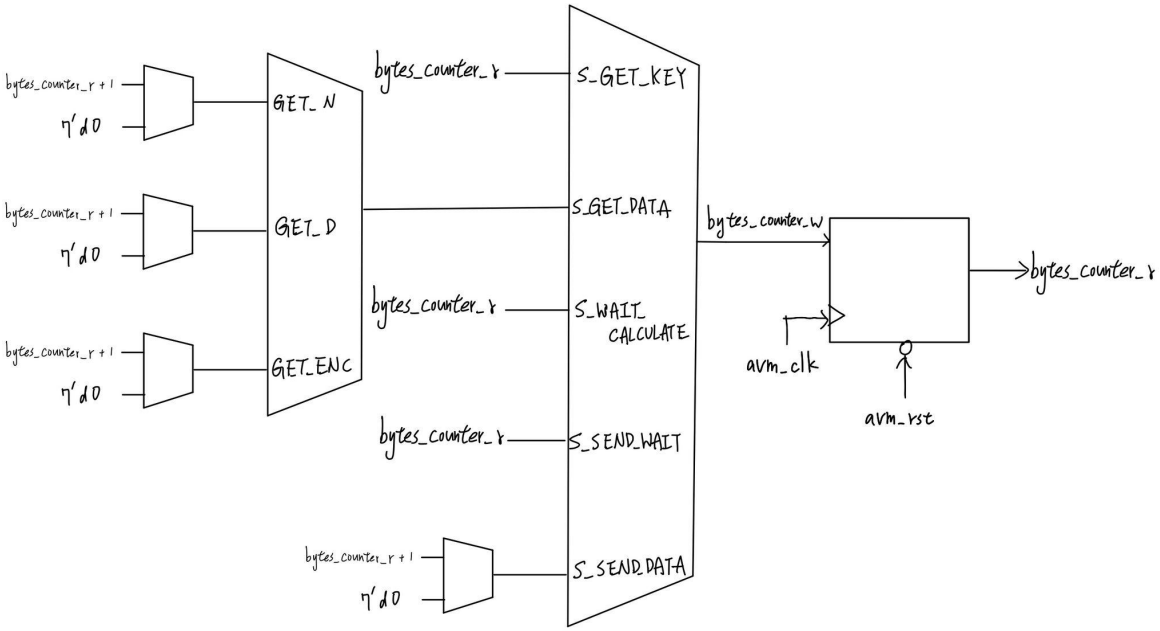

state_count_r
GET_D
state_count_r
GET_ENC
state_count_r
7'd0
GET_N
GET_D
GET_ENC
state_count_w
avm_clk
avm_rst
state_count_r


rsa_finished = 1
rsa_dec
dec_r << 8
1
dec_r
0
1
0
avm_clk
avm_rst
dec_r


bytes_counter <= 7'd31
enc_r << 8
enc_w[7:0]=avm_readdata[7:0]
1
enc_r
0
enc_w
avm_clk
avm_rst
enc_r

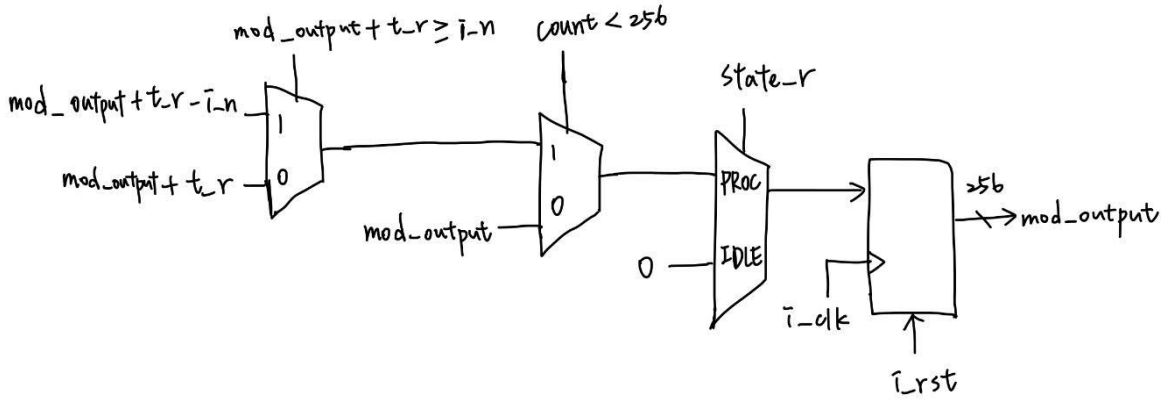

bytes_counter <= 7'd31
n_r << 8
n_w[7:0]=avm_readdata[7:0]
1
n_r
0
n_w
n_r
avm_clk
avm_rst


bytes_counter <= 7'd31
d_r << 8
d_w[7:0]=avm_readdata[7:0]
1
d_r
0
d_w
d_r
avm_clk
avm_rst

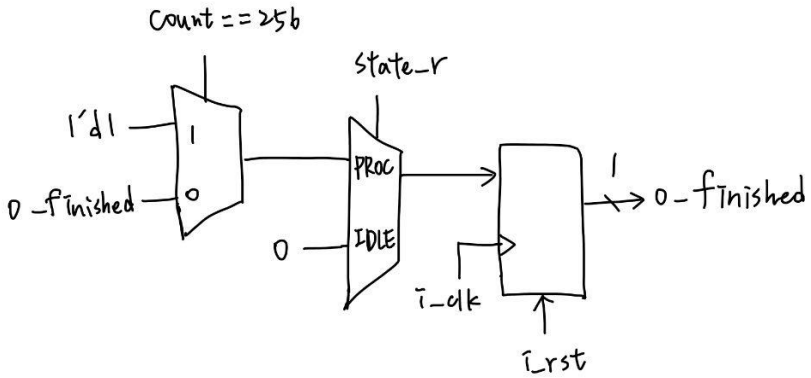

bytes_counter_r + 1
7'd0
bytes_counter_r + 1
7'd0
bytes_counter_r + 1
7'd0
GET_N
GET_D
GET_ENC
bytes_counter_r
S_GET_KEY
S_GET_DATA
bytes_counter_r
S_WAIT_CALCULATE
bytes_counter_r
S_SEND_WAIT
bytes_counter_r + 1
7'd0
S_SEND_DATA
bytes_counter_w
avm_clk
avm_rst
bytes_counter_r

2. core

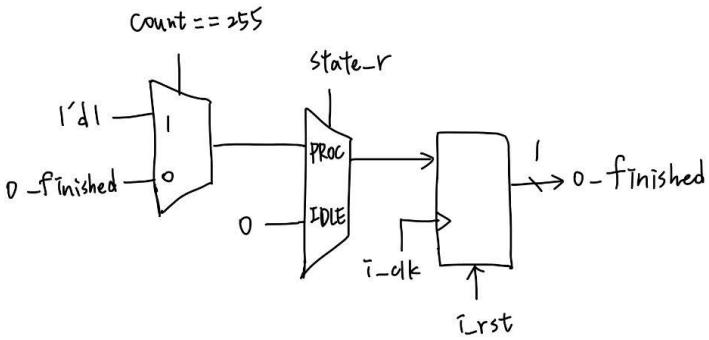
Modulo Product output:



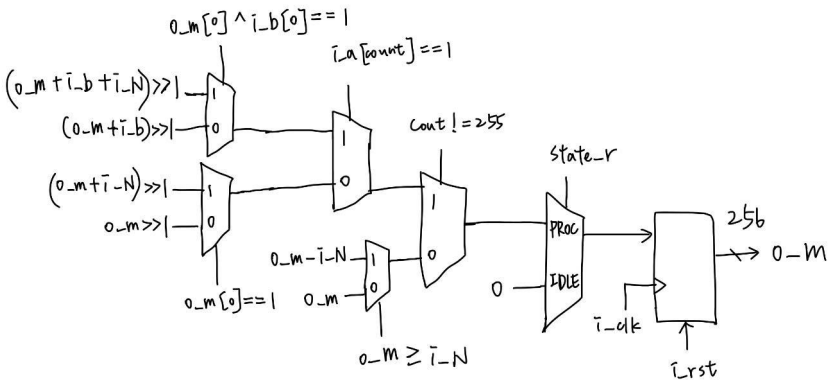
ModuloProduct finish:



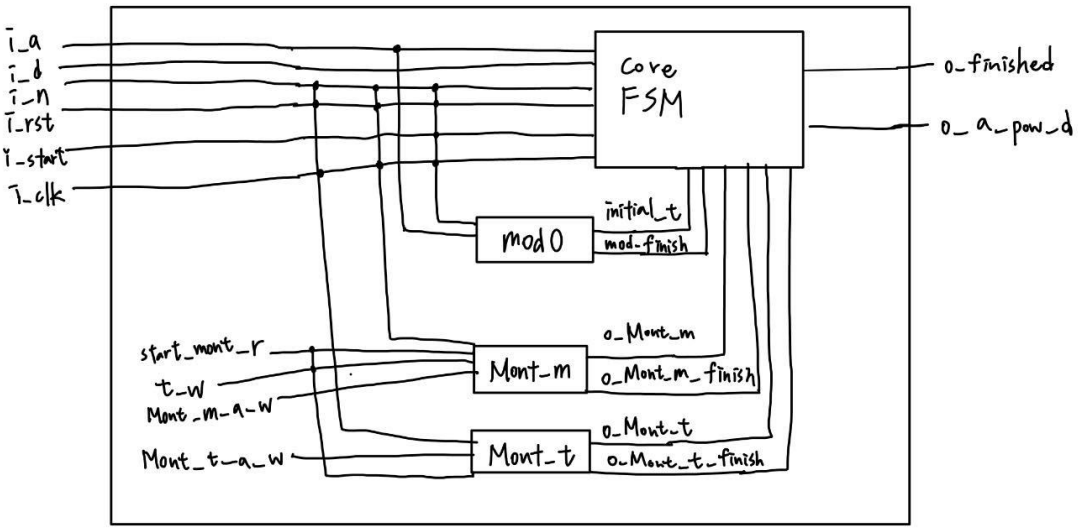
MontgemoryAlgorithm finish:



Montgemory Algorithm output:



Core datapath:



- FSM

  1. wrapper

     get_key: detect read signal.

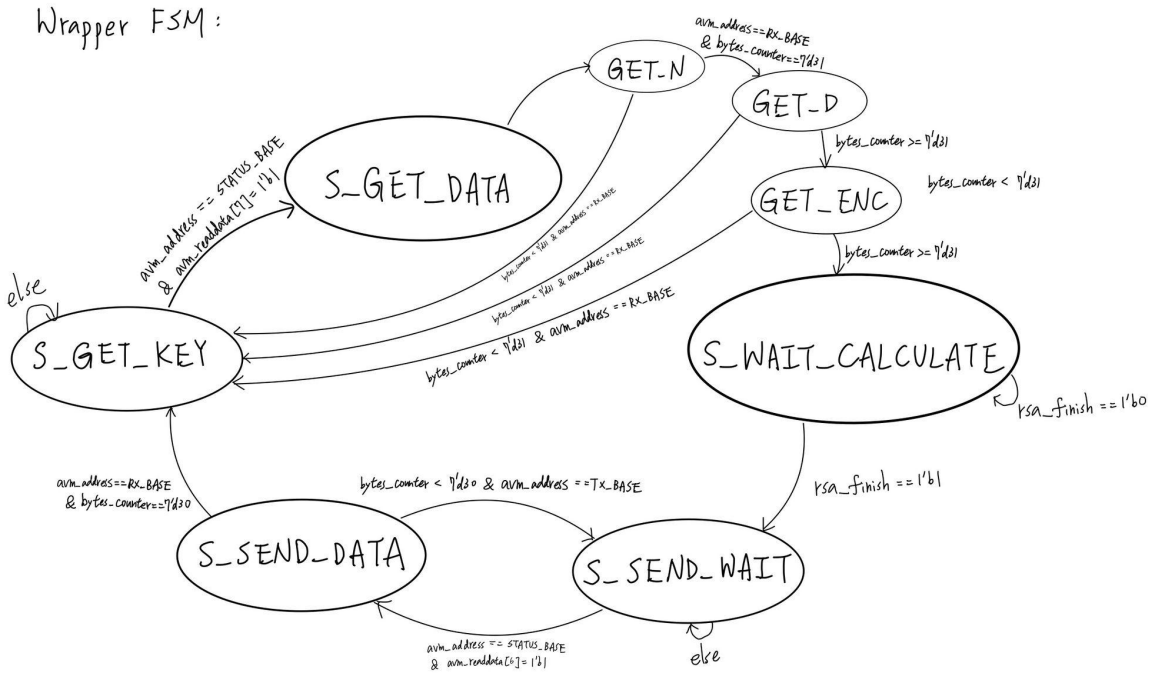
     get_data:read data. get_n get_d get_enc are sub-state in get data, control load location of read data(data is n or d or enc).

     wait_cal: waiting core.

     send_wait: detect write signal.

     send_data: write.

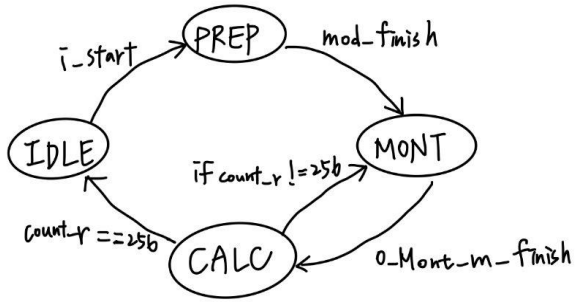
Wrapper FSM:



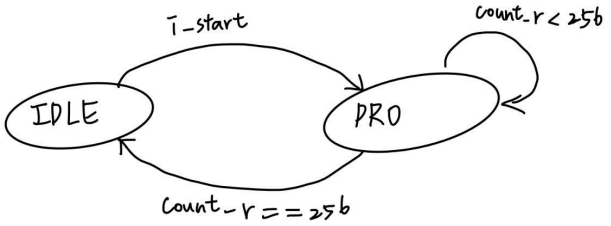
*avm_waitrequest == 0 should be checked before every state transitions

2. core

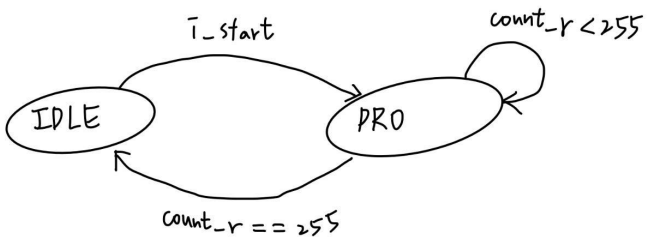
Core FSM:



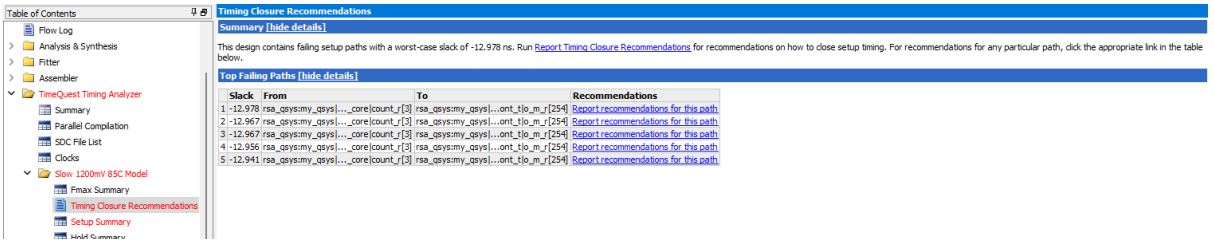
Modulo Product FSM:

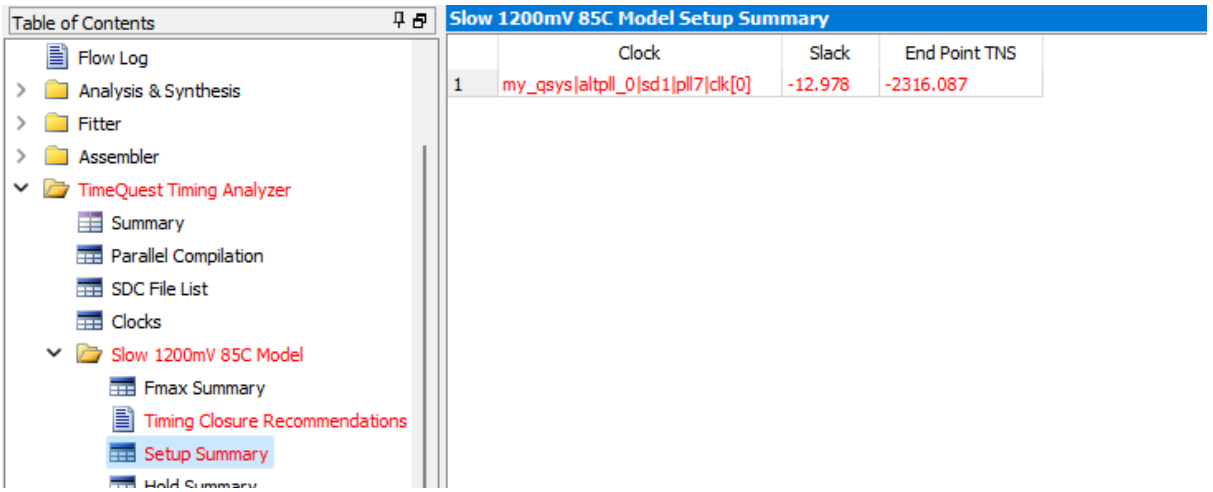


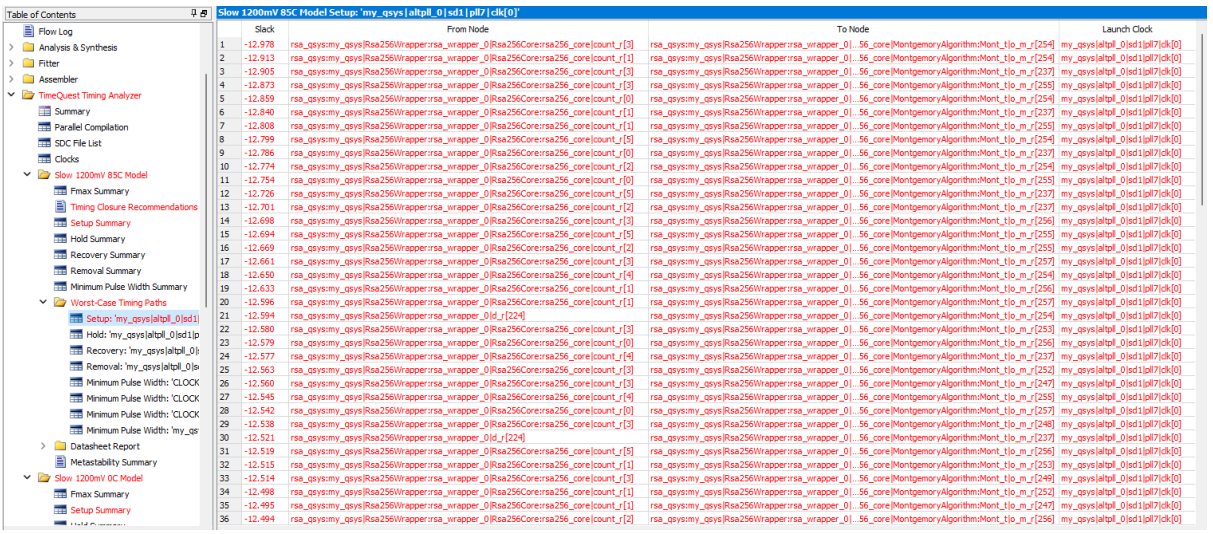
Montgemory Algorithm FSM:



- Timing summary







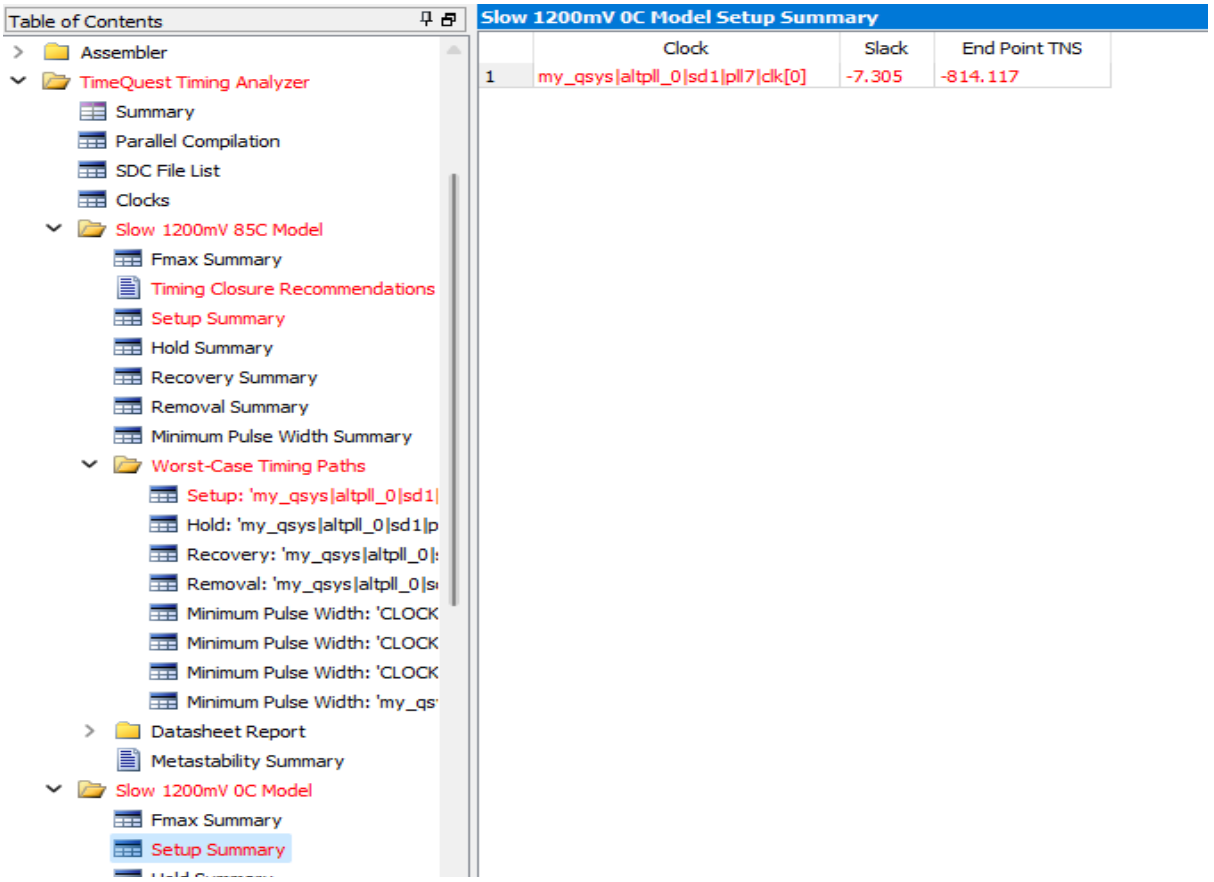


Table of Contents
Assembler
TimeQuest Timing Analyzer
Summary
Parallel Compilation
SDC File List
Clocks
Slow 1200mV 85C Model
Fmax Summary
Timing Closure Recommendations
Setup Summary
Hold Summary
Recovery Summary
Removal Summary
Minimum Pulse Width Summary
Worst-Case Timing Paths
Datasheet Report
Metastability Summary
Slow 1200mV 0C Model
Fmax Summary
Setup Summary
Slow 1200mV 0C Model Setup Summary
Clock
Slack
End Point TNS
1
my_qsys|altpll_0|sd1|pll7|clk[0]
-7.305
-814.117

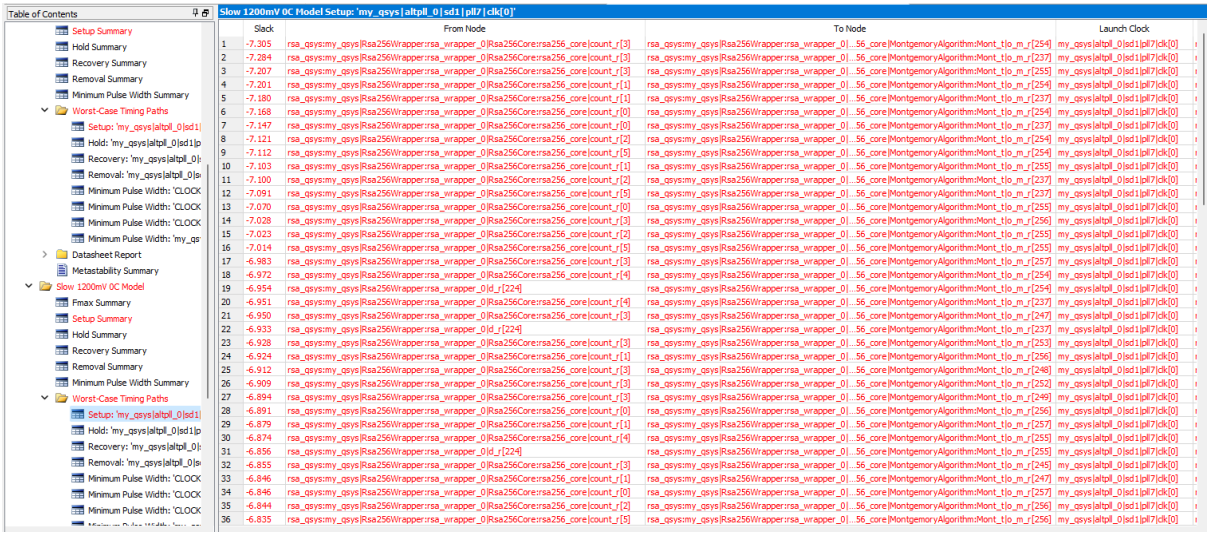


Table of Contents
Slow 1200mV 0C Model Setup: 'my_qsys|altpll_0|sd1|pll7|clk[0]'
Slack
From Node
To Node
Launch Clock

Table of Contents

- Removal: 'my_qsys|altpll_0|s
- Minimum Pulse Width: 'CLOCK
- Minimum Pulse Width: 'CLOCK
- Minimum Pulse Width: 'CLOCK
- Minimum Pulse Width: 'my_qs
- Datasheet Report
- Metastability Summary
- Slow 1200mV 0C Model
  - Fmax Summary
  - Setup Summary
  - Hold Summary
  - Recovery Summary
  - Removal Summary
  - Minimum Pulse Width Summary
  - Worst-Case Timing Paths
    - Setup: 'my_qsys|altpll_0|sd1|
    - Hold: 'my_qsys|altpll_0|sd1|p
    - Recovery: 'my_qsys|altpll_0|
    - Removal: 'my_qsys|altpll_0|s
    - Minimum Pulse Width: 'CLOCK
    - Minimum Pulse Width: 'CLOCK
    - Minimum Pulse Width: 'CLOCK
    - Minimum Pulse Width: 'my_qs
  - Datasheet Report
  - Metastability Summary
- Fast 1200mV 0C Model
- Multicorner Timing Analysis Summary
- Multicorner Datasheet Report Summa

Multicorner Timing Analysis Summary

	Clock	Setup	Hold	Recovery	Removal	Minimum Pulse Width
1	Worst-case Slack	-12.978	0.064	36.194	1.433	9.574
1	CLOCK2_50	N/A	N/A	N/A	N/A	16.000
2	CLOCK3_50	N/A	N/A	N/A	N/A	16.000
3	CLOCK_50	N/A	N/A	N/A	N/A	9.574
4	my_qsys|altpll_0|sd1|pll7|clk[0]	-12.978	0.064	36.194	1.433	19.684
2	Design-wide TNS	-2316.087	0.0	0.0	0.0	0.0
1	CLOCK2_50	N/A	N/A	N/A	N/A	0.000
2	CLOCK3_50	N/A	N/A	N/A	N/A	0.000
3	CLOCK_50	N/A	N/A	N/A	N/A	0.000
4	my_qsys|altpll_0|sd1|pll7|clk[0]	-2316.087	0.000	0.000	0.000	0.000

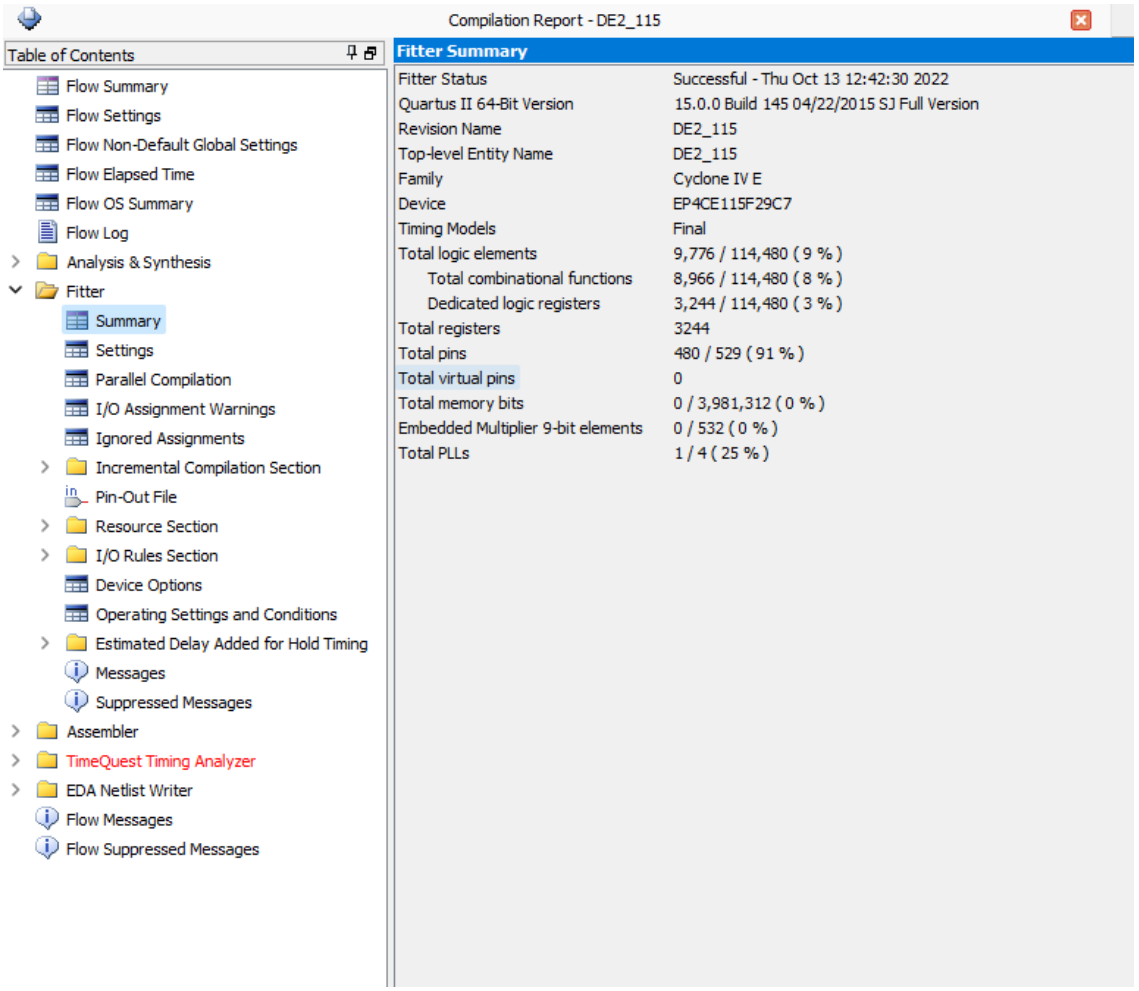
Table of Contents

- Metastability Summary
- Slow 1200mV 0C Model
  - Fmax Summary
  - Setup Summary
  - Hold Summary
  - Recovery Summary
  - Removal Summary
  - Minimum Pulse Width Summary
  - Worst-Case Timing Paths
    - Setup: 'my_qsys|altpll_0|sd1|
    - Hold: 'my_qsys|altpll_0|sd1|p
    - Recovery: 'my_qsys|altpll_0|
    - Removal: 'my_qsys|altpll_0|s
    - Minimum Pulse Width: 'CLOCK
    - Minimum Pulse Width: 'CLOCK
    - Minimum Pulse Width: 'CLOCK
    - Minimum Pulse Width: 'my_qs
  - Datasheet Report
  - Metastability Summary
- Fast 1200mV 0C Model
- Multicorner Timing Analysis Summary
- Multicorner Datasheet Report Summa
- Advanced I/O Timing
- Clock Transfers
- Report TCCS
- Report RSKM
- Unconstrained Paths
- Messages
- EDA Netlist Writer
- Flow Messages
- Flow Suppressed Messages

Unconstrained Paths

	Property	Setup	Hold
1	Illegal Clocks	0	0
2	Unconstrained Clocks	0	0
3	Unconstrained Input Ports	0	0
4	Unconstrained Input Port Paths	0	0
5	Unconstrained Output Ports	1	1
6	Unconstrained Output Port Paths	1	1

- Fitter Summary



- problem solving

1. Wrapper:

在寫wrapper遇到最大的問題是，在剛開始讀資料的時候一直沒有辦法接收到readdata且一直遇到simulation abort，後來發現是因為waitrequest的問題，一開始以為只有看status的時候才會需要讀waitrequest，但是後來發現read之前write之前也都需要等waitrequest，以上是第一個問題。

之後修好讀寫問題之後發現wrapper的sub-state控制會導致讀資料少讀，原本在get_n的時候是偵測到byte_count為31的時候才跳轉，但是這樣的話有一筆資料就會被忽略，解決方法就是調整sub-state的跳轉，byte_count是30的時候就要跳到get_d以此類推。

最後在寫資料的時候一直會多讀一筆，但最後想起來好像有兩個byte會是0所以少write一次之後就成功了。

2. Core:

在寫core的時候一開始有遇到資料讀不到的問題，導致output一直都卡在零，後來發現是submole和core之間接線的問題所造成。之後可以讀到input後，發現會一直算錯，後來檢查發現是submodule裡面出現overflow, 需要把一些register的bit數調大，同時也要注意最後存到輸出值的時候索取的bit位置。

一開始我們用core裡面的信號去判斷現在進行到的步驟，好讓FSM知道要跳到或維持在哪個state，但是後來發現這樣的寫法有點麻煩且容易出錯，於是後來我們改成在submodule裡面額外加上start的input訊號和finish的output訊號，這樣就可以更清楚的知道每個submodule各自進行到哪裡，在core裡面判斷FSM的下一步是哪個state時也可以直接讀到。