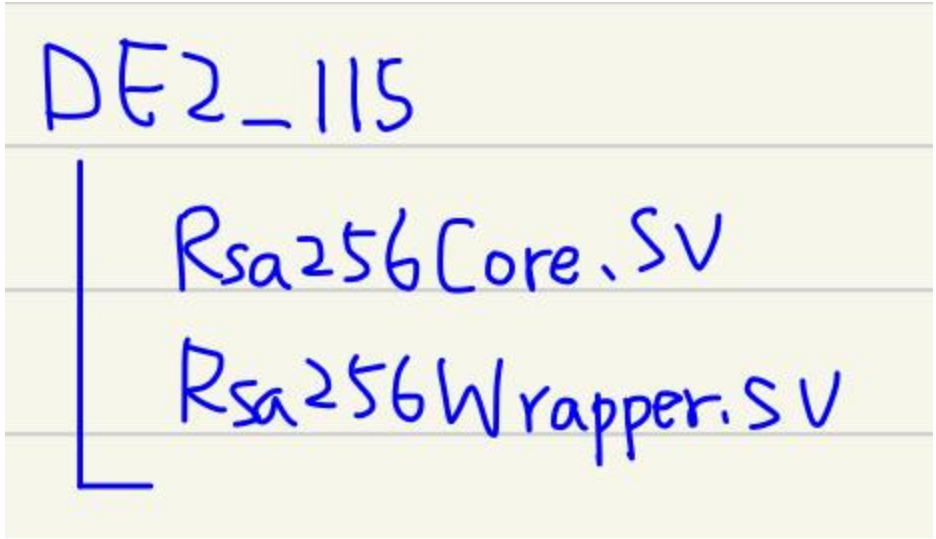
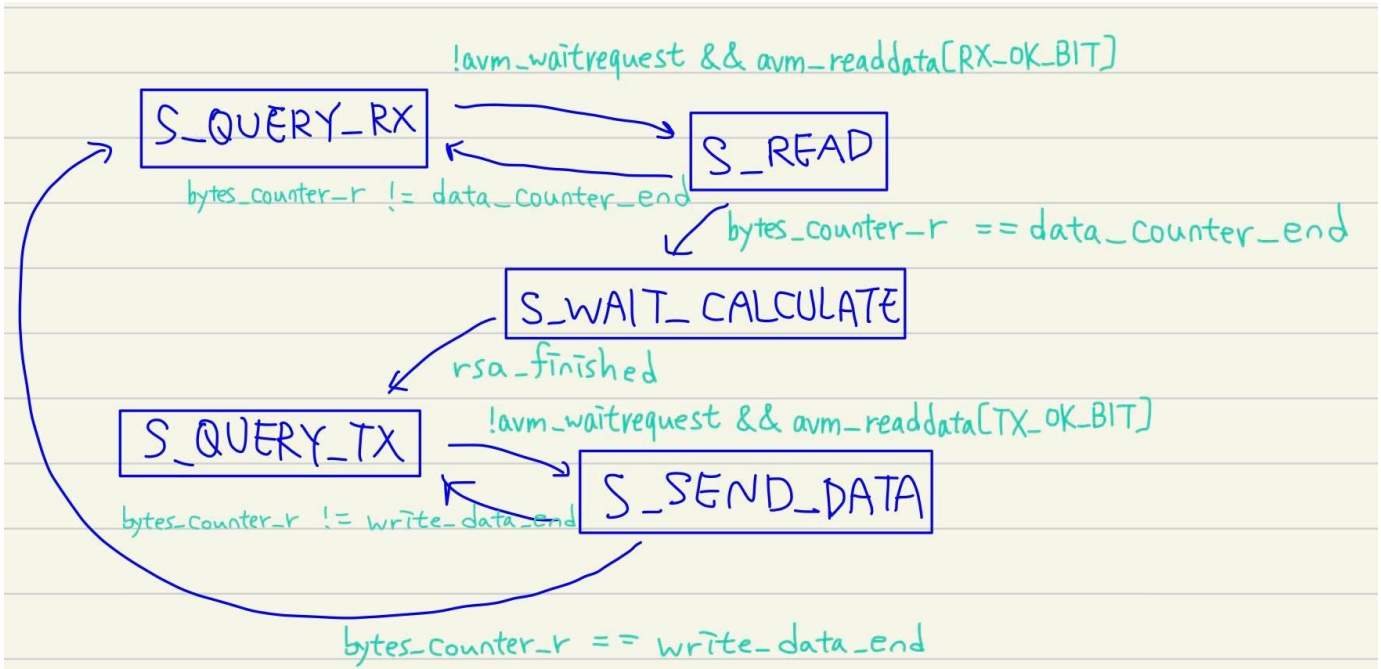
team05_lab2_report

b08901056 盧弘偉
b08901069 黃政勛
b08901175 郭柏言

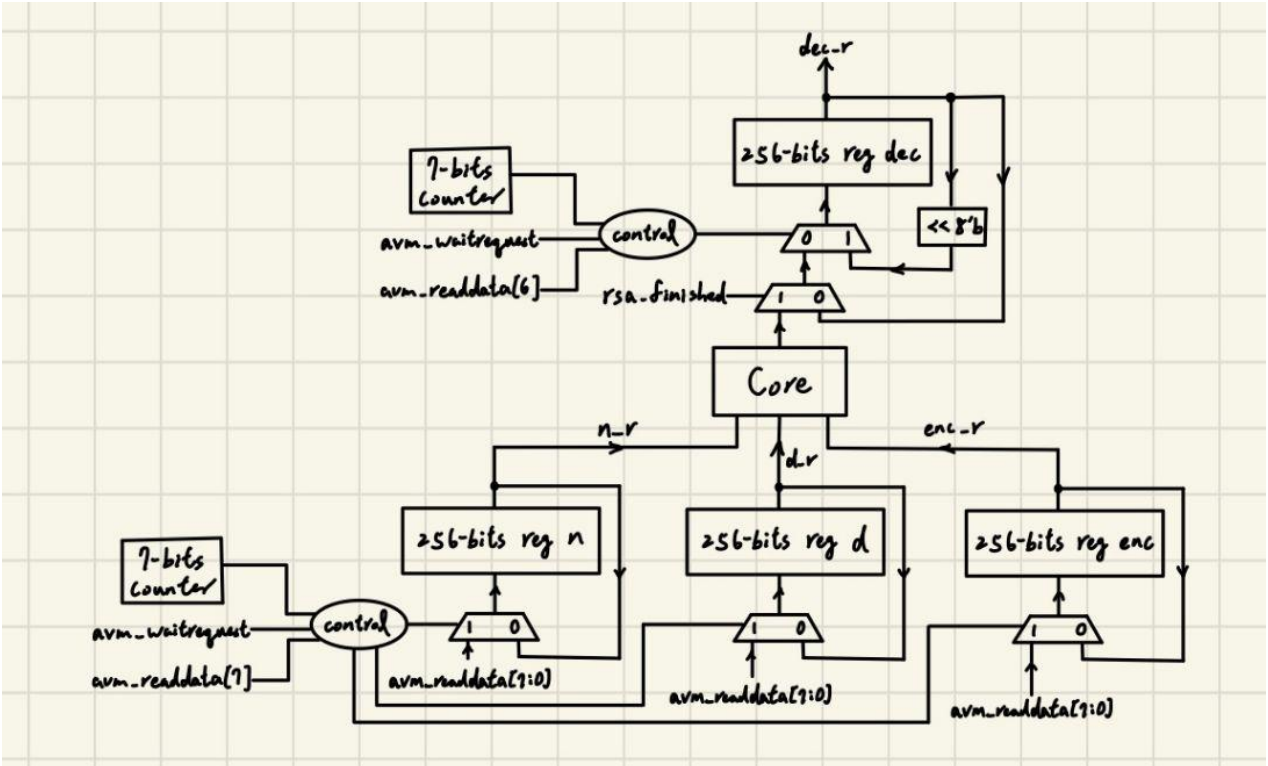
層級架構



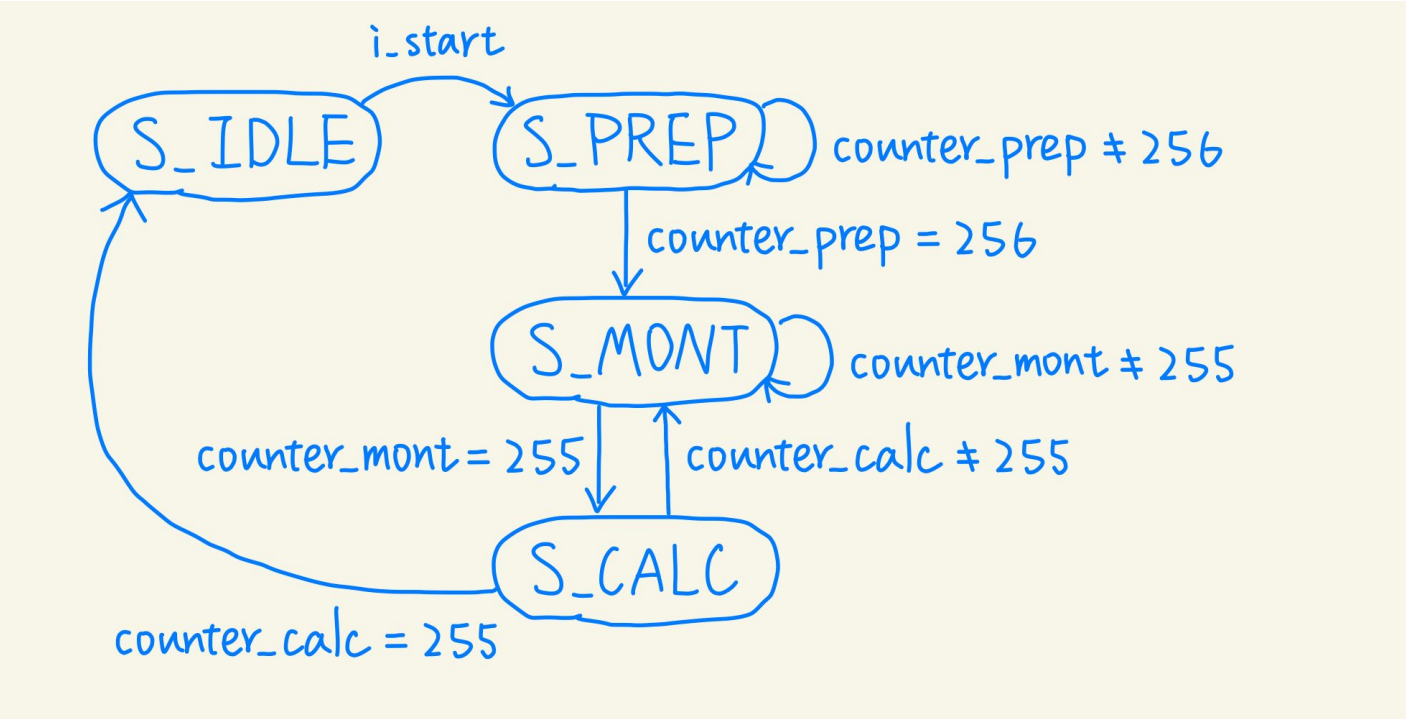
FSM - Wrapper


!avm_waitrequest && avm_readdata[RX_OK_BIT]
S_QUERY_RX
S_READ
bytes_counter_r != data_counter_end
bytes_counter_r == data_counter_end
S_WAIT_CALCULATE
rsa_finished
S_QUERY_TX
!avm_waitrequest && avm_readdata[TX_OK_BIT]
S_SEND_DATA
bytes_counter_r != write_data_end
bytes_counter_r == write_data_end

Block Diagram - Wrapper

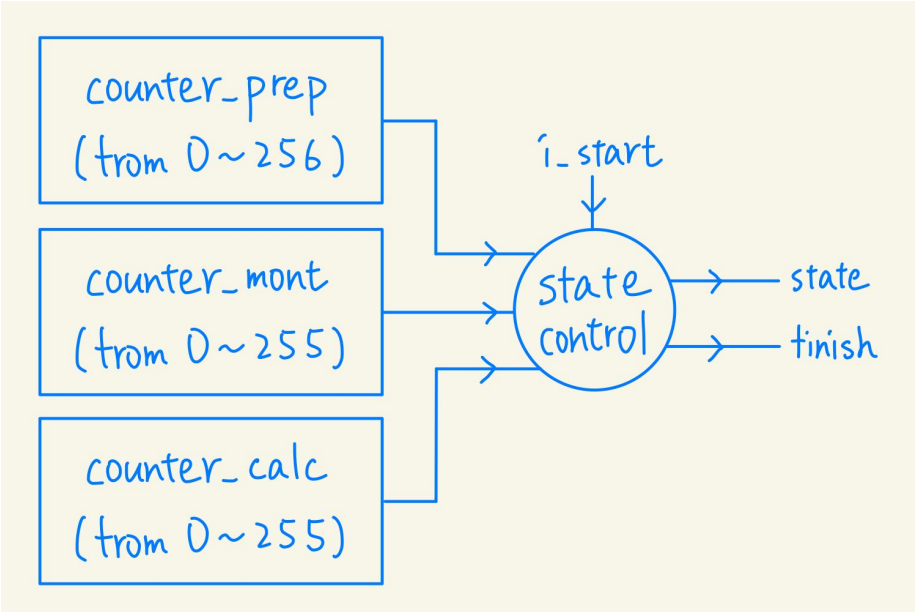


FSM - Core


i_start
S_IDLE
S_PREP
counter_prep ≠ 256
counter_prep = 256
S_MONT
counter_mont ≠ 255
counter_mont = 255
counter_calc ≠ 255
S_CALC
counter_calc = 255

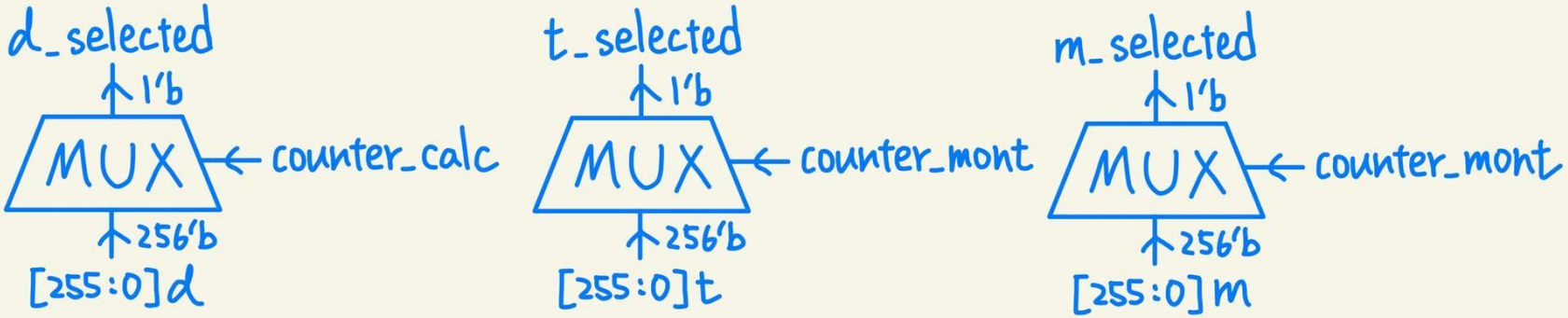
Block Diagram - Core

Three counters for states change control.



Block Diagram - Core

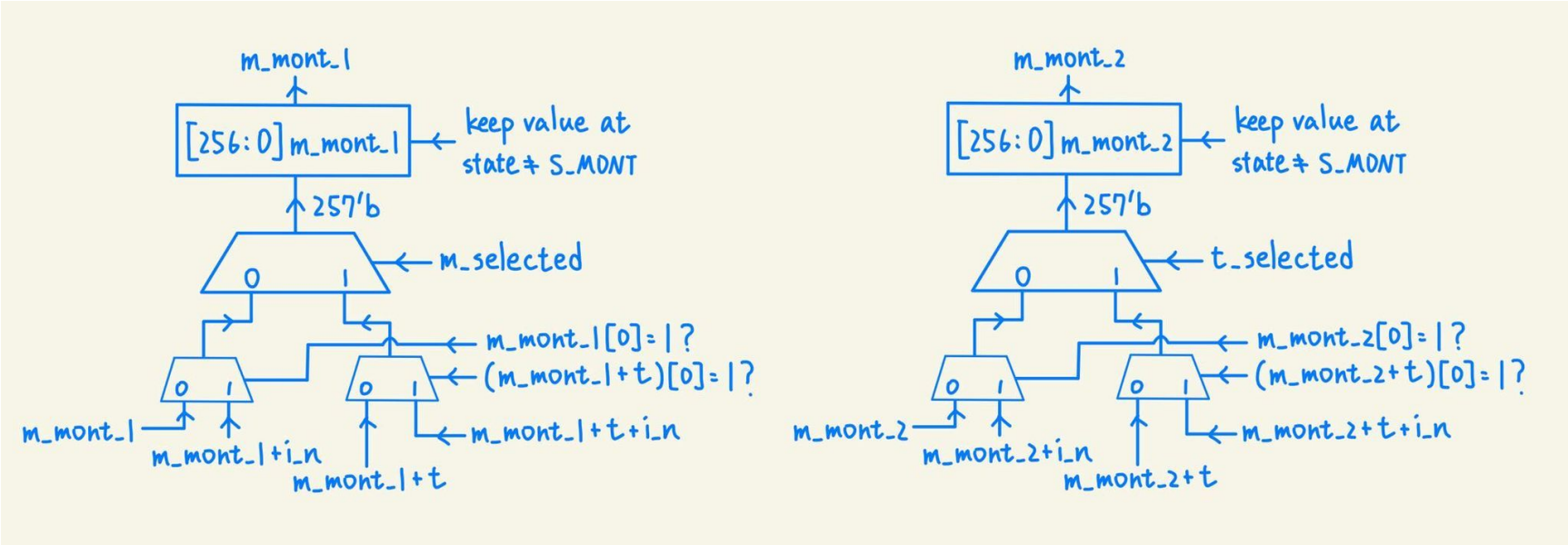
Three 256-1 MUX select i’th bit of d, t, and m.



Block Diagram - Core

Register m_mont_1 caculate (m*t*2^-256) mod i_n.

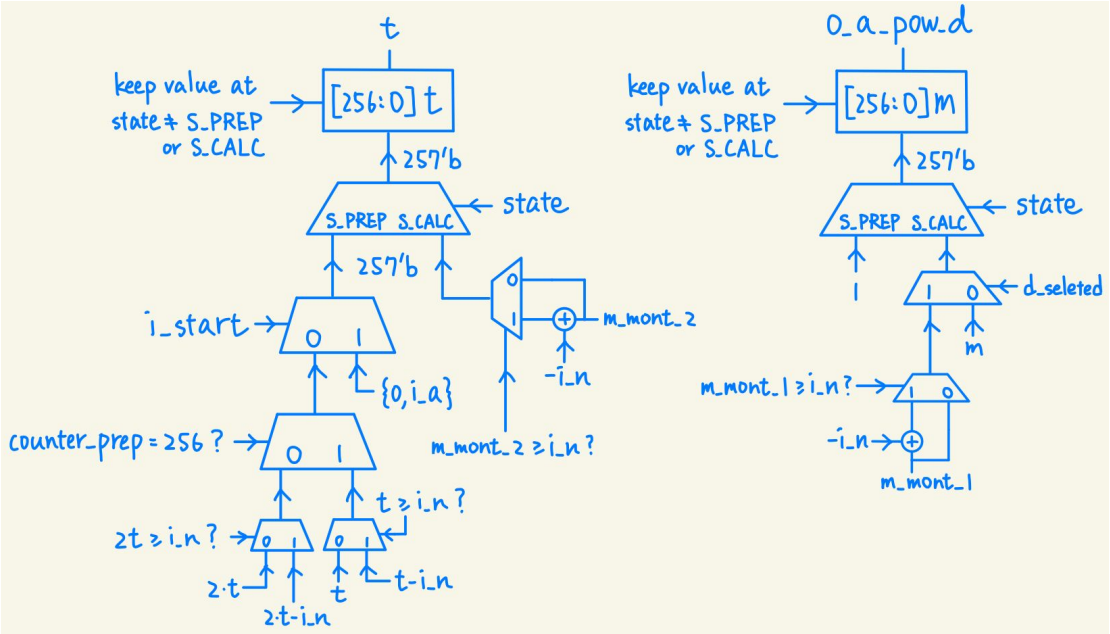
Register m_mont_2 caculate (t*t*2^-256) mod i_n. (both during state = S_MONT)



Block Diagram - Core

Initial t to (i_a*2^256) mod i_n, and set m to 1 when state = S_PREP.

Update t & m to m_mont_2 & m_mont_1 when state = S_CALC.



Fitter Summary

Fitter Summary	
Fitter Status	Successful - Wed Mar 23 14:07:30 2022
Quartus II 64-Bit Version	15.0.0 Build 145 04/22/2015 SJ Full Version
Revision Name	DE2_115
Top-level Entity Name	DE2_115
Family	Cyclone IV E
Device	EP4CE115F29C7
Timing Models	Final
Total logic elements	7,556 / 114,480 (7 %)
Total combinational functions	7,401 / 114,480 (6 %)
Dedicated logic registers	2,199 / 114,480 (2 %)
Total registers	2199
Total pins	518 / 529 (98 %)
Total virtual pins	0
Total memory bits	0 / 3,981,312 (0 %)
Embedded Multiplier 9-bit elements	0 / 532 (0 %)
Total PLLs	1 / 4 (25 %)

Timing Analyzer

TimeQuest Timing Analyzer Summary

Quartus II Version	Version 15.0.0 Build 145 04/22/2015 SJ Full Version
Revision Name	DE2_115
Device Family	Cyclone IV E
Device Name	EP4CE115F29C7
Timing Models	Final
Delay Model	Combined
Rise/Fall Delays	Enabled

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

遇到的問題與解決辦法

1. 剛寫完 Core 時跑 testbench 發現答案有錯，怎麼 debug 都找不出問題，後來跟隔壁組對答案才發現我們的 testbench 給的 gold 是錯的，用他們的 tb 跑也是錯的（直接跟他們要了 tb_verilog 整個資料夾換掉），但把我們的Core 拿去他們工作站跑卻是對的，目前還沒找出原因，猜測是 tb 把 dec 讀進來時編碼有問題導致結果不一樣。
2. 寫完 Core 和 Wrapper 之後跑 testbench 都成功，Quartus 編譯、燒錄也成功，但執行 python 時卻發現 FPGA 沒有傳東西回來（但應該有輸入測資）。後來我們修改Wrapper，在 wait_calculate 這個 state 讓 avm_read, avm_write 皆為 0 就修好了（原本是讓他 read RX_status）。我們認為可能是因為 RS232 protocol 在沒有要讀東西時不能亂把 avm_read 設成 1，但 testbench 並沒有規範這件事。