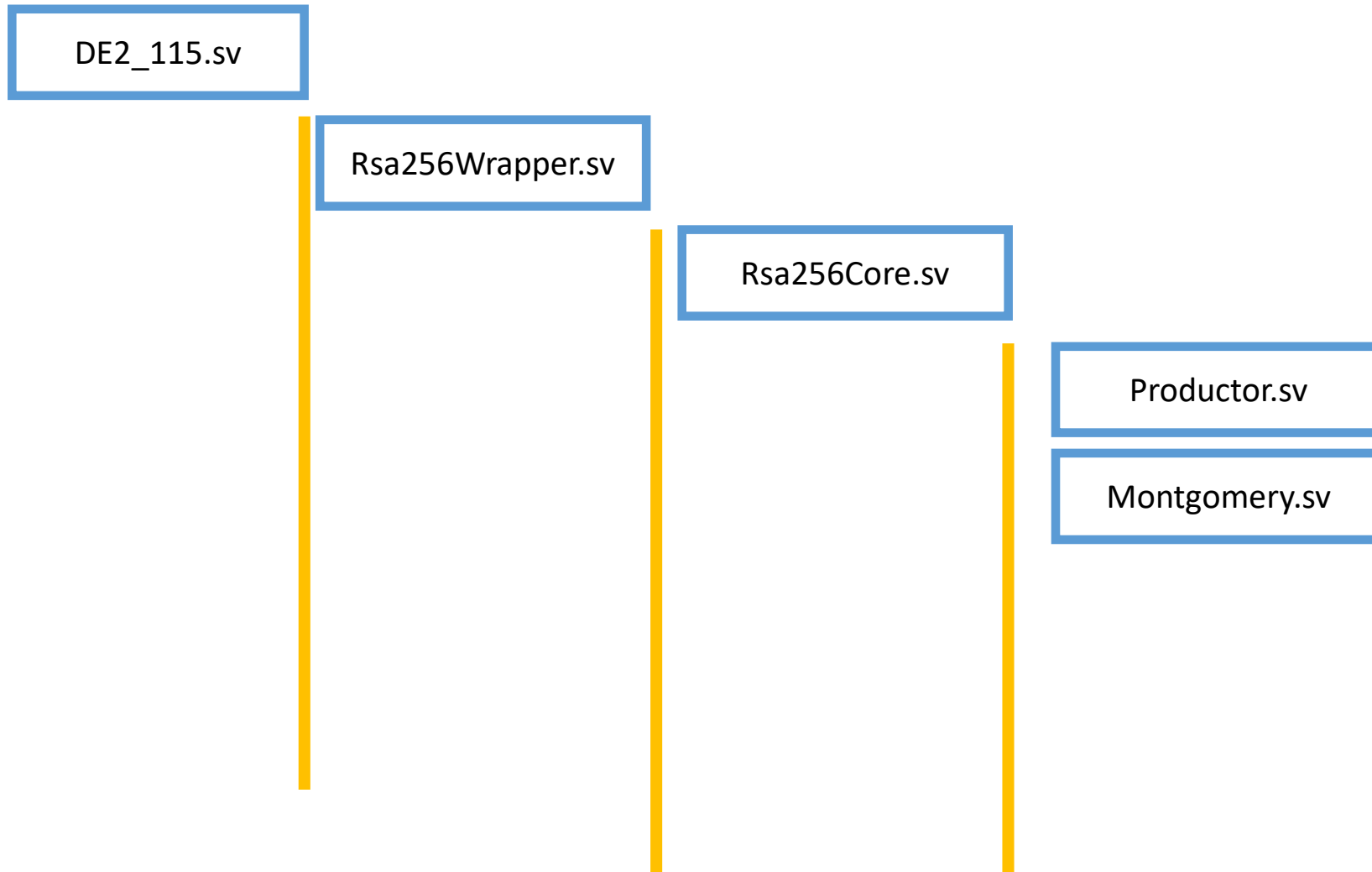
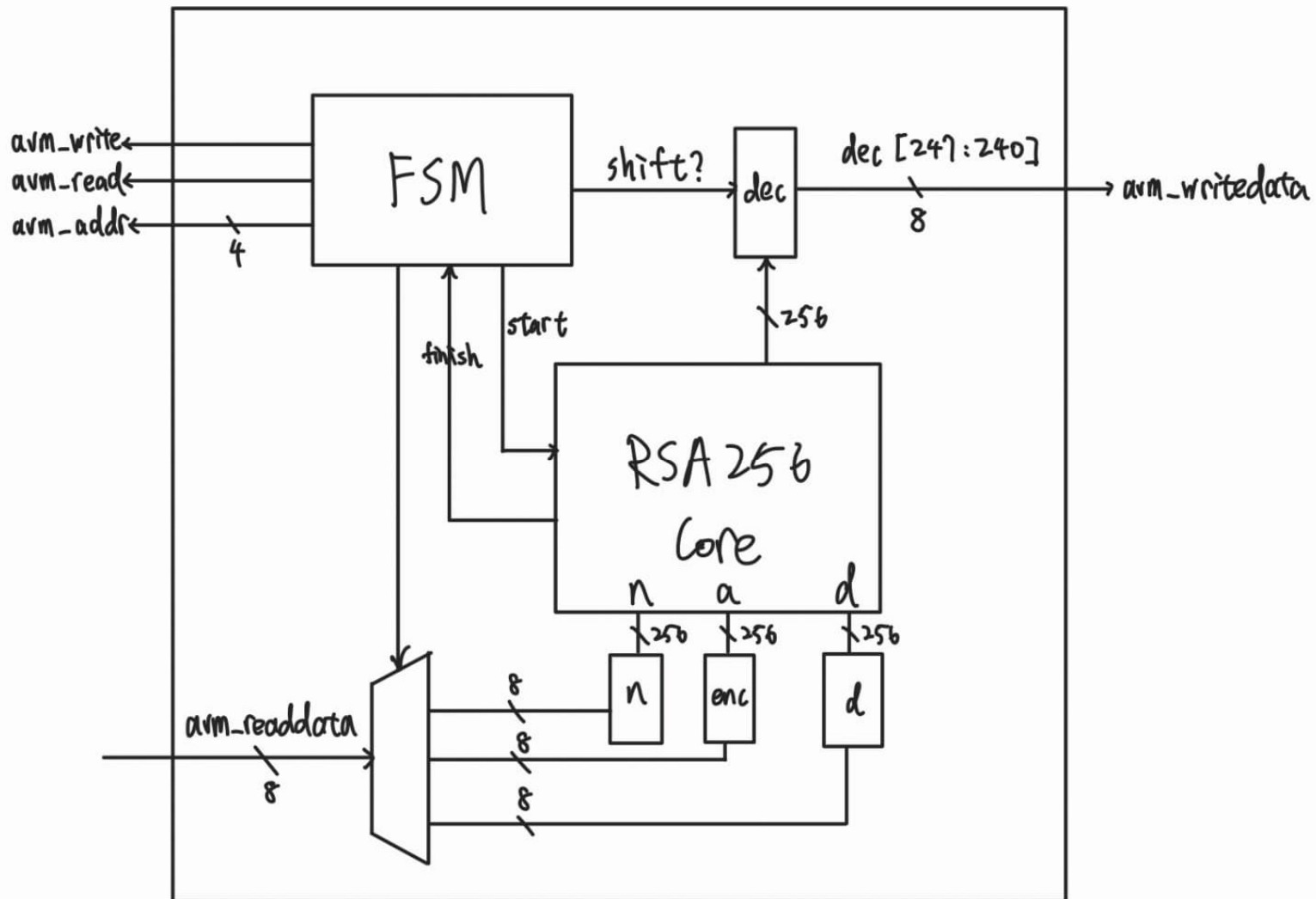


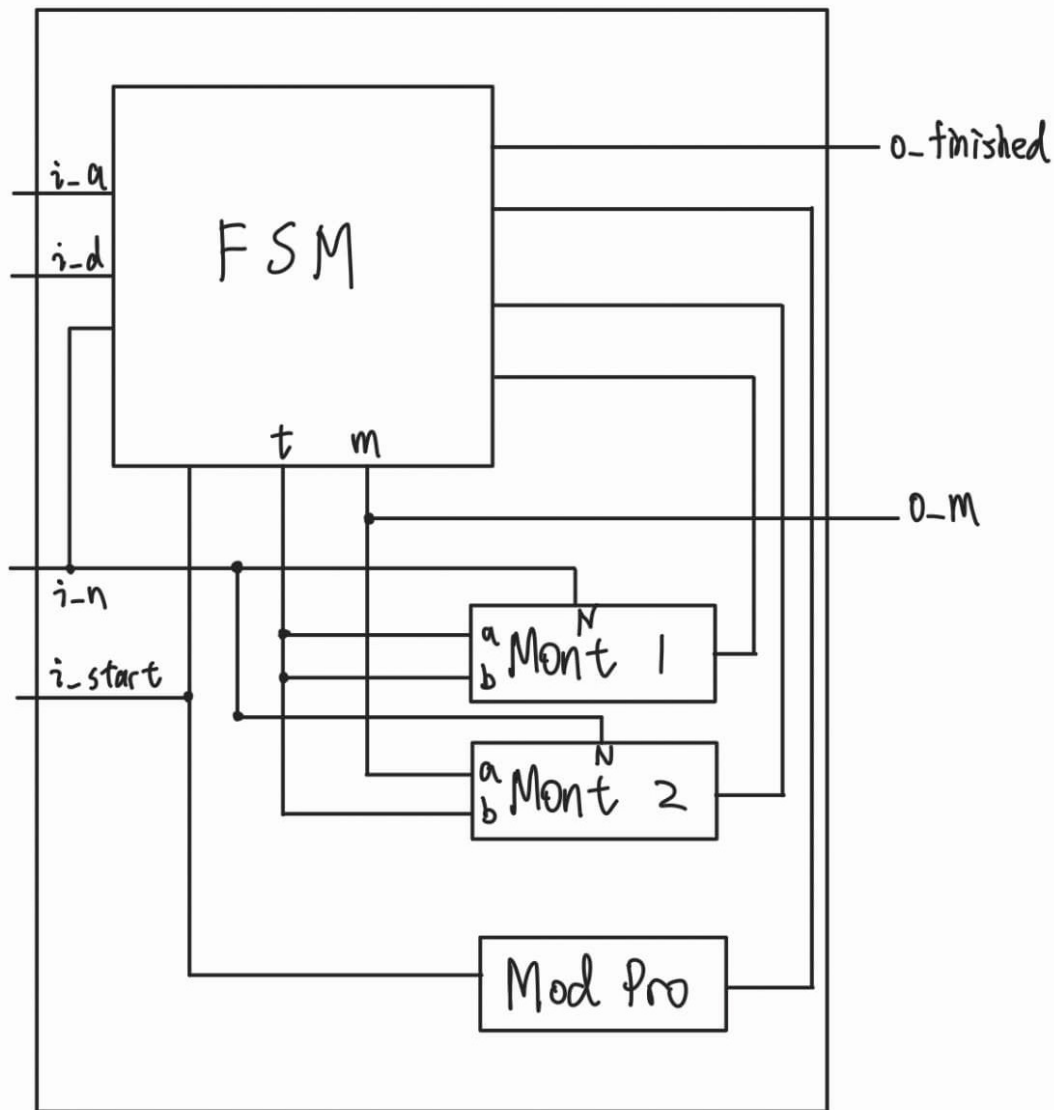
Team01_lab2_report

層級架構

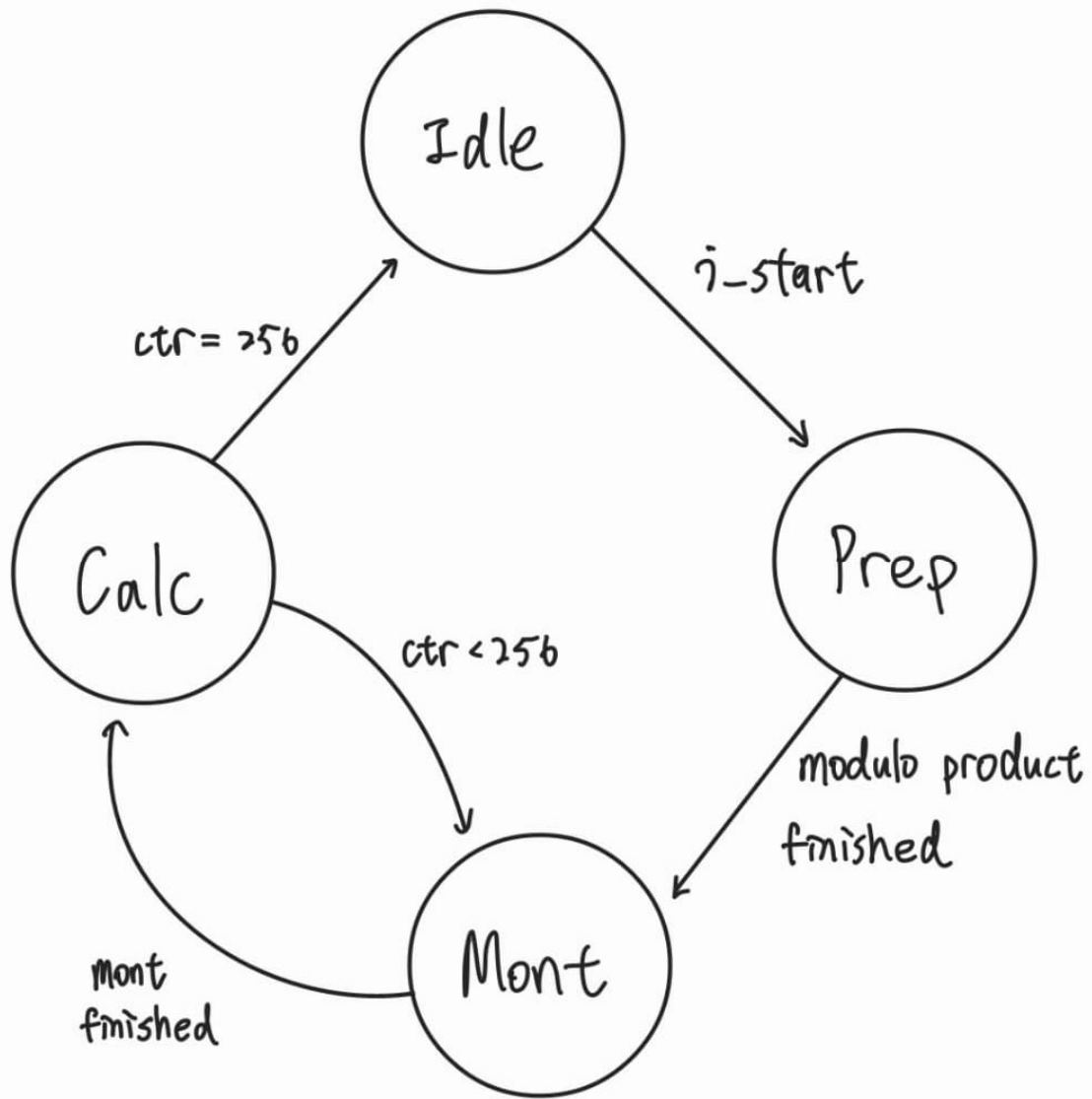




Datapath
wrapper



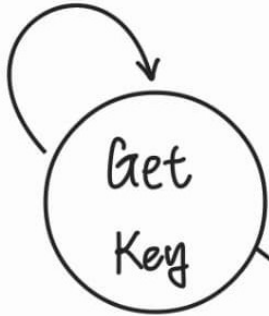
Datapath
core



FSM

core

! byte_ctr_w[6]



byte_ctr_w[6]
(64 bytes accepted)
↳ n & d



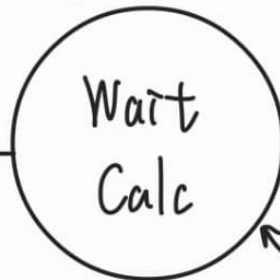
! byte_ctr_w[5]
↓
256 bit

byte_ctr_w[6]

byte_ctr_w == 32



byte_ctr_w < 32



rsa_finished

!rsa_finished

FSM

wrapper

遇到的問題和解法

Prb & Sol



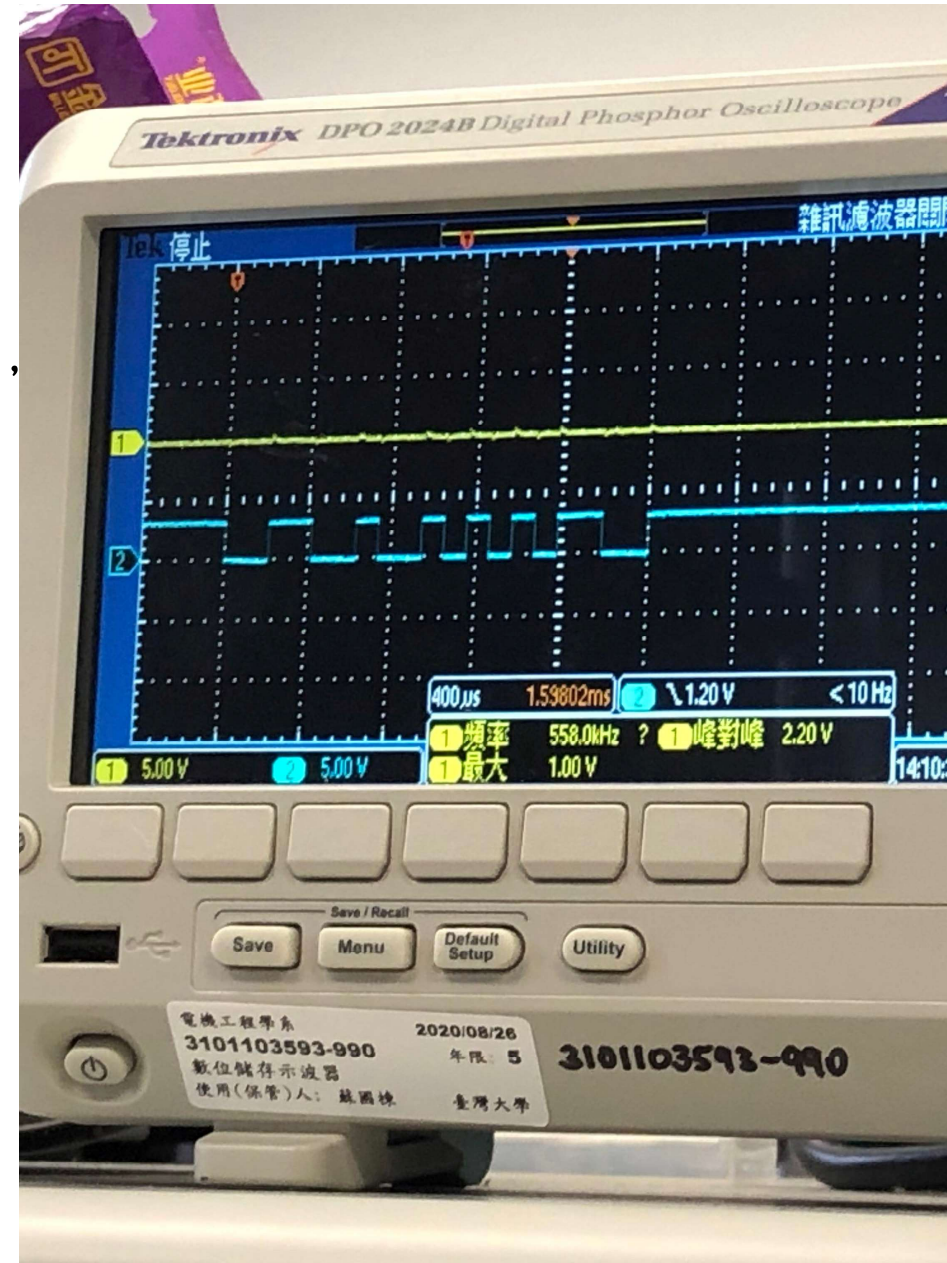
prb1.
ncverilog模擬出來的結果是錯的，但不知道哪裡錯

sol.
寫一個python程式計算每次montgomery應該算出的數字，並跟nWave的模擬結果比較最後發現是montgomery中發生了overflow

```
team01@dclab-workstation ~ % python temp.py
0x622835729cf894964298124e9f9978b60d7d2db3a720389f56d321260ab8b552
0 m = 0xc6b662ecb173c53cc7bb4212057f9c0ba283e000b98c9dcf5feaae7d6c933dfb
0 t = 0x34736a22e7f1e3b8be59f3603c4d8b1a64f21d770743a9318c0cebcdb67b1ef1
1 m = 0xc6b662ecb173c53cc7bb4212057f9c0ba283e000b98c9dcf5feaae7d6c933dfb
1 t = 0x9564d7d0fa86494d5b70a81e69fec4f0927b1eeca822df1b0544b47bf43b27eb
2 m = 0xc6b662ecb173c53cc7bb4212057f9c0ba283e000b98c9dcf5feaae7d6c933dfb
2 t = 0x8409ed9424608c683314434e5cff6b7364399e8828159af0f94ee5251b2b4b93
3 m = 0xf293c04b95a590834f892b0b7789576fb682dd2c2652376ad047c1cce1b60be
3 t = 0x7d1eaa14888e0a5af8d3dcd127353b99b0d4f30feeba0a46e6e78900982d356c
4 m = 0x348fbecfb7a439cf4b25d9506d00f7ebe29ad2f8e1bf46552ee23eb635eb1f94
4 t = 0x150517edad85c572e79dc66b66770ef6f14f34c7711d0aa793b8728ea77a8bak
5 m = 0x348fbecfb7a439cf4b25d9506d00f7ebe29ad2f8e1bf46552ee23eb635eb1f94
5 t = 0xb2e25b9c035a0a012f1244fea03fa777eb32cee32fd3fa0f99fda292390df99e
6 m = 0x8569782d68edb75ad8652669f00f6560ca5ef35b3d20ef1fc5570328009a546a
6 t = 0xa7148b7c1d99b892f3e22d5352bc59c350f2691cef35c30becc0dfe46c30607c
7 m = 0x5f0c699f7787d885193652580121d3ac3a689aaa53f09ad16dec9fd6ac90ba30
7 t = 0xad370d5857b042f3a5ce00052dc731be1b9e9e528987c4db9536542685d433c
```

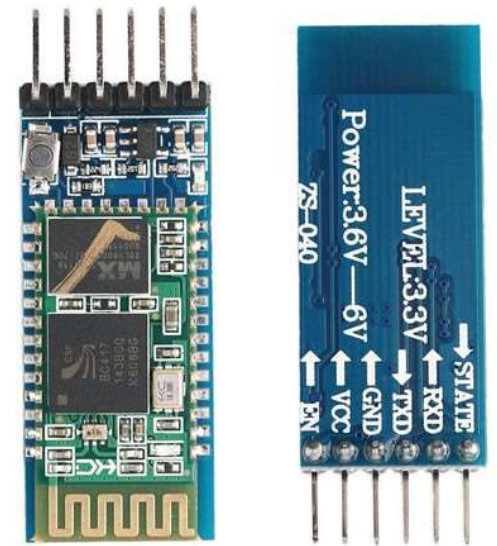

prb2. 我們bonus想嘗試實作藍牙傳輸資料，但一開始我們對藍牙模組收發的資料型式一無所知，不知道該從何做起(我們甚至還搞錯RX/TX腳位)

sol.我們寫一個python程式透過藍牙傳訊號給模組，並利用示波器觀察收到訊號時藍牙模組的波型，藉此得知藍牙如何傳輸資料以及該如何讀取藍牙模組的資料

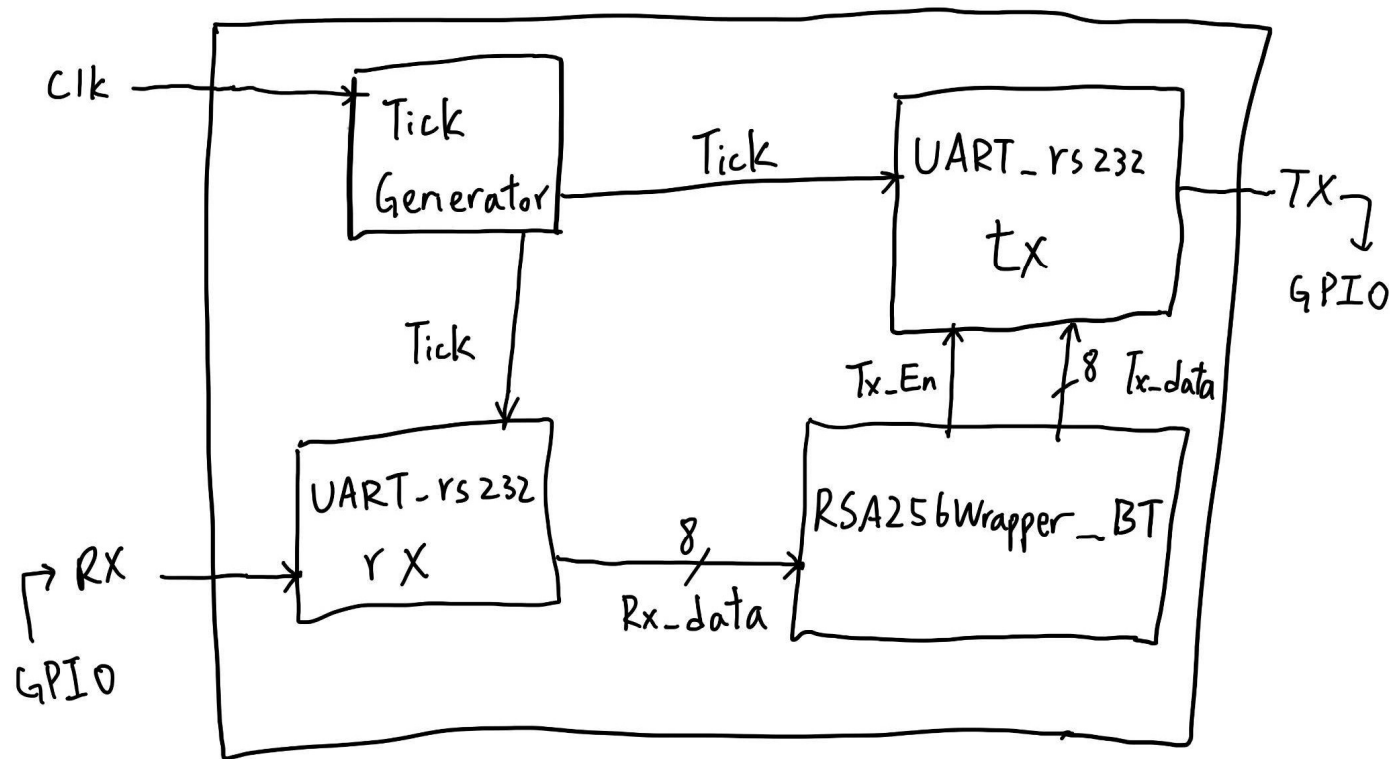


About bonus

- 因為原本的傳輸方法是利用傳輸線，中間有用到qsys，感覺有些部分不是自己寫的，所以我們bonus想挑戰自己實作UART。
- 我們最後選擇使用藍牙模組hc-05來收發訊號，然後使用的baudrate 是9600，傳輸速率大概也是10 kB/s。
- 由於baudrate是9600，所以我們製造一個比50MHz慢325倍的clk稱為Tick，然後每16個Tick讀一次RX的值/寫一次TX的值。



BT datapath



遭遇的問題

- 由於我們只有一個禮拜的時間可以做bonus，再加上我們很難用testbench來測試藍牙收發的訊號，所以有些bug抓不出來。我們曾經試過傳一個8bit訊號給FPGA並顯示在LEDG上，也從FPGA傳一個8bit訊號給電腦，分別都有收到正確的結果，但是和Wrapper接在一起後就一直沒辦法成功☹。
- 雖然如此，但這次bonus還是很有收穫，我想我們離成功應該只差一點點了，因為debug的方式有點難，幾乎都是靠LED燈的亮暗來看資料到底有沒有傳進去，再加上時間不夠，所以沒辦法在demo時展現出成功的樣子，但我們的bonus很有想法。

許願

希望dclab可以放一台示波器
(或是傳說中的邏輯分析儀)，這樣
在這種情況下或許會有助於debug
(大概吧)