HDL Digital Design (Graduate Level)
Spring 2024

HOMEWORK
REPORT

Must do self-checking before submission:

☐ Compress all files described in the problem into one zip file.
☐ All files can be compiled under ModelSim environment.
☐ All port declarations comply with I/O port specifications.
☐ Organize files according to File Hierarchy Requirement
☐ No waveform files or project files in deliverables

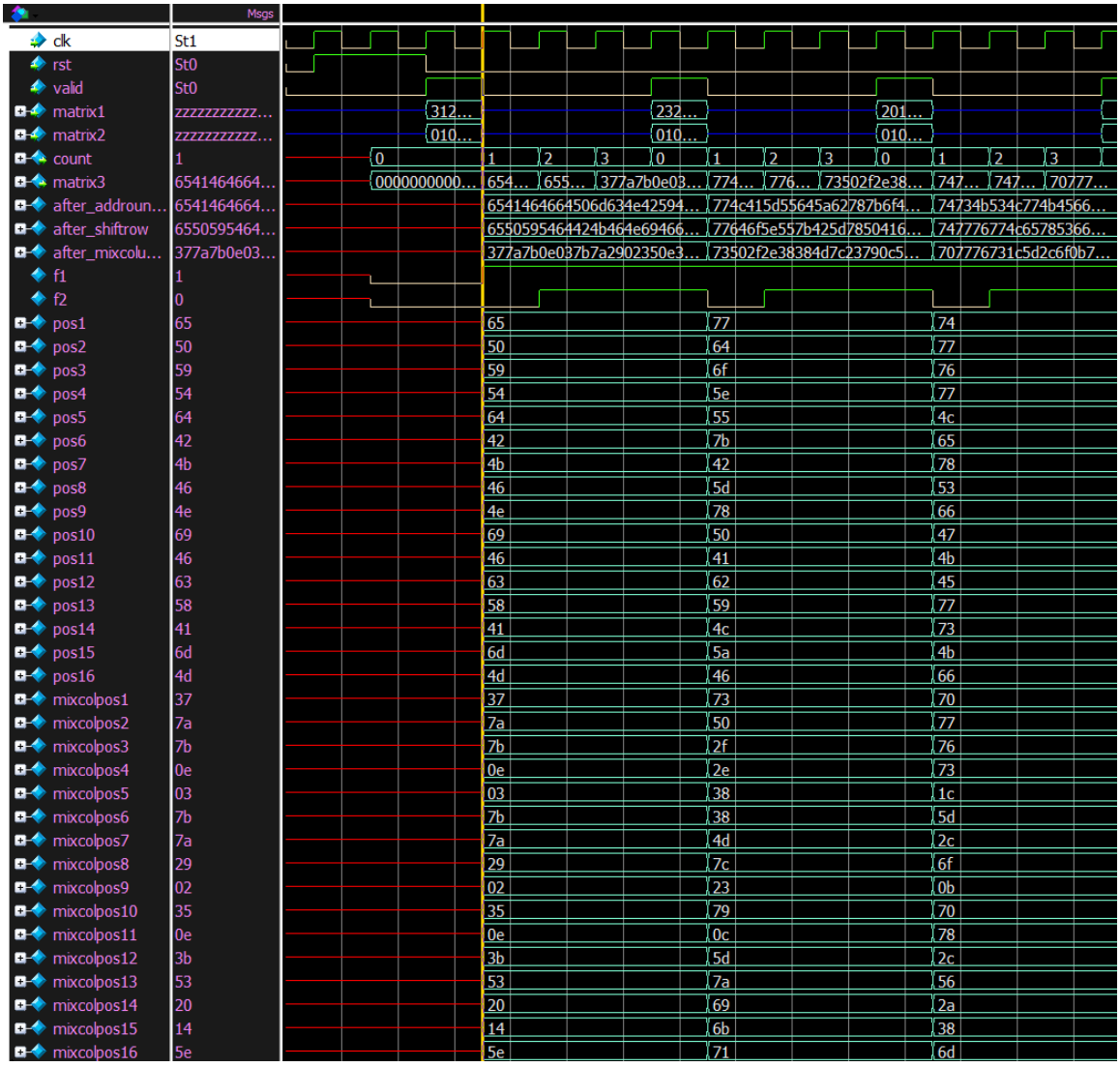
Due Date: 2024/03/14 8:59 a.m.

Student name: 蔡承哲
Student ID: Q36111150

1. Your simulation result on the terminal. (Transcript)

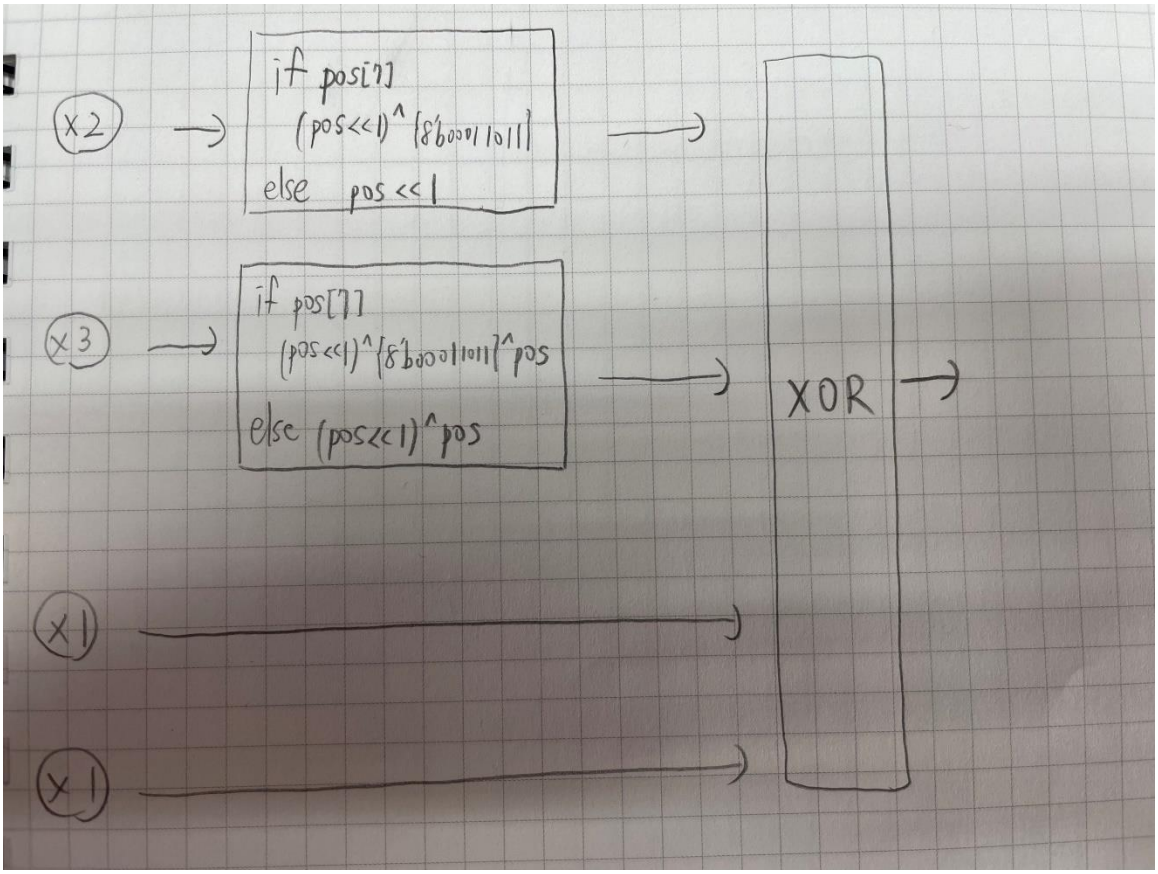
```
#
#         ****************************
#         **                        **       |__||
#         **  Congratulations !!    **      / O.O  |
#         **                        **    /_____   |
#         **  Simulation PASS!!     **   /^ ^ ^ \  |
#         **                        **  |^ ^ ^ ^ |w|
#         ****************************   \m___m__|_|
#
#
#
#
# ---------- Your score: 90/90 ----------
# ** Note: $stop    : D:/00_second_under/StudentID_Lab3/tb.sv(151)
#    Time: 122915 ns  Iteration: 1  Instance: /testfixture
# Break in Module testfixture at D:/00 second under/StudentID Lab3/tb.sv line 151
```

2. Explain the result by waveform.



reg pos1~pos16 用來存取 shiftrow 的結果，reg mixcolpos1~mixcolpos16 用來存取 mixcolumns 的結果。當 valid 訊號拉起後，matrix1 and matrix2 就會進來，一吃到輸入後，就可以同時完成三個 operation，接著只要累加 count，並同時輸出不同的 matrix 即可。

3. Draw the architecture of your MixColumns operation.



4. At last, please write the lesson learned from Lab3, particularly in the Finite Field concepts.
瞭解了 AES Mix-Columns Transformation 的運算，雖然一開始看助教給的 appendix 沒有很懂，尤其是處理 overflow 的部分，不過幸好給補充連結，看完後就順利把作業給完成了。