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

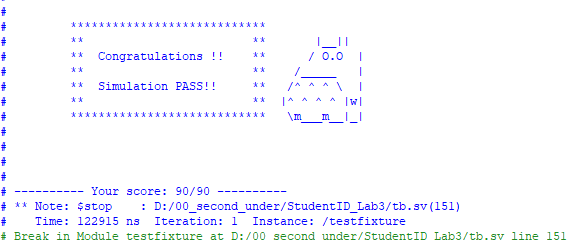
No waveform files or project files in deliverables

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)

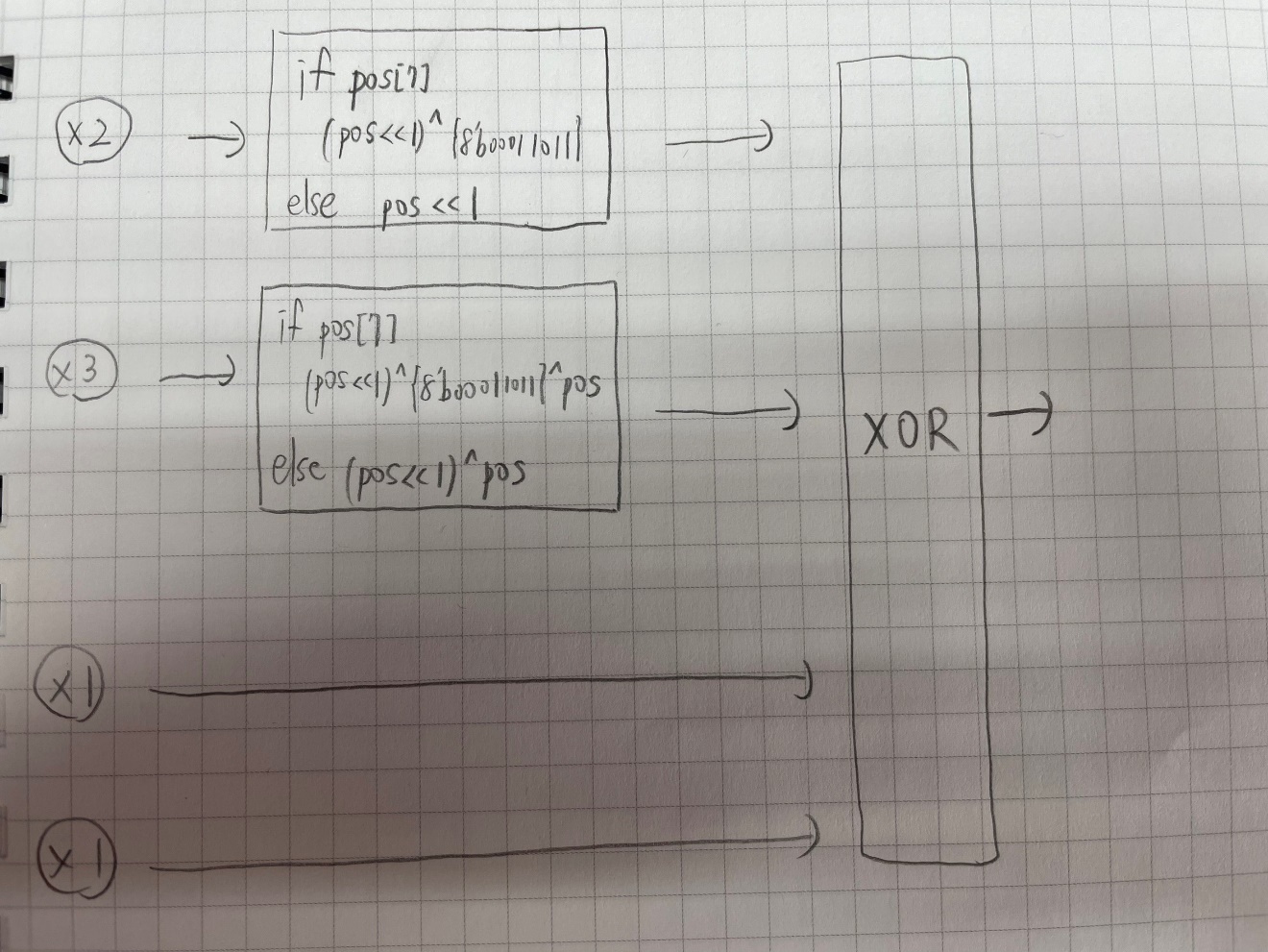


1. Explain the result by waveform.



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。

1. Draw the architecture of your MixColumns operation.



1. 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。