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

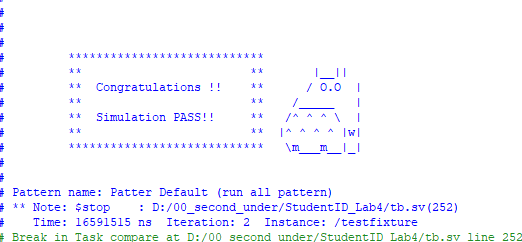
Due Date: 2024/03/21 8:59 a.m.

Student name: 蔡承哲

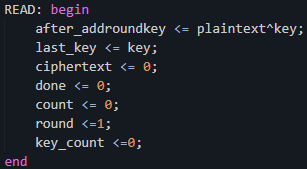
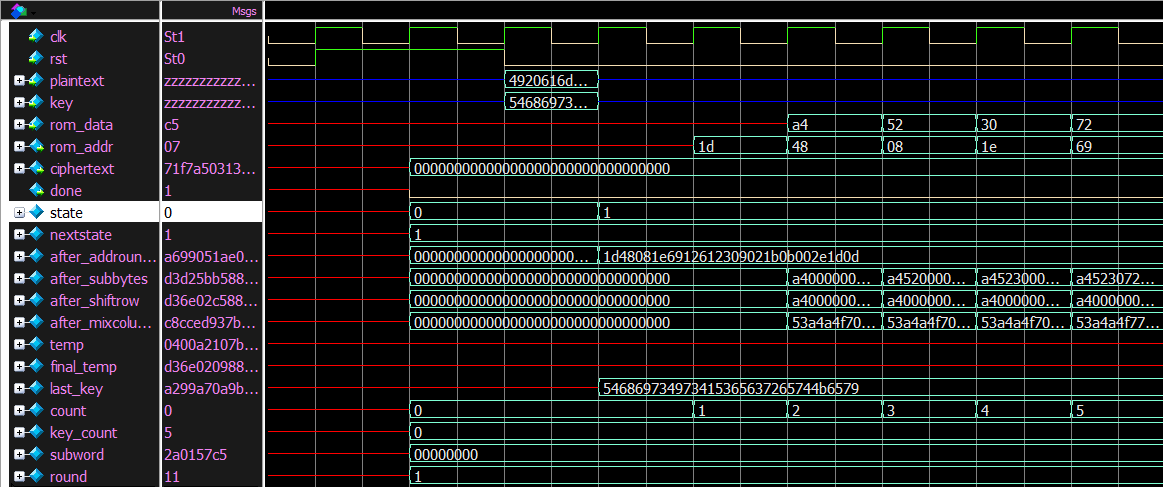
Student ID: Q36111150

1. Paste simulation result on the terminal and result of two cipher image.

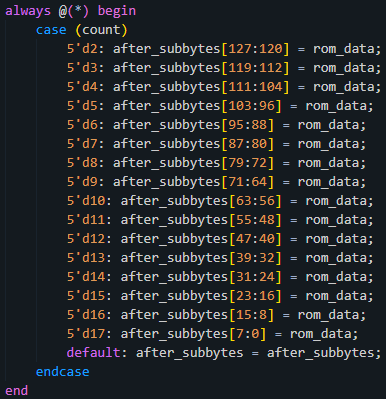
|  |  |  |
| --- | --- | --- |
|  | mount | tux |
| Original |  |  |
| Cipher |  |  |



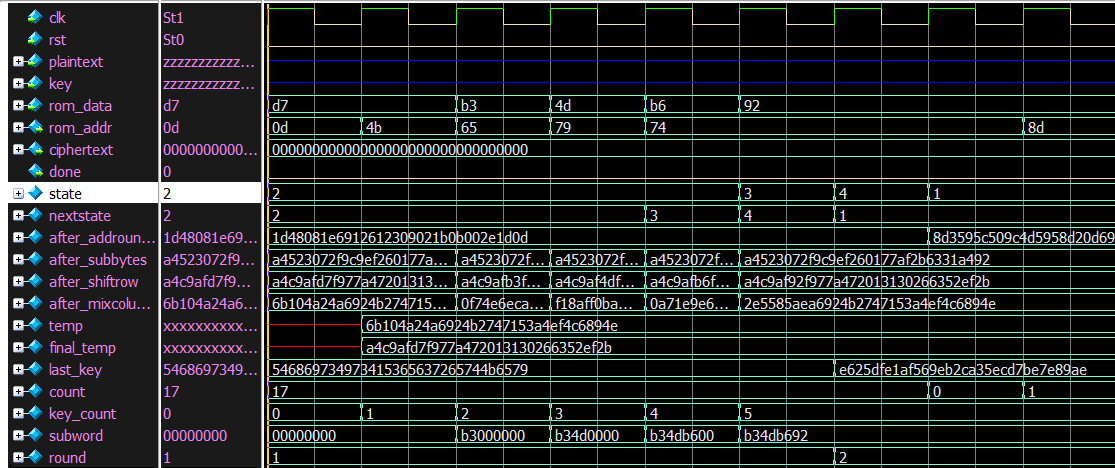
1. Explain the result by waveform.

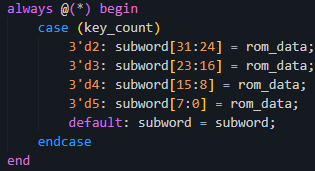
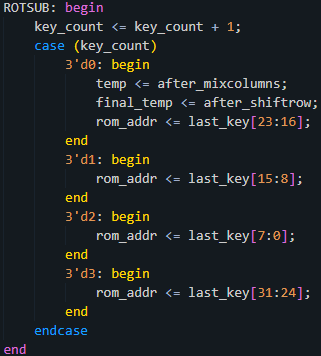


首先在state0(READ)的時候等待plaintext與key的輸入，然後把plaintext^key的結果賦值到after\_addroundkey。同時也把key賦值到last\_key，後續update key會用到。

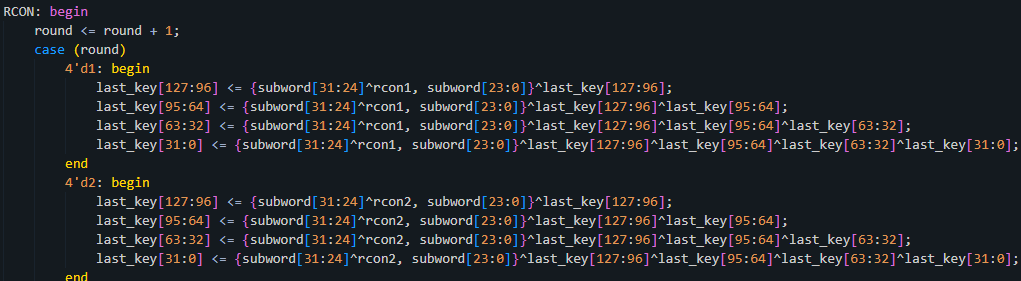


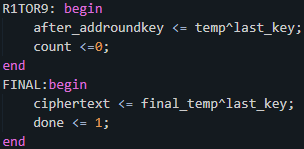
接著就從state0跳到state1(SUBBYTES)，這裡主要做的就是把after\_addroundkey的每一個byte依序當成rom\_addr輸出，且等待rom\_data回傳，依序存入after\_subbytes。





因為做完subbytes後，我們還缺少新的key去做下一輪，所以state1跳到state2(ROTSUB)，因為做完subbytes的同時，就會得到after\_mixcolumns，所以在這個state也會同時暫存after\_mixcolumns(前9輪會用到)與after\_shiftrow(最後一輪用)。經過這個state後就可以得到subword。





接著state2跳到state3(RCON)產生新的key，然後就再跳到state4(R1TOR9)，把temp(after\_mixcolumns)^last\_key的結果再度傳入after\_addroundkey。之後就依序做每一輪，最後一輪，狀態跳到state5，因為不需要做mixcolumns，所以做後結果就是final\_temp(after\_shiftrow)^last\_key。

1. Draw your own Finite State Machine.



1. At last, please write the lesson learned from Lab4 and discuss why Cipher\_tux still has contour on the image.

* 學會使用狀態機
* 因為這次的加密模式是使用ECB mode，所以也是造成影像中有輪廓的原因。在影像的上下文中，因為具有相同顏色或陰影的影像區域將產生相同的加密區塊。