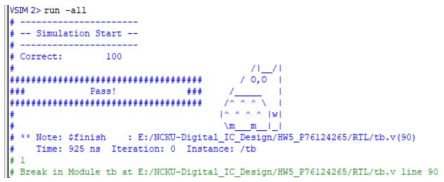
2024 Digital IC Design Homework 5

NAME	李尚宸
Student ID	P76124265
Score = area*timing (ps)	Score = 45356 * 925000 = 41,954,300,000 (Area = 45356 + 0 + 0 = 45356 Timing = 925000 ps)
Cycle time (ns)	8 ns

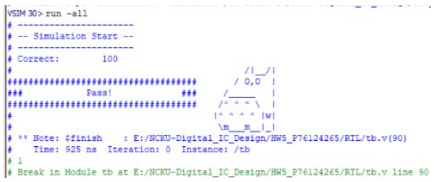
Simulation Result

Functional simulation	Completed	Gate-level simulation	Completed

(your functional sim result)



(your gate-level sim result)



Description of your design

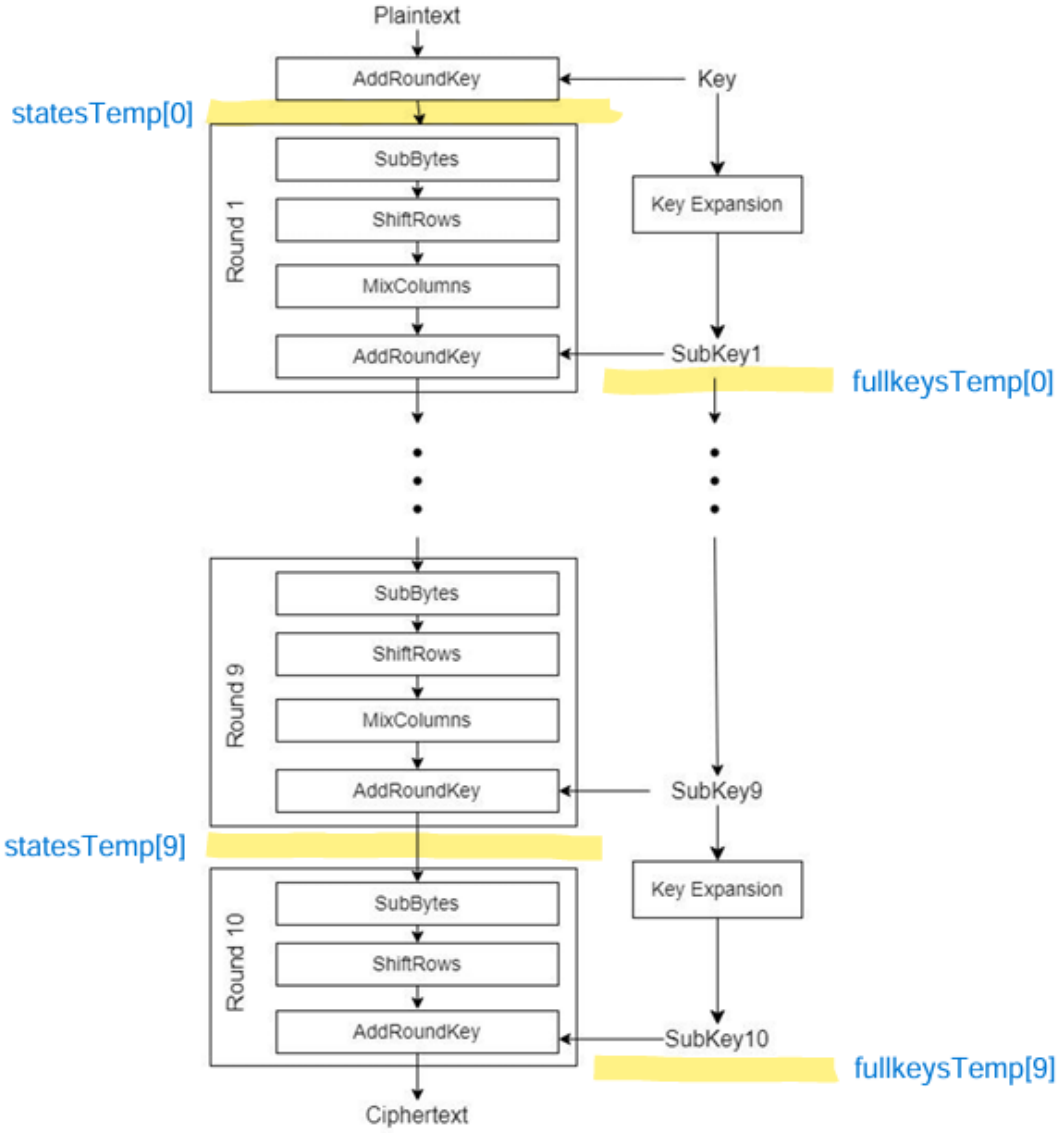


Fig. 1. AES Encryption path

AES.v: 循序電路，在每個 posedge，將 statesTemp 和 fullkeysTemp 的值分別 assign 給 states 和 fullkeys

Others.v: 組合電路，實現 AES 需要的 modules，當 states 和 fullkeys 的值更新後，modules 會計算下一輪的 key 和 state，最後將計算結果分別 assign 給 statesTemp 和 fullkeysTemp

Flow Summary

<<Filter>>

Flow Status	Successful - Sun Jun 16 00:43:51 2024
Quartus Prime Version	20.1.1 Build 720 11/11/2020 SJ Lite Edition
Revision Name	AES
Top-level Entity Name	AES
Family	Cyclone IV E
Device	EP4CE75F29C8
Timing Models	Final
Total logic elements	45,356 / 75,408 (60 %)
Total registers	2693
Total pins	387 / 427 (91 %)
Total virtual pins	0
Total memory bits	0 / 2,810,880 (0 %)
Embedded Multiplier 9-bit elements	0 / 400 (0 %)
Total PLLs	0 / 4 (0 %)

The scoring standard: (The smaller, the better)

Scoring =

*Area cost * Timing cost*

Area cost =

*Total logic elements + total memory bits + 9*embedded multiplier 9-bit elements*

Timing cost =

Simulation time

Flow Summary

<<Filter>>

Flow Status	Successful - Mon May 20 14:38:37 2024
Quartus Prime Version	20.1.1 Build 720 11/11/2020 SJ Lite Edition
Revision Name	AES
Top-level Entity Name	AES
Family	Cyclone IV E
Device	EP4CE75F29C8
Timing Models	Final
Total logic elements	45,971
Total registers	2954
Total pins	387
Total virtual pins	0
Total memory bits	0
Embedded Multiplier 9-bit elements	0
Total PLLs	0

```
# Correct:        100
#                                             /|__/|
####################################        / O,O  |
###             Pass!              ###     /_____   |
####################################      /^ ^ ^ \  |
#                                        |^ ^ ^ ^ |w|
#                                         \m___m__|_|
# ** Note: $finish    : C:/Users/diclab/Desktop/DIC2024/HW5_/tb.v(99)
#    Time: 991250 ps  Iteration: 0  Instance: /tb
```