

2024 Digital IC Design Homework 5

NAME	陳俐蓉						
Student ID	N26120113						
Score = area*timing (ps)	65,821,003,500						
Cycle time (ns)	8.0 ns (SDC 內設定), 11.0 ns (合成跑模擬的 cycle time)						
		Clock Name	Type	Period	Frequency	Rise	Fall
	1	clk	Base	8.000	125.0 MHz	0.000	4.000

Simulation Result

Functional simulation	Completed	Gate-level simulation	Completed
-----------------------	-----------	-----------------------	-----------

(your functional sim result)

```
# -----#  
# -- Simulation Start --#  
# -----#  
# Correct:      100  
#  
##### /|_/  
##### / O,O |  
### Pass! ### |  
##### / ^ _ \  
##### | ^ ^ ^ |w  
# | m m |_  
# ** Note: $finish : D:/DIC/HW5/RTL2/tb.v(90)  
# Time: 1059250 ps Iteration: 0 Instance: /tb
```

(your gate-level sim result)

```

#-----
# -- Simulation Start --
#-----
# Correct:      100
#
##### /|_|/|
##### / O,0 |
###      Pass!      ### /_____|
##### / ^ ^ ^ \ |
##### | ^ ^ ^ |w|
#      |m__m_| |
#
# ** Note: $finish      : D:/DIC/HW5/SYN2/tb.v(90)
#      Time: 1370500 ps  Iteration: 0  Instance: /tb

```

Synthesis Result

Flow Status	Successful - Tue Jun 18 15:05:22 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	48,027 / 75,408 (64 %)
Total registers	5489
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 %)

Description of your design

AES128 會將輸入的 128 位元資料和 key 一起進行 10 次重複加密，前 9 次加密依序包含 SubBytes、ShiftRows、MixColumns、AddRoundKey，第 10 次加密依序包含 SubBytes、ShiftRows、AddRoundKey，每次加密都會把前一次的 key 做 key expansion 來製造新的 key。因為每個 cycle 輸入端都會送入新的資料，為了讓每 cycle 都能接收並處理新資料，所以這裡在每次加密之間都插入一個 pipeline，將加密資料和 valid 訊號送入 pipeline 一起傳遞，因此第一筆資料在 10 個 cycle 後才會加密完成並輸出。

ShiftRows

雖然步驟裡是先做 SubBytes 再做 ShiftRows，但其實交換這兩個步驟並不影響結果，因此我的設計裡選擇先做 ShiftRows，在資料送入 pipeline 時就先在 register 裡排好 ShiftRows 後的資料順序：



Register index(idx)和 128bit 輸入資料(P)位元之間的關係可以用 $S_{r,c}$ 的 r 和 c 表示：

register[idx] = P[127-32c-8r : 120-32c-8r]

r = idx[1:0]

c = idx[1:0] + idx[3:2]

MixColumns

此步驟是將每個 column 的 $S_{r,c}$ 去乘以一個特定的矩陣，並用 GF(2^8)去表示。

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$

以下為 GF(2^8)乘法硬體實現方式：

$$S_{r,c} \cdot (01) = S_{r,c}$$

$$S_{r,c} \cdot (02) = S_{r,c} \ll 1$$

$$S_{r,c} \cdot (03) = S_{r,c} \cdot ((01) \oplus (02)) = S_{r,c} \oplus (S_{r,c} \ll 1)$$

The scoring standard: (The smaller, the better)

$$\text{Scoring} = \text{Area cost} * \text{Timing cost} = 65,821,003,500$$

$$\text{Area cost} = \text{Total logic elements} + \text{total memory bits} + 9 * \text{embedded multiplier 9-bit elements} = 48027$$

$$\text{Timing cost} = \text{Simulation time} = 1370500 \text{ ps}$$