## 2024 Digital IC Design Homework 5

NAME	陳俐蓉				
Student ID	N26120113				
Score =	65,821,003,500				
area*timing (ps)					
	8.0 ns (SDC 內設定), 11.0 ns (合成跑模擬的 cycle time)				
Cycle time (ns)	Clock Name Type Period Frequency Rise Fall				
	1 clk Base 8.000	125.0 MHz 0.000 4.000			
	Simu	ation Result			
Functional	C1-4-4	Gate-level			
simulation	Completed	simulation			
(your functi	onal sim result)	(your gate-level sim result)			
<b>#</b>	_	<b>#</b>			
# Simulation Start -	- -	# Simulation Start #			
# Correct: 100	/1_	# Correct: 100 // # //_//			
**************************************					
***************************************		·			
# Wanan deiniah	\mm	**			
	D:/DIC/HW5/RTL2/tb.v(90) Iteration: 0 Instance: /				
	Synt	nesis Result			
Flow Status		Successful - Tue Jun 18 15:05:22 2024			
Quartus Prim	ne Version	20.1.1 Build 720 11/11/2020 SJ Lite Edition			
Revision Nan	ne	AES			
Top-level En	tity Name	AES			
Family		Cyclone IV E			
Device		EP4CE75F29C8			
Timing Mode	els	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%)			

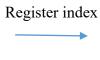
## **Description of your design**

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:

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$



0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

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  $\mathrm{GF}(2^8)$ 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(28)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)
```

Scoring = Area cost \* Timing cost = 65,821,003,500

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

elements = 48027

 $Timing\ cost = Simulation\ time = 1370500\ ps$