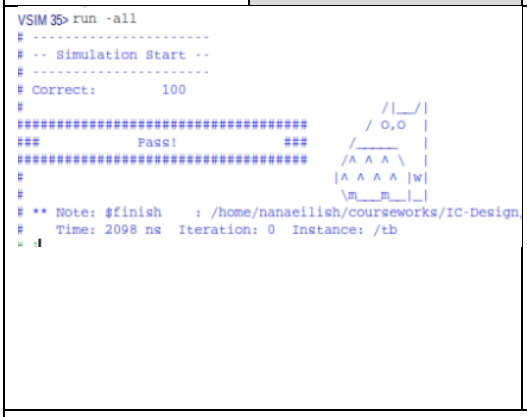
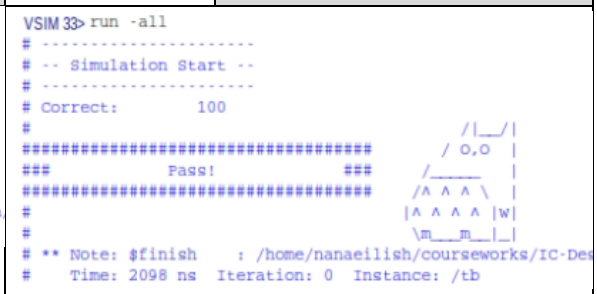
2024 Digital IC Design Homework 5

NAME	楊晴雯
Student ID	P76114511
Score = area*timing (ps)	
Cycle time (ns)	18

Simulation Result

Functional simulation	Completed	Gate-level simulation	Completed





Description of your design

A data goes into 10 rounds, in which the first 9 rounds are identical. Therefore, I design round modules called (1) `AESRound` (2) `AESLastRound`, each accepts `rc, Pi, Ki, Po, Ko` as inputs.

`rc`: round count (i)

`Pi`: the input text (halfway-encoded text or plaintext) for this round

`Ki`: the input (sub) key for this round

`Po`: the output text; the input text for next round

`Ko`: the output (sub) key for the next round

All of the steps within a round are implemented as combinational logics or functions within logics. The round modules encompass the steps as its submodules. The round modules are implemented as combinational logics as well.

AES.v is the main (top) module of the design; it is the only module that accepts a clock signal (sequential), and the pipelining required for this assignment is done here using a 127*11 register for input and encoded texts (`reg [127:0] P_mem[0:NUM_ROUNDS]`) and another 127*11 register for initial key and subkeys (`reg [127:0] key_mem[0:NUM_ROUNDS]`). We pipeline after every round, meaning that a round is done within a cycle. That is, the datapath of a normal round containing subbytes, shift rows, mix columns and key expansion is

the critical path of this design.

```
//
// Designer: P76114511 Ching-Wen Yang
//
// `include "helpers.v"
// `include "round.v"
// `include "aes_sbox.v"
module AES(
    input wire clk,
    input wire rst,
    input wire [127:0] P,
    input wire [127:0] K,
    output reg [127:0] C,
    output reg valid
    );
    localparam NUM_ROUNDS = 10;

    // write your design here //
    reg [127:0] key_mem [0:NUM_ROUNDS];
    reg [127:0] P_mem [0:NUM_ROUNDS];
    wire [127:0] key_result [0:NUM_ROUNDS];
    wire [127:0] P_result [0:NUM_ROUNDS];

    AESRound r1(.rc(4'b0000), .Pi(P_mem[0]), .Ki(key_mem[0]), .Po(P_result[0]), .Ko(key_result[0]));
    AESRound r2(.rc(4'b0001), .Pi(P_mem[1]), .Ki(key_mem[1]), .Po(P_result[1]), .Ko(key_result[1]));
    AESRound r3(.rc(4'b0010), .Pi(P_mem[2]), .Ki(key_mem[2]), .Po(P_result[2]), .Ko(key_result[2]));
    AESRound r4(.rc(4'b0011), .Pi(P_mem[3]), .Ki(key_mem[3]), .Po(P_result[3]), .Ko(key_result[3]));
    AESRound r5(.rc(4'b0100), .Pi(P_mem[4]), .Ki(key_mem[4]), .Po(P_result[4]), .Ko(key_result[4]));
    AESRound r6(.rc(4'b0101), .Pi(P_mem[5]), .Ki(key_mem[5]), .Po(P_result[5]), .Ko(key_result[5]));
    AESRound r7(.rc(4'b0110), .Pi(P_mem[6]), .Ki(key_mem[6]), .Po(P_result[6]), .Ko(key_result[6]));
    AESRound r8(.rc(4'b0111), .Pi(P_mem[7]), .Ki(key_mem[7]), .Po(P_result[7]), .Ko(key_result[7]));
    AESRound r9(.rc(4'b1000), .Pi(P_mem[8]), .Ki(key_mem[8]), .Po(P_result[8]), .Ko(key_result[8]));
    AESLastRound r10(.rc(4'b1001), .Pi(P_mem[9]), .Ki(key_mem[9]), .Po(P_result[9]), .Ko(key_result[9]));
    integer i;
    reg [6:0] r_count;

    always@(posedge clk or posedge rst) begin
        if (rst) begin
            // clean key_mem, P_mem
            for (i = 0; i <= NUM_ROUNDS; i = i + 1) begin
                key_mem[i] <= 128'h0;
                P_mem[i] <= 128'h0;
            end
            r_count <= 0;
            valid <= 0;
        end
        else begin
            r_count <= r_count + 1; // the global round count
            key_mem[0] <= K;
            P_mem[0] <= P ^ K;
            // round 1 ~ 9
            for (i = 1; i <= NUM_ROUNDS; i = i + 1) begin
                key_mem[i] <= key_result[i - 1];
                // add round key
                P_mem[i] <= P_result[i - 1] ^ key_result[i - 1];
            end
            C <= P_mem[NUM_ROUNDS];
            valid <= 1 & (r_count > NUM_ROUNDS+1);
        end
    end
endmodule
```

References: SudarshanHV/AESVerilog (github.com)

Flow Status	Successful - Thu Jun 20 15:16:03 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	45,618 / 75,408 (60 %)
Total registers	2824
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

TA's

```
# 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
```