



ECSE 325

LAB 3 REPORT

Martin Kruchinski(260915767)
Menad Kessaci(260807381)

GROUP 35



G35_mod_exp:

Introduction:

The circuit below implements a basic modular exponentiation that is going to be used in our public-key based message time stamping system. Given the flowing as inputs:

- A 14-bit signal for the exponent d
- A 10-bit signal representing a message c

The circuit calculates the following:

$$s = c^d \bmod n$$

(where n is 33401)

This means that the following circuit uses the circuit from Lab 2 as a component to calculate the modulus operation.

S is the 16-bit output of the circuit, which represents the result of the whole exponentiation and modulus operation.

VHDL description of the circuit:

```
1  --
2  -- entity name: g35_mod_exp
3  -- implements s = c^d modulo 33401
4  --
5  -- Version 1.0
6  -- Authors: (Martin Kruchinski and Menad Kessaci)
7  -- Date: March 18, 2022
8  library ieee; -- allows use of the std_logic_vector type
9  use ieee.std_logic_1164.all;
10 use ieee.numeric_std.all;
11 entity g35_mod_exp is
12 port ( d : in std_logic_vector(13 downto 0);
13       c : in std_logic_vector(9 downto 0);
14       start : in std_logic;
15       clk : in std_logic;
16       reset : in std_logic;
17       s : out std_logic_vector(15 downto 0);
18       ready : out std_logic);
19 end g35_mod_exp;
20
21
22 architecture design of g35_mod_exp is
23 --component declaration
24 component g35_modulo33401
25 port (
26     A : in std_logic_vector(31 downto 0);
27     Amod33401 : out std_logic_vector(15 downto 0);
28     Afloor33401 : out std_logic_vector(16 downto 0)
29 );
30 end component;
31
32 --intermediate signals declaration
33 signal k : integer := 0;
34 signal interS: std_logic_vector(15 downto 0);
35 -- signal interS2: std_logic_vector(15 downto 0);
36 signal multiplication: std_logic_vector(31 downto 0);
37 signal floor: std_logic_vector(16 downto 0);
38 begin
```

```

38 begin
39 modulo : g35_modulo33401 port map(A => multiplication, Amod33401 => interS, Afloor33401 => floor);
40
41 counter: process(clk)
42 begin
43     if reset = '1' then
44         k <= 0;
45     elsif rising_edge(clk) then
46         if start = '1' then
47             k <= k + 1;
48         end if;
49     end if;
50 end process;
51
52 algorithm: process(d, c, reset, start, clk,k)
53
54 variable interS2 : std_logic_vector(15 downto 0);
55 begin
56     if reset = '1' then
57         ready <= '0';
58         interS2 := std_logic_vector(to_unsigned(1, 16));
59     elsif rising_edge(clk) then
60         if start = '1' then
61             if k < to_integer(unsigned(d)) then
62
63                 if k = 0 then
64                     interS2 := std_logic_vector(to_unsigned(1, 16));
65                 else
66                     interS2 := interS;
67                 end if;
68                 multiplication <= std_logic_vector(resize(unsigned(interS2) * unsigned(c),32));
69             else
70                 ready <= '1';
71             end if;
72         end if;
73     end if;
74 end process;
75
76 s <= interS;
77 end design;

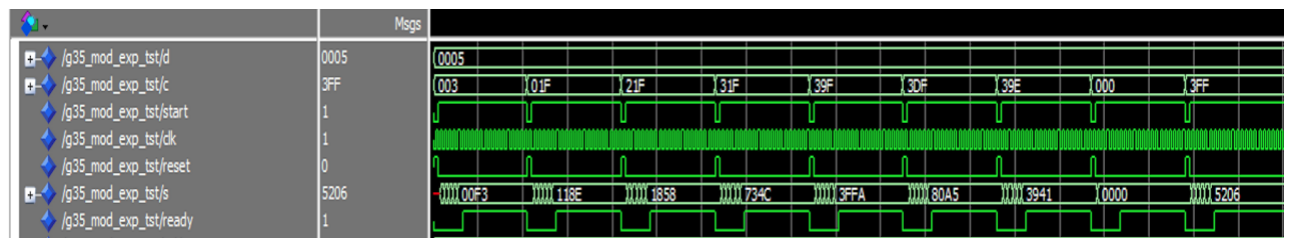
```

Testbench:

```
32  ENTITY g35_mod_exp_tst IS
33  END g35_mod_exp_tst;
34  ARCHITECTURE g35_mod_exp_arch OF g35_mod_exp_tst IS
35  -- constants
36  -- signals
37
38  COMPONENT g35_mod_exp
39  port ( d : in std_logic_vector(13 downto 0);
40        c : in std_logic_vector(9  downto 0);
41        start : in std_logic;
42        clk : in std_logic;
43        reset : in std_logic;
44        s : out std_logic_vector(15 downto 0);
45        ready : out std_logic);
46  END COMPONENT;
47  signal d : std_logic_vector(13 downto 0);
48  signal c : std_logic_vector(9  downto 0);
49  signal start : std_logic;
50  signal clk : std_logic;
51  signal reset : std_logic;
52  signal s : std_logic_vector(15 downto 0);
53  signal ready : std_logic;
54  begin
55
56      clk_process: process
57      begin
58          clk <= '0';
59          wait for 5 ns;
60          clk <= '1';
61          wait for 5 ns;
62      end process;
63
64
65  i1 : g35_mod_exp
66  PORT MAP (
67  -- list connections between master ports and signals
68  d=> d,
69  c => c,
70  start=> start,
71  clk => clk,
72  reset => reset,
73  s => s,
74  ready => ready
75  );
76
```

78	always : PROCESS	125	--Case 6:
79	BEGIN	126	wait for 200 ns;
80	--Case 1:	127	reset <= '1';
81	reset <= '1';	128	start <= '0';
82	start <= '0';	129	c <= "1111011111";
83	d <= "00000000000101";	130	wait for 10 ns;
84	c <= "00000000011";	131	reset <= '0';
85	wait for 10 ns;	132	start <= '1';
86	reset <= '0';	133	
87	start <= '1';	134	--Case 7:
88		135	wait for 200 ns;
89	--Case 2:	136	reset <= '1';
90	wait for 200 ns;	137	start <= '0';
91	reset <= '1';	138	c <= "1110011110";
92	start <= '0';	139	wait for 10 ns;
93	c <= "0000011111";	140	reset <= '0';
94	wait for 10 ns;	141	start <= '1';
95	reset <= '0';	142	
96	start <= '1';	143	--Case 8:
97		144	wait for 200 ns;
98	--Case 3:	145	reset <= '1';
99	wait for 200 ns;	146	start <= '0';
100	reset <= '1';	147	c <= "0000000000";
101	start <= '0';	148	wait for 10 ns;
102	c <= "1000011111";	149	reset <= '0';
103	wait for 10 ns;	150	start <= '1';
104	reset <= '0';	151	
105	start <= '1';	152	--Case 9:
106		153	wait for 200 ns;
107	--Case 4:	154	reset <= '1';
108	wait for 200 ns;	155	start <= '0';
109	reset <= '1';	156	c <= "1111111111";
110	start <= '0';	157	wait for 10 ns;
111	c <= "1100011111";	158	reset <= '0';
112	wait for 10 ns;	159	start <= '1';
113	reset <= '0';	160	
114	start <= '1';	161	WAIT;
115		162	END PROCESS always;
116	--Case 5:	163	END g35_mod_exp_arch;
117	wait for 200 ns;		
118	reset <= '1';		
119	start <= '0';		
120	c <= "1110011111";		
121	wait for 10 ns;		
122	reset <= '0';		
123	start <= '1';		
124			

Simulation results:



Expected results:

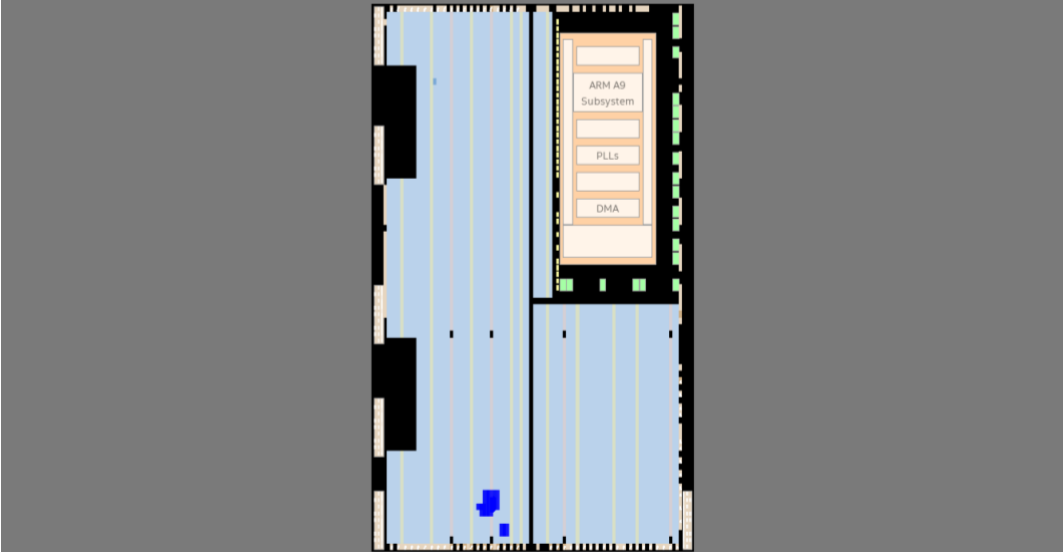
```
Test number: 1   C: 3   D: 5   C^5 Mod 33401 = f3
Test number: 2   C: 1f   D: 5   C^5 Mod 33401 = 118e
Test number: 3   C: 21f   D: 5   C^5 Mod 33401 = 1858
Test number: 4   C: 31f   D: 5   C^5 Mod 33401 = 734c
Test number: 5   C: 39f   D: 5   C^5 Mod 33401 = 3ffa
Test number: 6   C: 3df   D: 5   C^5 Mod 33401 = 80a5
Test number: 7   C: 39e   D: 5   C^5 Mod 33401 = 3941
Test number: 8   C: 0     D: 5   C^5 Mod 33401 = 0
Test number: 9   C: 3ff   D: 5   C^5 Mod 33401 = 5206
```

Flow Summary:

Flow Summary	
<<Filter>>	
Flow Status	Successful - Thu Mar 24 17:38:31 2022
Quartus Prime Version	16.1.0 Build 196 10/24/2016 SJ Lite Edition
Revision Name	g35_modulo33401
Top-level Entity Name	g35_mod_exp
Family	Cyclone V
Device	5CSEMA5F31C6
Timing Models	Final
Logic utilization (in ALMs)	140 / 32,070 (< 1 %)
Total registers	33
Total pins	44 / 457 (10 %)
Total virtual pins	0
Total block memory bits	0 / 4,065,280 (0 %)
Total DSP Blocks	1 / 87 (1 %)
Total HSSI RX PCSs	0
Total HSSI PMA RX Deserializers	0
Total HSSI TX PCSs	0
Total HSSI PMA TX Serializers	0
Total PLLs	0 / 6 (0 %)
Total DLLs	0 / 4 (0 %)

Chip planner layout:

Coordinate: Editing Mode: ECO - 5CSEMA5F31C6



Node Properties

Selected elements: Add11-1

Properties/Modes

Properties/Modes	Values
Full Name	g35_mod_exp[g35_modulo33401]
Coordinate	(31, 5)
Resource Type	LAB combinational cell
Location	LABELL_X31_Y5_N0
Location Assignment	No
F0 LUT Mask	OFF0
F1 LUT Mask	OFF0
F2 LUT Mask	FOFF
F3 LUT Mask	FOFF
Latch Type	none
F0 LUT Equation	c \$ d
F1 LUT Equation	N/A

Top Combinational / Bottom Combinational

Properties Fan-in Fan-out

Node Properties Layers Settings Color Legend

Timing Analysis Summary:

For 4 period:

Requested Fmax = 250 MHz

Fast 1100mV 0C Model Hold Slack Value = 0.365

Slow 1100mV 85C Model Setup Slack Value = -14.543

Slow 1100mV 85C Model Fmax = 53.93 MHz

List the Worst-case Timing paths for the Setup times:

	Slack	From	To
1	-14.543	multiplication[16]	multiplication[0]
2	-14.543	multiplication[16]	multiplication[1]
3	-14.543	multiplication[16]	multiplication[2]
4	-14.543	multiplication[16]	multiplication[3]
5	-14.543	multiplication[16]	multiplication[4]

Logic utilization (in ALMs): 140 / 32,070 (< 1 %)

For 19 period -> passing

Requested Fmax = 52.63 MHz

Fast 1100mV 0C Model Hold Slack Value = 0.188

Slow 1100mV 85C Model Setup Slack Value = 1.315

Slow 1100mV 85C Model Fmax = 56.55 MHz