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:



(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:**

Text

Description automatically generated

Text

Description automatically generated

**Testbench:**

Text

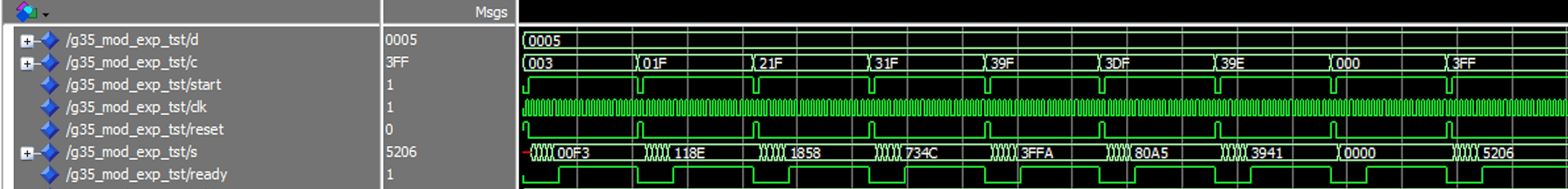
Description automatically generated

A picture containing graphical user interface

Description automatically generatedA picture containing calendar

Description automatically generated

**Simulation results:**



**Expected results:**

Calendar

Description automatically generated

**Flow Summary:**

Graphical user interface, text, application, email

Description automatically generated

**Graphical user interface

Description automatically generatedChip planner layout:**

**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\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_