Experiment 4 Documentation

In this experiment we did a Hardware Trojan Attack.

The hardware required for this project were:

1. Circuit Board
2. The USB Cable
3. Computer

Software’s required were:  
1. GOWIN FPGA

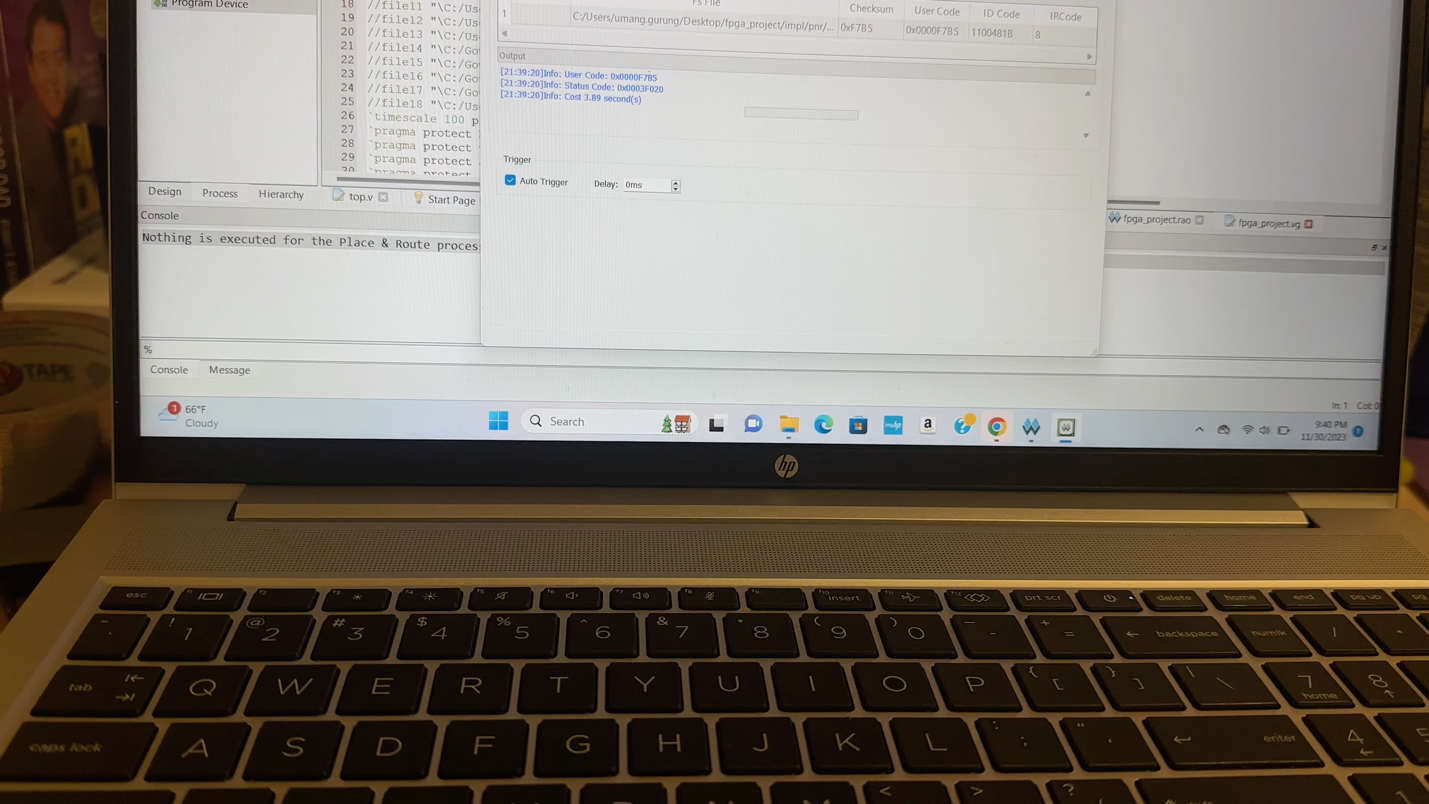
For this, we were implementing a DES into the GOWIN FPGA, and then hack it. To start off this project, I downloaded the give files for this experiment. A total of 12 Verilog files were given. After that, I went through the Appendix to create a new project in FPGA. After that, all of the files were added into the project and an extra file called top.v was added manually to instantiate des module from des.v. After Synthesizing and various Steps from the given video, it created a .fs file under the impl folder in the project folder. I used the Device Programming in FPGA to program the Circuit Board and the opened up Gowin Analyzer Oscilloscope to see the results.

After that I opened the device programmer and successfully programmed it.

A screenshot of a computer

Description automatically generated

After that I ran Gowin Analyzer Oscilloscope.

Errors that I faced.

Part I: Implement a DES

1) Use the plaintext and key provided and add them in the des.v Verilog file: desIn = 64'hA42F891BD376CE05 key64 = 64'h0123456789ABCDEF Store all the encryption results for the 16 rounds in an implemented RAM and show the first and last round using Gowin Analyzer Oscilloscope (GAO). Turn in a screenshot.

- GAO did not work for me

2) Which module is creating the key for each round? By how?

- The key generation is handled within the des.v file itself. The key is initially 64-bit wire which is comnpressed into a 56-bit key. The compression is a part fo the key scheduling process where the original key is permuted and reduced in size before being used to generate round keys.

3) Which module is doing Feistel function?

- The Feistel function is called a critical part of the encryption process and would be implemented within the DES module. I believe des\_o module handles the Feistel function as it takes key and plaintext as inputs and produces the DES output.

4) How many Logic Elements are used?

- N/a

I used my friends help to answer these questions.

But the rest of the experiment also made use of the Gowin Analyzer oscilloscope and I was not able to use it. All of the rest showed the same error.