Hardware Trojan Attacks 1

1. Make sure user downloads “HaHav3\_helpful\_codes.zip”
2. Open FPGA IDE
   1. Select “New Project”
   2. Name project “ex4”
   3. For Device Select the following:
      1. Series: GW1N
      2. Device: GW1N-9
      3. Package: LQFP144
      4. Speed: C6/I5
   4. Press “next”
3. Click your project folder and press “Add files”
   1. Ensure all files are added from the experiment 4 codes
   2. Also include “gowin\_pin\_assignments.cst” & “sampe\_top.v”
4. Click “Hierarchy” and set sample\_top.v to “Set as top module”
5. On the process tab, click “Synthesize” and run
6. Next, add a new GAO file, ensure “Standard” is switched to “lite”
7. Go to the new GAO file,
   1. Click the “…” button next to the clock
   2. Press search
   3. Select CLK\_50
8. In the GAO file, under “Capture signals”
   1. Press search
   2. Select “des\_instance/cnt[3:0]”
   3. Also select “des\_instance/desout[63:0]
9. Click “place & route”
   1. Click “enable programmer”
   2. Select device and press the program button (furthest right button)
   3. Press the “auto” button
   4. You should see the output of the DES encryption process. The encryption process will undergo 16 rounds of transformation inside the DES algorithm.

A screen shot of a computer

Description automatically generated

Part 2

1. Locate des\_0 file inside des.v
2. You will want to add the following code to test different triggers:
   1. A computer code with numbers and symbols

      Description automatically generated with medium confidence
3. Return back to capture signals
   1. Add des\_instance/key56[55:0]
   2. Add your modified key (Trojan Key)
4. Synthesize & Place & Route
5. Go back to the Gowin Analyzer Oscilloscope and download your modified code
   1. Click the Auto button
   2. You will see that once the des 4 least significant bits displays “0110”, the modified key “Trojan Key” will flip its LSB to “0” here is an example right after one of the three triggers were hit:

A screenshot of a computer

Description automatically generated

Part 3

1. You will change the des\_0 module as you did in part 2
   1. Make sure to include a current\_state & next\_state like the picture below:
2. Add the following 2 signals:
   1. Current\_state
   2. Next\_state
3. Synthesize and Place & Route
4. Open Oscilloscope, download file, and select “Auto”
5. You will notice that if the modified “Trojan key” is different from the key, you have successfully inserted into the circuit A screenshot of a computer

   Description automatically generated