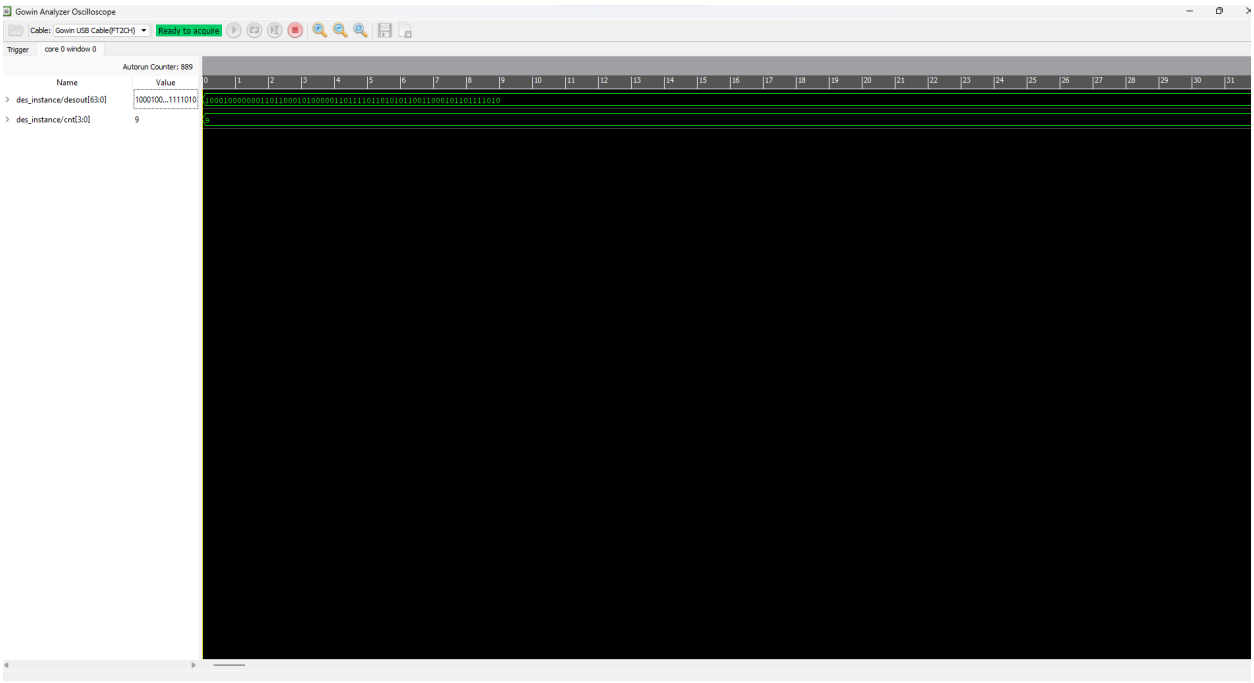
Hardware Trojan Attacks 1

1. Make sure user downloads “HaHav3_helpful_codes.zip”
2. Open FPGA IDE
    a. Select “New Project”
    b. Name project “ex4”
    c. For Device Select the following:
        i. Series: GW1N
        ii. Device: GW1N-9
        iii. Package: LQFP144
        iv. Speed: C6/I5
    d. Press “next”
3. Click your project folder and press “Add files”
    a. Ensure all files are added from the experiment 4 codes
    b. 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,
    a. Click the “…” button next to the clock
    b. Press search
    c. Select CLK_50
8. In the GAO file, under “Capture signals”
    a. Press search
    b. Select “des_instance/cnt[3:0]”
    c. Also select “des_instance/desout[63:0]
9. Click “place & route”
    a. Click “enable programmer”
    b. Select device and press the program button (furthest right button)
    c. Press the “auto” button
    d. You should see the output of the DES encryption process. The encryption process will undergo 16 rounds of transformation inside the DES algorithm.

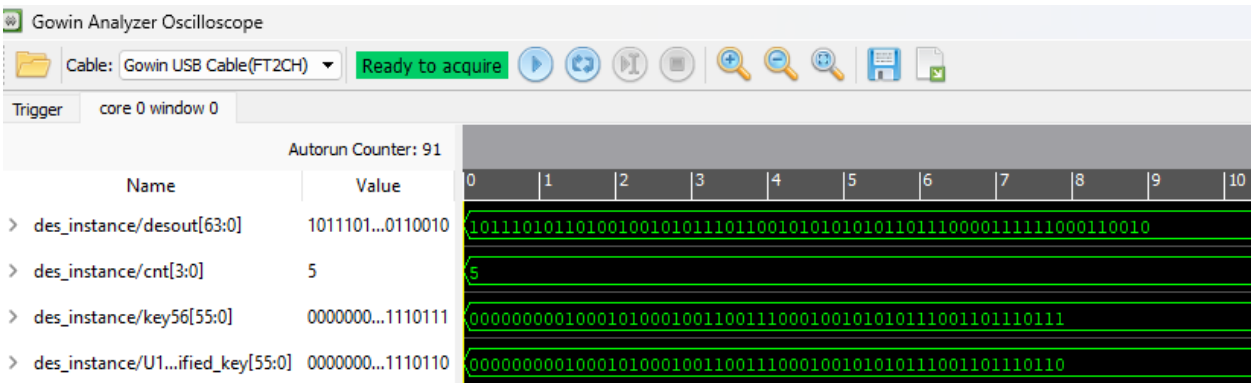


Part 2

1. Locate des_0 file inside des.v
2. You will want to add the following code to test different triggers:

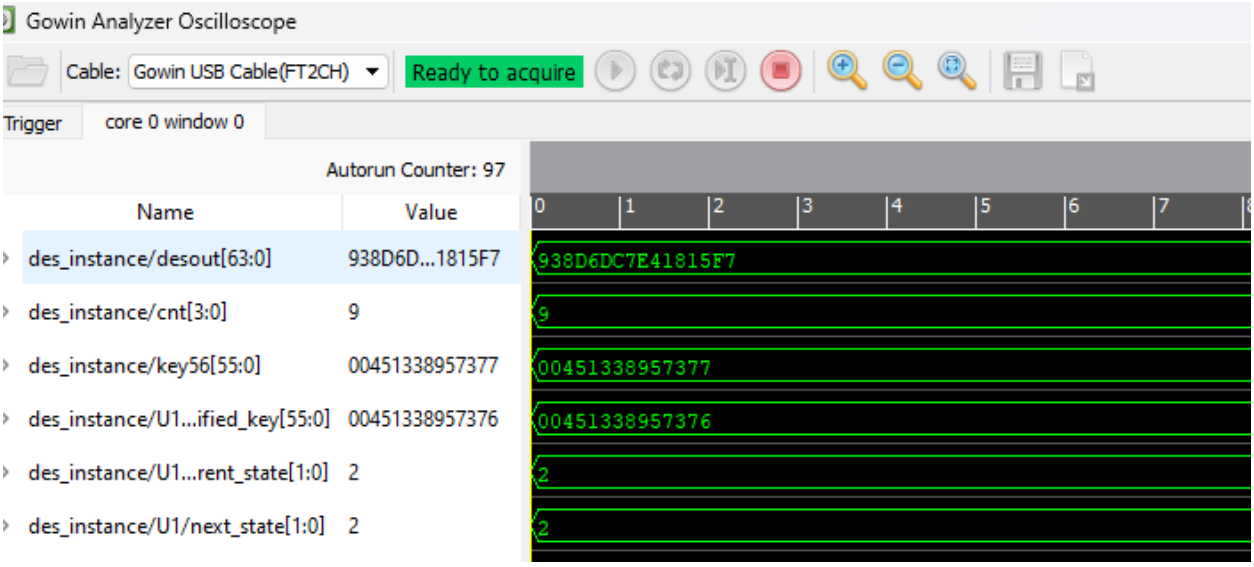
```
// Trojan trigger conditions for different parts of the experiment
wire trigger_0110 = (out[1:4] == 4'b0110);
wire trigger_1001 = (out[1:4] == 4'b1001);
wire trigger_1010 = (out[1:4] == 4'b1010);

    // Register to hold the possibly modified key
reg [55:0] modified_key;
always @(posedge clk) begin
    if (trigger_0110 || trigger_1001 || trigger_1010) begin
        // Invert the LSB of the key if any trigger condition is met
        modified_key <= {key[55:1], ~key[0]};
    end else begin
        // No trigger condition met, keep the original key
        modified_key <= key;
    end
end
```

   a.
3. Return back to capture signals
   a. Add des_instance/key56[55:0]
   b. Add your modified key (Trojan Key)
4. Synthesize & Place & Route
5. Go back to the Gowin Analyzer Oscilloscope and download your modified code
   a. Click the Auto button
   b. 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:



Part 3

1. You will change the des_0 module as you did in part 2
    a. Make sure to include a current_state & next_state like the picture below:
2. Add the following 2 signals:
    a. Current_state
    b. 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



Part 4 Extended: Change the trigger condition

1. The direction the sensor is sensing the acceleration is perpendicular to the HaHa Board.
2. Attached is the Verilog code that changes the trigger condition for the Trojan (src/des_extended.v). Once the board is more than 45-degrees tilted, the trojan will be triggered.