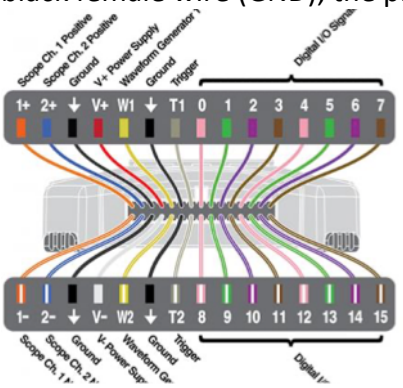
Bus Snooping Attack

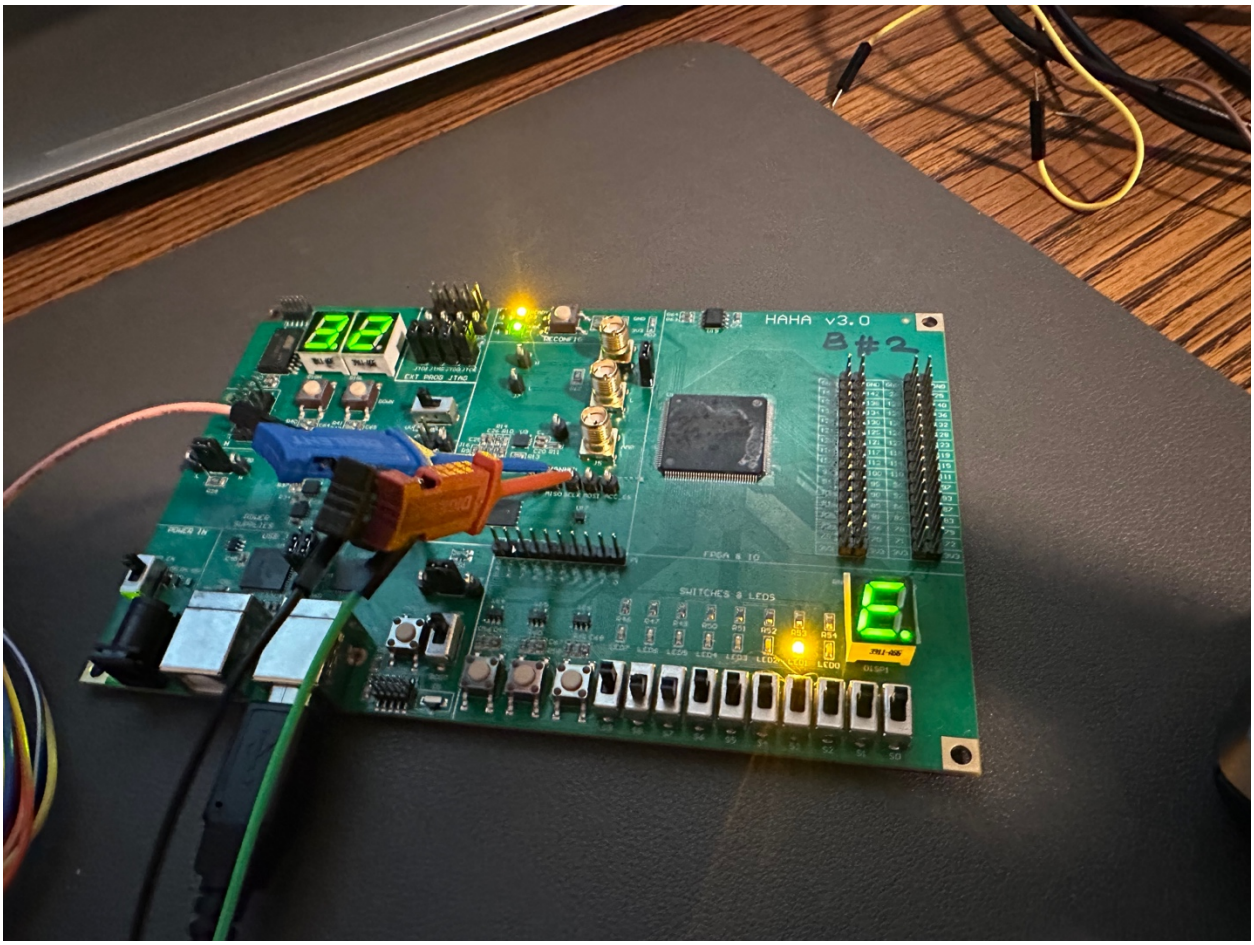
The goal of this experiment is to carry out a bus snooping attack at board level which leads to retrieving secret information from a system through physical access.

Steps:

1. Program microcontroller using Atmel Flip software. Use “U_1.hex” file for working accelerometer.
2. Lie HaHa board on a flat surface and hit the MCU RST button until you see at least 1 LED light up.
3. Slowly tilt the HaHa board and you should see multiple LED’s lighting up towards the direction of the tilt.
4. Turn HaHa board off
5. If no male to male jumper wires are in your kit, you will need 3 “Mini Grabber Test Clips” with one of the colors ideally being black for the “GND” connection
6. Now with the Analog Discovery 2, insert the connector into the Discovery 2, find the top black female wire (GND), the pink 0, and green 1 digital I/O signals. (see diagram below)

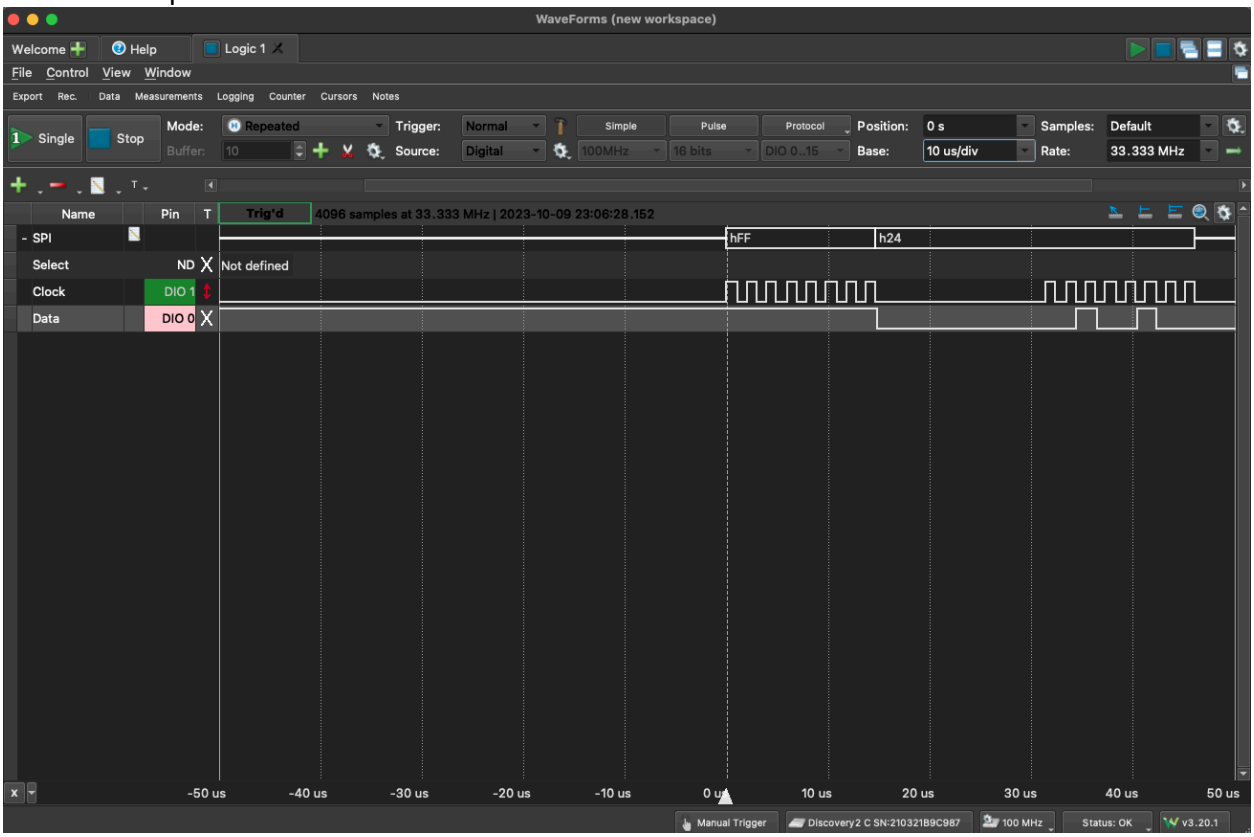


7. Now, insert the 3 wires into 3 different mini grabber test clips.
8. Attach Pink 0 wire to “MISO”, Green 1 wire to “SCLK”, and black to GND pin (located at J15)



9. Open Waveforms software, click on “Logic” on the left side.
10. Click “Click to add channels” and click SPI
11. Select should be set to “none”, Clock should be set to DIO 1, and Data should be set to DIO 0. Now, click “Add”
12. You will see clock and data on a panel on the left side, click the black “X” on the clock, and change to “Edge”
13. Turn on your HaHa board and ensure the LED’s change and the board tilts
14. On the top right of your screen, change the “Base” to “10 us/div”

15. Observe the pattern such as the one below:



Questions:

Which line would you say is the clock line? How fast is the clock running at?

In most communication protocols, the clock line is the one with a regular, repeating pattern. On an oscilloscope, you should observe a square wave that consistently goes up and down. The frequency of this wave indicates the speed of the clock. To determine how fast the clock is running, you can measure the time between two rising (or falling) edges of the clock signal. The inverse of this time will give you the frequency of the clock. For instance, if the time period between two rising edges is 10 ns, then the clock frequency is 100 MHz.

Which line would you say is the data line?

The MISO line stands for "Master In Slave Out". Given the typical SPI naming convention, MISO would be the data line where data is transmitted from the slave to the master. The data line typically does not have a consistent pattern like the clock line, unless the same data is being sent repetitively. You'll see changes in the MISO line corresponding to the data being transmitted.

How to prevent such attacks:

Shielding: Encase the board or sensitive traces in a metal shielding to prevent easy probing.
Traces: Route critical traces internally within the multi-layer PCB instead of on the surface.
Tamper Detection: Implement mechanisms that can detect tampering and erase sensitive data upon detection.
Encryption: Encrypt data on the bus. This won't prevent the data from being intercepted, but it will make the intercepted data meaningless without the decryption key.