Experiment 5 Summary

This experiment focused on designing and analyzing a hardware trojan attack, where the trojan is triggered by specific conditions, particularly the temperature of a chip. The experiment was conducted in several parts using a FPGA on a Hardware Hacking (HaHa) board. This program was not completed in its entirety, but parts 1 – 3 were predicted using online material and ChatGPT interpretation.

Part 1: The experiment began with designing a system using the FPGA's internal ADC, PLL, and RAM to measure the on-chip temperature and display it in the memory content window. The temperature measurements were verified against room temperature readings.

Part 2: The temperature value was then displayed using LEDs and a 7-segment display. The design involved processing temperature data from the RAM output and displaying it in a readable format.

Part 3: A temperature-triggered trojan was implemented. This trojan was designed to alter data in a second instance of RAM when the temperature exceeded 40 degrees Celsius. When activated, the trojan inverted the data value in the memory, observed through the in-system memory window.

The experiment demonstrated how a hardware trojan could be activated by a physical parameter change, in this case, temperature, and how it could corrupt important data in a system's memory under specific conditions. The findings highlight the potential vulnerabilities in hardware systems to such trojans, especially when they are activated under seemingly normal operating conditions like temperature changes.