University of Maryland, Baltimore County
CMPE/ENEE 491/691
Spring 2023
HW-4: Trojan Detection
Jordan Kieltyka

Using Testability Parameters for Trojan Detection

The method used for determining the location of the trojans in the provided circuit is through using the SCOAP technique and calculating the value for CC. The value for CC is equal to the square root of the sum of CC0 to the second power and CC1 to the second power. This method is effective, because the higher the CC value, the more difficult it is for a user to control the signal for testing for the presence of a trojan.

CC0 and CC1 were obtained through using the TetraMAX tool, which were then used for the calculation of CC. CC0 and CC1 were parsed from a TetraMAX output file and CC calculated using a C based program. Only pins with inputs were taken into consideration during the parsing for CC0 and CC1, since the connected-net of the input pins is simply an output signal from a previous gate or direct input.

The CC value was calculated using CC(s) = sqrt[CC0(s)^2 * CC1(s)^2]. After the CC value was calculated, it was then compared to the current list of top thirty highest CC values. If the signal was lower than the current top thirty, or was a duplicate of what was in the current top thirty, it was simply discarded. This process was repeated until all input type pins were compared against the top thirty CC list.

It was discovered that there were a few locations where CC0 and CC1 were greater than 254. This is important since the max CC0 and CC1 value the TetraMAX tool can go up to is 254. This means that the CC values for these signals could be much higher than calculated, and would result in a location where a trojan would be extremely difficult to detect.