Impact of Gate Grouping on Hardware Trojan Detection

Alex Yeoh

*Wright State University*

Yeoh.3@wright.edu

I. Background

In Dr. Xue’s dissertation [1], in the section called *Self-Reference-based Hardware Trojan Detection*, he discussed the impact of the size of gate groupings on the efficacy of his proposed hardware trojan (HT) detection method. Following this line of thought, Christopher Otey, Jacob Buchanan, and I considered the impact of grouping different gates together with the same gate grouping size on the efficacy of Dr. Xue’s HT detection method.

II. Gate Groupings

For this, we decided to use CUT2 from [1] as seen below in figure 1 because it was already partitioned into gate groups of size 2.

A diagram of a block diagram

Description automatically generated

Figure 1: Partitioned CUT2 from [1].

With the circuit and the gate groupings size decided upon, we designed two more gate grouping patterns for the same circuit, as seen below in figure 2.

A collage of diagrams

Description automatically generated

Figure 2: All gate groupings used.

III. Gate Design

The gates were made at a transistor level as seen in appendix A with local VDD and VSS pins to implement the HT detection method in [1] which requires the CUT to be segmented into different regions that have separate power and ground rails. The gate widths were modified through trial and error to minimize the skew of the gates as seen in appendix B. The trojan chosen was a bypass inverter because that is the same trojan used in [1]; however, due to the lack of mention on the sizing of the HT used in [1], we decided to use a 2:1 PMOS to NMOS ratio for the widths of the HT to keep in line with standard VLSI design practices.

IV. Calculating Ideal Power for Each Gate Group

We initially needed to determine the power consumed by any single gate for all their relevant input patterns. To do this, we simulated the gate using typical-typical (tt) analysis, used pulse inputs to generate every input pattern, and averaged the simulated power of the gate at the relevant time periods as seen below in figure 3.

A screenshot of a computer

Description automatically generated

Figure 3: ADEL for generating tt static power for a 2-input gate.

We performed this analysis for all the gates and the clock tree, and the resulting power can be seen below in table 1.

A screenshot of a table

Description automatically generated

Table 1: Relevant average powers

Before using the average powers from the tt simulations seen in table 1 above, we determined the inputs for each gate in the CUT as seen below in figure 4. This was accomplished by mapping the relevant inputs to each input of the gates of the CUT and using Excel’s Boolean logic functions to solve for what the input to a gate would be if the input was an output of a gate. The full results of the input determination process for each segment can be seen in appendix C.

A diagram of a circuit

Description automatically generated

Figure 4: Mapping the input of a gate to the output of another gate following the CUT.

After generating the inputs for every gate, the power values simulated in table 1 above are mapped to the gates by referencing the gates inputs as seen below in figure 5. The full results of this are shown in appendix D.

A screenshot of a computer

Description automatically generated

Figure 5: Determining gate power by input.

With the power for each gate determined, the power for each gate grouping can be determined by adding together the power for the relevant gates as shown in figure 6 below following the groupings depicted in figure 2 above.

A screenshot of a computer

Description automatically generated

Figure 6: Determining power by gate grouping.

V. Simulating Measured Power

To determine the measured power, the circuits shown in figures A9, A10, and A11 from appendix A are simulated with Monte-Carlo analysis with the test cases shown in figure 7 below.

A screenshot of a computer

Description automatically generated

Figure 7: ADEXL for simulating and gathering measured power data.

The test cases allow for all the segments to be simulated and all the relevant average measured power to be gathered all at once and for all the data to be exported to a Comma Separated Value (CSV) file which allows the power data to be easily transferred to Excel.

VI. Data Analysis

With the measured power data in Excel, we followed [1] by using the excel solver to solve for λclock with the bounds expanded due to the different process size, seen below in figure 8.

A screenshot of a graph

Description automatically generated

Figure 8: Using the Excel solver.

This process was repeated with HTs of various sizes until each gate grouping had a different minimum detectable HTs in segment 1. Every iteration can be seen in appendices E, F, and G for the paper groupings, grouping 1, and grouping 2 respectively. Using the expanded bounds, the minimum detectable HT size for each grouping is 0.892%, 0.571%, and 0.785% for the paper group, group 1, and group 2 respectively, as seen below in table 2.

A table with numbers and text

Description automatically generated

Table 2: Segment 1 λclock values at different HT% of CUT

After calculating Λ, it becomes evident that the bound for Λ will need to be increased to approximately 36% to not falsely detect a hardware trojan in segment 3. As such, the minimum detectable HT sizes are 0.892%, 0.785%, and 0.682% for the paper group, group 1, and group 2 respectively, as seen in table 3 below.

A table with numbers and symbols

Description automatically generated

Table 3: Minimum Λ values

VII. Conclusion

As seen in the data analysis section, different gate groupings did have an impact on the minimum detectable HT. As seen in table 2 above, the minimum detectable HTs when looking at λclock were at 0.892%, 0.571%, and 0.785% of the CUT for the paper group, group 1, and group 2 respectively. As seen in table 3 above, the minimum detectable HTs when looking at Λ were at 0.892%, 0.785%, and 0.682% of the CUT for the paper group, group 1, and group 2 respectively.

**References**

[1] H. Xue, “Hardware Security and VLSI Design Optimization Hardware Security and VLSI Design Optimization,” Ph.D. dissertation, Dept. Elect., Wright State Univ., Dayton, OH, USA, 2018. Accessed: Apr. 26, 2024. [Online]. Available: https://corescholar.libraries.wright.edu/cgi/viewcontent.cgi?article=3347&context=etd\_all

Appendix A: Gate Designs

The following are the schematics for all the gates used.

A screenshot of a computer

Description automatically generated

Figure A1: Schematic for an inverter.

A screenshot of a computer

Description automatically generated

Figure A2: Schematic for a NAND2 gate.

A diagram of a computer

Description automatically generated

Figure A3: Schematic for an AND 2 gate.

A diagram of a computer

Description automatically generated

Figure A4: Schematic for A NOR2 gate.

A diagram of a computer

Description automatically generated

Figure A5: Schematic for an OR2 gate.

A diagram of a circuit board

Description automatically generated

Figure A6: Schematic for a XOR2 gate.

A diagram of a computer

Description automatically generated

Figure A7: Schematic for a D-type Flip-Flop.

A screenshot of a computer

Description automatically generated

Figure A8: Schematic for the bypass inverter trojan.

A diagram of a computer

Description automatically generated

Figure A9: Schematic for the CUT.

A diagram of a computer

Description automatically generated

Figure A10: Schematic for the CUT with the trojan inserted in segment 0.

A diagram of a computer

Description automatically generated

Figure A11: Schematic for the CUT with the trojan inserted in segment 1.

Appendix B: Tested Widths

The following are the tables for all the recorded tested widths for sizing the gates in appendix A.



Table B1: Table of recorded inverter width tests.



Table B2: Table of recorded NAND2 width tests.



Table B2: Table of recorded AND2 width tests.

A table with numbers and a yellow line

Description automatically generated

Table B2: Table of recorded NOR2 width tests.

A yellow line with black numbers

Description automatically generated with medium confidence

Table B2: Table of recorded OR2 width tests.

A table with numbers and a yellow line

Description automatically generated

Table B2: Table of recorded XOR2 width tests.

A table with numbers and a yellow line

Description automatically generated

Table B2: Table of recorded D-type Flip-Flop width tests.

Appendix C: Inputs for Every Gate by Segment

The following are the tables for all the inputs of every gate based on the input pattern.

A table with numbers and symbols

Description automatically generated

Table C1: Inputs for every gate in segment 1 by segment input pattern.

A table of numbers with a number in the center

Description automatically generated with medium confidence

Table C2: Inputs for every gate in segment 2 by segment input pattern.

A table with numbers and symbols

Description automatically generated

Table C3: Inputs for every gate in segment 3 by segment input pattern.

Appendix D: Power for Every Gate by Segment

The following are the tables for the power of every gate based on their inputs.

A table with numbers and symbols

Description automatically generated

Table D1: Power for every gate in segment 1 by input.

A table of numbers and a line

Description automatically generated

Table D2: Power for every gate in segment 2 by input.

A table with numbers and a number

Description automatically generated

Table D3: Power for every gate in segment 3 by input.

Appendix E: Paper Grouping Data

The following are the tables for the Data for the paper groupings.

A screenshot of a spreadsheet

Description automatically generated

Table E1: Data when HT is 1% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table E1: Data when HT is 0.8920% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table E1: Data when HT is 0.7851% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table E1: Data when HT is 0.6819% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table E1: Data when HT is 0.5713% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table E1: Data when HT is 0.1382% of the CUT.

Appendix F: Grouping 1 Data

The following are the tables for the Data for group 1.

A screenshot of a spreadsheet

Description automatically generated

Table F1: Data when HT is 1% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table F1: Data when HT is 0.8920% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table F1: Data when HT is 0.7851% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table F1: Data when HT is 0.6819% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table F1: Data when HT is 0.5713% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table F1: Data when HT is 0.1382% of the CUT.

Appendix G: Grouping 2 Data

The following are the tables for the Data for the group 2.

A screenshot of a spreadsheet

Description automatically generated

Table G1: Data when HT is 1% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table G1: Data when HT is 0.8920% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table G1: Data when HT is 0.7851% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table G1: Data when HT is 0.6819% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table G1: Data when HT is 0.5713% of the CUT.

A screenshot of a spreadsheet

Description automatically generated

Table G1: Data when HT is 0.1382% of the CUT.