Project: Trusted Electronic Systems

Advisor: Dr. Geiger & Dr. Chen

Members: Fatema Aftab (Team Leader), Yitao Liu (Key Concept Holder), Qian Chang (Communications Leader) Chao Huang (Communications Leader), Colton Bachman (Webmaster), Xin Hu (Webmaster)

Weekly Summary

The main goal for this week was to do research about hardware Trojan detecting and build our senior design website. We met with Dr. Geiger and Dr. Chen on February 3rd and reported what we did for last week. From our researching and meeting with the two professors, we find the key point for us so far is how to detect hardware Trojan. Therefore, we did lots of research about the methods of detecting HT last week. On the other hand, Xin Hu and Colton Bachman start making our senior design website.

Pending Issue

1. Figure out a good way that can detect hardware Trojan (HT).
2. Finish the website
3. Career fair this week, we may need to change some schedule for someone who want to go to career fair.

Plans for next week

Continuing work on detecting HT. Discuss with Dr. Chen and Dr. Geiger about the method we found last week about detect HT. If they are valid and operable, we are going to digger more information in this direction. Meanwhile, we still need to read more paper about HT and HT detecting.

Personal Contribution

(No team contribution because we are not start our project yet. For this part, some of the teammates provide what they read and their notes for our future project.)

- Colten Bachman (2 hrs):

He spent about 2.5 hours researching the topic and working on the website with Xin. He made a quick website with Weebly and I'm looking for a good way to export the files and put it on our server. The paper I read about dealt with detecting hardware trojans. They described ways to detect like failure analysis-based testing, 'standard' VLSI fault detection tools, and precisely measuring voltage in versus voltage out. The most reliable methods the paper described seem to take NP time to detect trojans using the failure analysis testing. That paper also classified trojans into different categories: type, size, distribution, structure. The activation characteristics were also categorized into externally activated and internally activated categories.

- Xin Hu (9 hrs):

Main point:

Using Pearson product-moment correlation coefficient to find the Hardware Trojan.

Detail:

According to last week's research, I found that no matter what a hardware Trojan hidden in CS, when the Trojan is activated and starts running, it will cost the extra power from IC. Although we know that a sophisticated hardware Trojans will try to control their size and power but if we divided IC into several different parts, I think it can still be found the different power cost between clean ICs and hacked ICs. Assmue fclk is IC's running clock time, K is the timing for IC running an operation. Pv is the process variation from this IC, and Pr is the random variation from IC. So we have Pt =P(fclk, K) + Pv + Pr.. In addition, for a IC which has a hardware Trojan, we have Pt = P(fclk, K) + Pv + Pr + Pt(fclk, K). Pt means the cost power from hardware Trojan. As function shows, I found if the process variation and random variation are small enough to be ignored, we could found the hardware Trojan by using this function. However, due to scientific rigor, we must be reduced to the minimum possible error. At this point, I think we could using the average to reduce the error. Let's assume to we have an original IC that do not hiding hardware Trojan. We could use this function to calculate multiple times to have the average of cost power. Sn = (P1, P2, P3 …. Pm). This is real simple way to ignore the process variation and random variation in the Physics and Chemistry measure, it calls Golden Model (GM). So when we have this GM, what we need to do for detect the hardware Trojan is analyze is that the variation is out of the acceptable error number between GM and Trojan ICs.

- Qian Chang (4 hrs):

Main point:

Using current integration and localized current analysis to detect Trojan.

Detail:

We can assume that IC authentication phase is done after manufacturing test. If Itrojan _ free (t) and Itrojan _ inserted (t) denote the instantaneous supply current drawn by Trojan-free and Trojan- inserted circuit at time t, respectively, then the integrated current at time t for Trojan-free and Trojan-inserted circuit (Qtrojan-free(t) and Qtrojan-inserted(t)) can be expressed by equations (1) and (2) (note that dq = I . dt)

$$Q_{trojan\text{-}free}(t) = \int I_{trojan\_free}(t) \cdot dt \quad (1)$$

$$Q_{trojan\text{-}inserted}(t) = \int I_{trojan\_inserted}(t) \cdot dt = \int (I_{trojan\_free}(t) + I_{trojan}(t)) \cdot dt \quad (2)$$

where Itrojan(t) denotes the current drawn by Trojan. Since same pattern set is applied to both golden chips and chip

Under-authentication, the difference between Itrojan _ free (t) and Itrojan _ inserted (t) comes from (1). The additional current drawn by Trojan gates and (2) changes in the circuit current due to process variations. By integrating the charge along time axis for both chips, their cumulative difference at time t can increase as more number of patterns are applied. During Trojan detection phase, the total supply current is integrated for chip-under-authentication and the golden chip separately. All Trojan gates located on chip will contribute to overall current consumption. Therefore, the total supply current's difference beyond the predefined threshold between the two chips will imply the existence of Trojan.

- Fatema Aftab

Mainly focused on reading detecting Trojan hardware paper, and doing research about it.

- Chao Huang:

I read three papers and did some researches for relative information. I focused on what kind of detecting method is more compatible for different kind of Trojans. In additional, I also did some research about how to target hardware Trojan. I did find some method to detect HT, but they all somehow depend on types of Trojan.

- Yitao Liu

Keep working on papers about hardware Trojan detection, and made a lot of preparation on notebook for researches and the project

Team member: name	Contributions in this week(hours)
Chao Huang	5hrs
Colten Bachman	2.5hrs
Qian Chang	8hrs
Yitao Liu	6.5hrs
Fatema Aftab	7hrs
Xin Hu	9hrs