Statement of Research

As the semiconductor fabrication process advance, the design complexity rises a lot, and the cost has become prohibitive. It is almost impossible for every company nowadays to design and fabricate every part of their products in-house. They usually have to focus on a specific business and rely on other companies to take care of the rest. For example, to make an iPhone, Apple design the CPU. They need to use EDA tools from EDA tool vendors to simulate and make the best design. Then, they send it to TSMC in Taiwan for fabrication. Also, they might need DRAM from SK Hynix from Korea and have TSMC integrate them and maybe have another company to test and package it. For a single component, there are already few companies involved, not to mention the rest. This kind of paradigm opens vast possibilities for an adversary to insert malicious circuit and incurs serious security problems.

It is estimated that around 1% of the total semiconductor devices sold around the world are counterfeit [1]. These counterfeit semiconductors cost the United States alone a loss of $7.5 billion per year [2]. In 2015, the semiconductor industry posted its total sales, amounting to $335.2 billion [3]. However, it remains unknown how many of these total sales are counterfeit. One of the significant implications for such a large number of counterfeit Integrated Circuits (IC) is the presence of an unsecure supply chain. With an unsecure supply chain comes the risk of Hardware Trojans, which are surreptitiously placed malicious alterations in the IC that are triggered to cause system failure or to covertly leak confidential information and thereby compromise security and privacy [4]. This scenario has become even more probable due to the globalization of IC development, where ICs are designed, fabricated, assembled, and tested all around the globe.

To make sure the security of the IC throughout its lifecycle we proposed the Digital Twin approach. The Digital Twin is a virtual/digital representation of the IC. You may view it as a virtual golden model. During the design time, typically, we have the design, libraries, and benchmarks. We use them to simulate, implement and verify our design and then we get the layout for fabrication. So we take this information to build our Digital Twin through machine learning or some statistical methods. Later, after the fabrication, we put the chip into post-manufacturing test and field operation. We use the internal signals, and information gathered from the embedded sensors and the external sensors to make out Digital Twin up-to-date. So that it can adapt to the process variation and aging effect. We can then use the Digital Twin as a golden model to detect the hardware Trojan.

Reference

[1] N. Kae-Nune and S. Pesseguier, “Qualification and Testing Process to Implement Anti-Counterfeiting Technologies into IC Packages,” in Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013, 2013, pp. 1131–1136.

[2] C. LEVIN, “The committee’s investigation into counterfeit electronic parts in the department of defense supply chain,” 2011.

[3] D. Rosso, “Global Semiconductor Sales Up 7 Percent Year-to-Year,” Semiconductor Industry Association (SIA), 2017. [Online]. Available: http://www.semiconductors.org/news/2017/01/03/global_sales_report_2015/global_semiconductor_sal es_up_7_percent_year_to_year/. [Accessed: 23-Jan-2017].

[4] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, “Hardware trojan attacks: Threat analysis and countermeasures,” Proc. IEEE, vol. 102, no. 8, pp. 1229–1247, 2014.