# Hardware Trojan Detection through Electromagnetic Side-Channel Statistical Analysis: A Gold Chip Free Approach

**Presenter:** Jiaji He and Xiaolong Guo
**Advisor:** Dr. Yier Jin
University of Central Florida

Hardware Trojan (HT) has become a major threat for the integrated circuit (IC) industry and supply chain. There are already many hardware Trojan detection methods, among which the side-channel based method is one of the most promising techniques. However, most of existing solutions require some sort of golden circuit for signature generation and comparison. We propose a novel method utilizing the electromagnetic (EM) side-channel to detect HTs in the circuit. We also developed a method to generate the spectrum signature using the design at early stage to serve as the golden reference. We will demonstrate the effectiveness of the proposed method on FPGA using Trojan-infected AES benchmarks from the Trust-Hub.

Figure 1 shows the setup of our demo, where we use a SAKURA-G board specifically designed for research and development on hardware security as the FPGA platform. The board is fixed on an X-Y-Z positioning system in order to conveniently adjust the position of the board. The probe used for collecting the EM radiation/signal belongs to RF family from LANGER. Also the probe is fixed on another X-Y-Z positioning system so as to accurately adjust the probe to the best position, and the probe is just above the surface of the FPGA (note that during the live demonstration, we may not bring the X-Y-Z positioning system with us due to its weight). After the EM signal is collected from the probe, a pre-amplifier is used to amplify the signal. Other equipment includes an oscilloscope and a laptop.

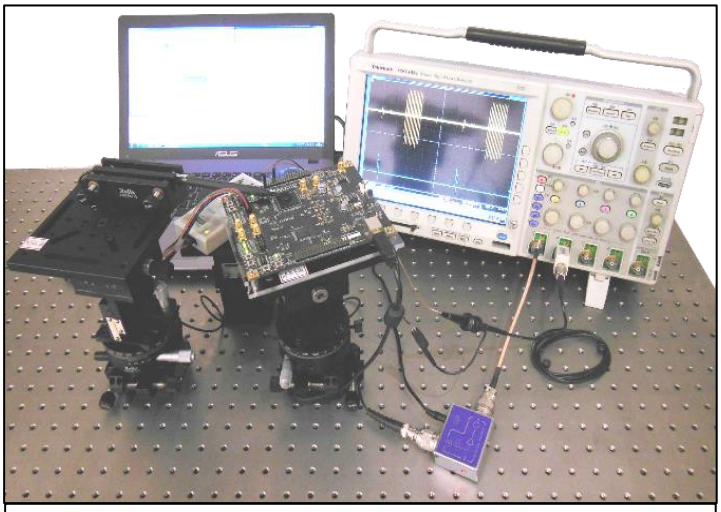

*Figure 1. The setup of the EM-based Trojan detection demo.*

We will run selected AES benchmarks downloaded from Trust-Hub.com. In order to carry out the Trojan detection, we first need to use the simulation data at early stage to generate the golden signature reference. Then after the EM signal is collected from the real circuit, we can compare and find out the differences between these two set of data.

For the audience, we will show how to use the simulation data at early stage of the IC lifecycle to generate the spectrum. We will further show whether the Trojan is activated through the indicating lights on the board. After the data is collected and transport to the computer, with the help of the data processing, we will be able to find the differences when the Trojan is activated.