HOST 2018: Student HW Demonstration Proposal

Presenting Author: Andrew Stern

Authors: Andrew Stern, Joey Botero, Bicky Shakya, Haoting Shen, Domenic Forte, Mark Tehranipoor

Title: EM-based Fingerprinting for Counterfeit Detection with Demonstration on Remarked ICs

Research Description:

The globalized nature of the semiconductor supply chain has made counterfeit integrated circuits (ICs) a pervasive issue. Modern counterfeit detection techniques are limited by relatively high cost, lengthy inspection time and can even be destructive in nature. We demonstrate a novel method of counterfeit IC detection which takes advantage of design-specific electromagnetic (EM) fingerprinting. Using the clock distribution network, we can generate a design-specific fingerprint which relies on the physical parameters of the chip without any additional overhead. We demonstrate this technique on 8051 microcontrollers from three vendors and differentiate between them using machine learning with approximately 99% accuracy. This EM-based fingerprinting technique provides a complex attack surface while remaining a fast and low-cost approach for detecting several types of counterfeit ICs.

Note: The paper discussing this research is currently under review for publication.

Hardware Demonstration:

The hardware demonstration will show how integrated circuits using the same functional IP can be clearly differentiated through electromagnetic fingerprinting. Using 8051 ICs from different vendors to emulate remarked ICs, we are able to take a measurement of 2 microseconds and easily distinguish between the various vendors by using principal component analysis. Demonstrating this using an unsupervised machine learning technique shows that if a buyer is sent several chips and does not have a golden IC to compare against, they are still able to separate the ICs into different groups. Once this is completed, only 1 IC from each group needs to be further inspected as you can be more confident that all parts have similar characteristics. Alternatively, if a golden IC is available, you can easily compare it against the acquired chips under test.

Figure 1 shows the required setup. This includes an oscilloscope, two power supplies, a waveform generator, wide-band amplifier, device breakout board, near-field EM probe and holder and a laptop running MATLAB.

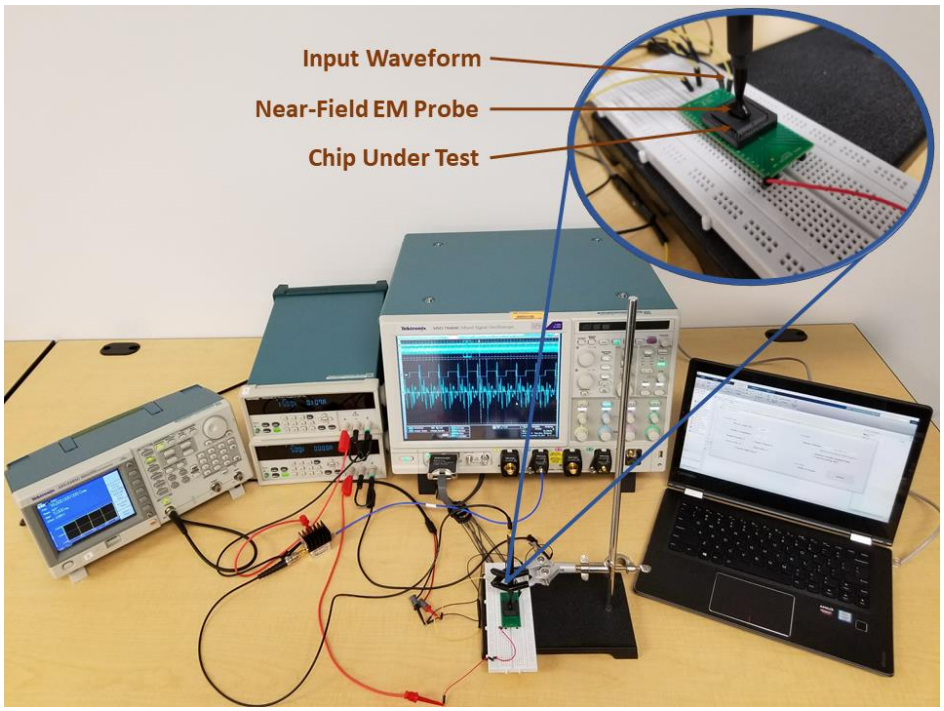

Figure 1: EM-based Fingerprinting Demo Experimental Setup

Observables:

This demo will show how quickly and easily ICs can be tested through EM-based fingerprinting. Using only the power, ground, and clock input pins, this method does not require extensive knowledge of the device or any test vector generation. Additionally, this all done without programming the device, so this method can be extended to one-time-programmable (OTP) devices as well.

A GUI will be used to describe the collected data and the result derived from the machine learning model comparison. Several devices will be available for the audience to choose from as to not introduce any inherent bias within the demonstration. It should be noted that the devices chosen for the demonstration will not have been included in the training set, although are a part of the same vendor-specific device family.