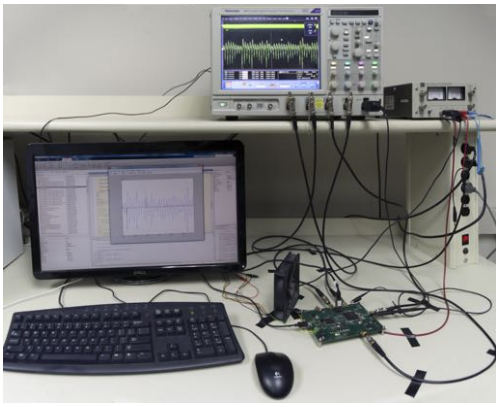
# HOST Demo Proposal : Firmware Instruction Identification Using Side-Channel Power Analysis

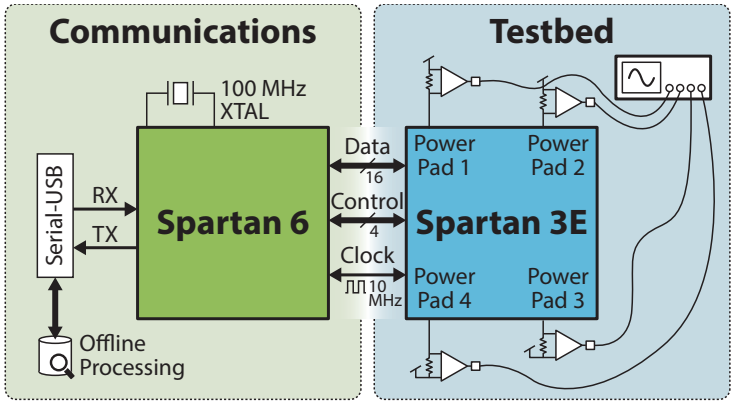
## Proposal

In this work, we present results from Side-Channel Analysis performed over multiple power supply pins and demonstrate the relationship between the power transients and machine-level instructions on an instance of the openMSP430 processor on an FPGA. However, this technique is also applicable to standalone ASIC instances. Our approach is based on templates constructed from principal components representing instructions identified from the power profiles of different instruction sequences. This technique can be used to predict the sequence of clock cycles per instruction (CCPI) in a known firmware and identify anomalies caused by modification of code on a tightly constrained embedded system. A submission is pending review at CHES 2016 based on this work.

## Experimental Setup

A custom board, comprising of a Spartan 6 FPGA and a Spartan 3E FPGA (DUA), was designed and fabricated to measure power consumption data during software execution. The Spartan 6 FPGA functioned as the control/communication device to convey debug and control data to the DUA. Current consumption of the device, was measured via a Tektronix DPO7354C oscilloscope, while post-processing was performed offline using MATLAB.






## Demonstration Observables

Demonstration will include generation of multi-clock cycle instruction template classification results. Test data captures will be analyzed for anomalies with reference to a known firmware utilizing the optimal sequence of CCPI technique. Anomalies demonstrated will include code insertions and re-arrangement of instructions within a known firmware. In conjunction with collecting data using oscilloscopes, we are currently working on data collection using on-board ADCs and should be able to present a functional system for the demonstration.

## References

Rao, S. K., Krishnankutty, D., Robucci, R., Banerjee, N., & Patel, C. (2015, May). Post-layout estimation of side-channel power supply signatures. In Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium on (pp. 92-95).