Detecting in-Silicon Hardware Trojans with Side Channel Analysis

Franco Mezzarapa, Joshua Joseph, Dr. Mike Borowczak, Phd
DRACO LAB | University of Central Florida
Dept. Of Electrical and Computer Engineering

DRACO

Abstract

This work presents a manufactured device that contains two sets of isolated hardware: one containing an encryption scheme and the other containing identical encryption logic alongside several hardware trojans. The objective is to expand upon prior research in hardware trojan detection by applying side-channel power analysis on a physical device during encryption operations. Utilizing similar Automated Machine Learning techniques, this work aims to validate prior simulation results in a hardware medium and detect the presence of key corruption alongside information leakage through power capture anomalies.

Motivation/Problem

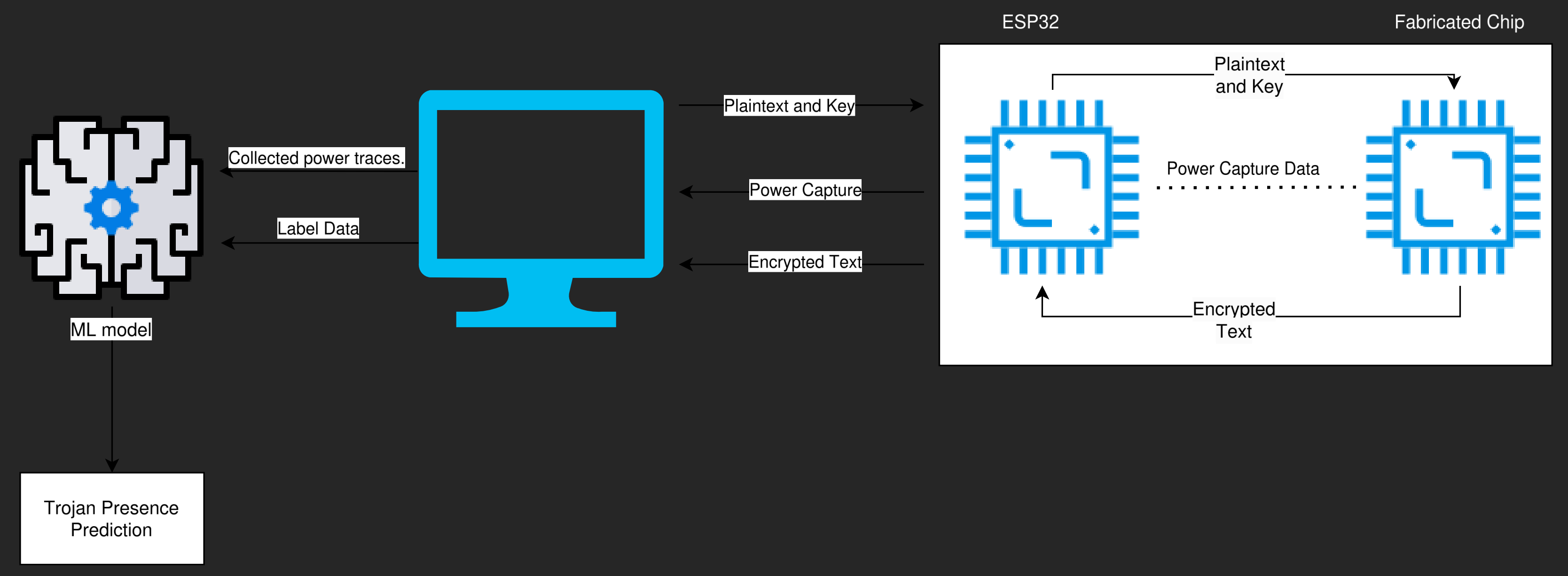
Offshore manufacturing and information-sensitive applications of integrated circuits (ICs) have resulted in a growing need for validation techniques to ensure hardware security. A Hardware Trojan (HT) is one of these threats as it is malicious logic that modifies the intended behavior of the circuit.

While verification of manufactured devices is thorough, additional safeguards are imperative to confidently identify units affected by errors in verification or sophisticated supply chain attacks.

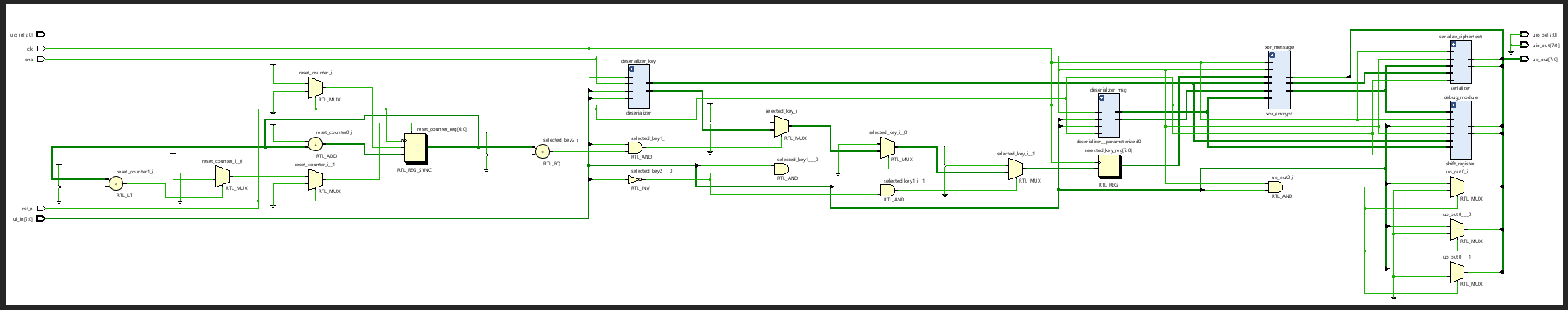
Side Channel Analysis (SCA) is a promising avenue that can be used to monitor signals by leveraging physical exposure to the device, allowing for the capture of power and information by probing exposed inputs/output pins. Previous work using SCA, specifically Differential Power Analysis, was successful in the collection of power traces to train machine learning models to distinguish between a firmware-implemented trojan in comparison to non-trojan activity on the Chip Whisperer's STM32- F030 MCU.

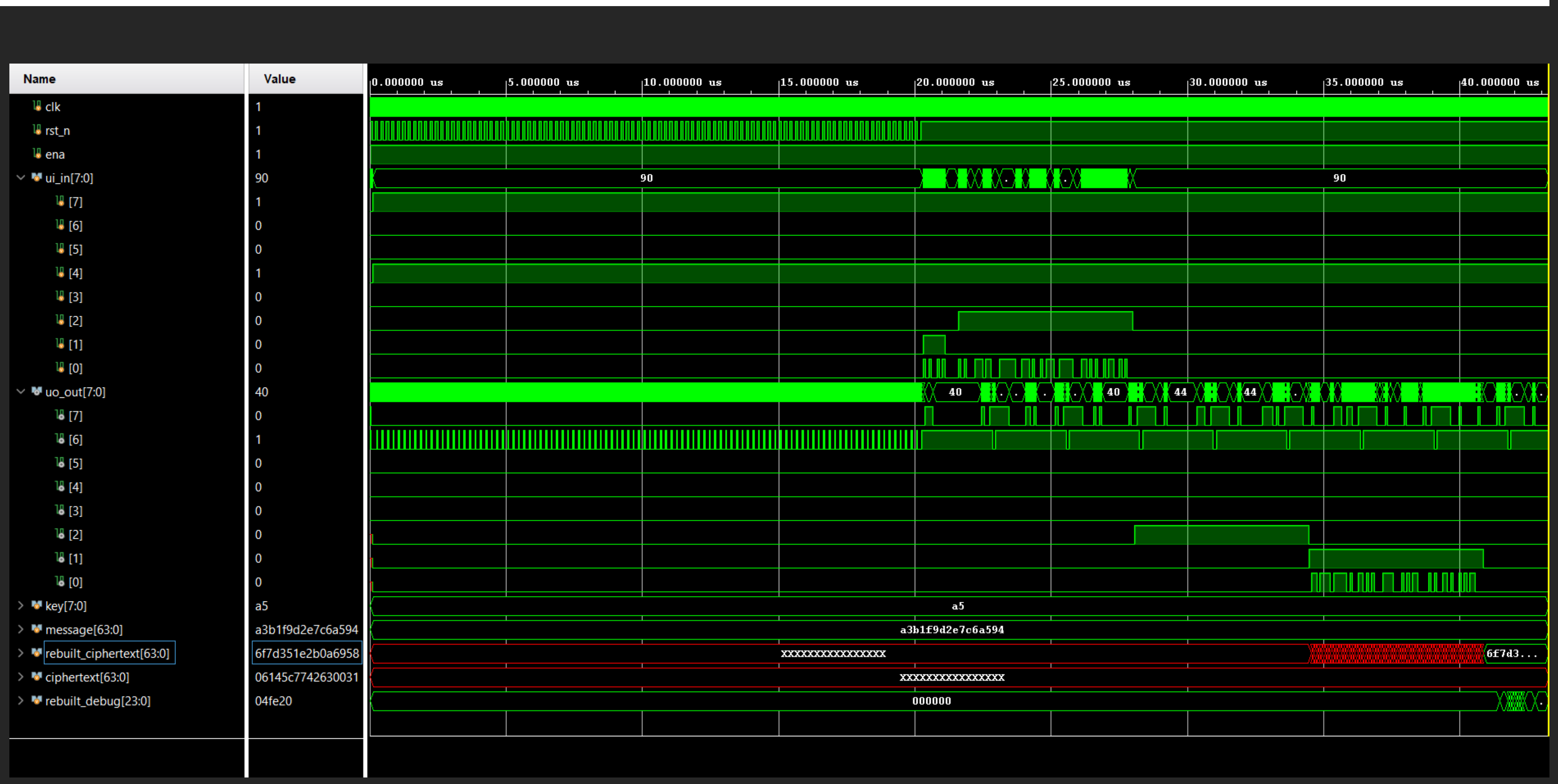
Hypothesis

Prior works indicate that side-channel differential power analysis is effective at detecting simulated hardware trojans on an embedded system microprocessor. When moving this design onto an ASIC, we hypothesize that the same principles continue to apply, allowing us to leverage the difference in power consumption between a non-compromised chip and a compromised chip.



Current Work & Results





Name	Value
clk	1
rst_n	1
ena	1
ui_in[7:0]	90
[7]	1
[6]	0
[5]	0
[4]	1
[3]	0
[2]	0
[1]	0
[0]	0
uo_out[7:0]	40
[7]	0
[6]	1
[5]	0
[4]	0
[3]	0
[2]	0
[1]	0
[0]	0
key[7:0]	a5
message[63:0]	a3b1f9d2e7c6a594
rebuilt_ciphertext[63:0]	6f7d351e2b0a6958
ciphertext[63:0]	06145c7742630031
rebuilt_debug[23:0]	04fe20

Future Work/Discussion

Derivations of this work can be applied in offensive and defensive security fields. Offensively, future work consists of improving upon the hardware trojans used in this experiment to determine if the side channel detection techniques used are still viable for more sophisticated attacks that reduce their footprint and evade verification. Defensively, the development of a system on chip utilizing edge artificial intelligence can be implemented to capture and monitor abnormalities in consumption to determine the presence of a hardware trojan.

Contact

Franco Mezzarapa
franco.mezzarapa@ucf.edu
Joshua Joseph
joshua.joseph@ucf.edu
DRACO LAB | www.ece.ucf.edu/DRACO
Dr. Mike Borowczak, Lab Director
Dept. Of Electrical & Computer Engineering
College of Engineering and Computer Science

Acknowledgements

This work is funded by the DRACO Lab at the University of Central Florida. A special thank you to both Alicia Thoney and Calvin VanWormer for the verification of the encryption module.