UC CINCINNATI

UNDERGRADUATES PURSUING RESEARCH IN SCIENCE AND ENGINEERING (UPRISE)

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
COLLEGE OF ENGINEERING AND APPLIED SCIENCE

SUMMER RESEARCH OPPORTUNITIES FOR UNDERGRADUATE students

APPLICATION DEADLINE: 02/01/2024

PROJECT TITLE: **<u>Deep Learning Side-Channel Attacks</u>**

Boyang Wang
Department of Electrical and Computer
Engineering
College of Engineering and Applied Science
Rhodes 806A
boyang.wang@uc.edu

Project Description

A side-channel attack can infer the secret key on a device (e.g., a microcontroller, a secure chip on a credit card, or an IoT device) by analyzing power consumption when the device runs encryption algorithms, such as Advanced Standard Encryption (AES). It is one of the primary threats to the security of embedded systems. While countermeasures (e.g., random delays, hiding, and masking) have been proposed to defend against traditional side-channel attacks, recent deep-learning-based side-channel attacks can defeat these existing countermeasures. Despite the promising results reported in recent studies, deep-learning-based side-channel attacks are not robust as they are sensitive to discrepancy between training data and test data. For instance, a deep neural network trained with data collected from one microcontroller (e.g., 8-bit XMEGA) may not derive high accuracy over data collected from another microcontroller (e.g., 8-bit XMEGA) due to minute changes in power measurements.

This project aims to enhance the robustness of deep-learning-based side channel attacks. The students in this project will have the opportunities to (1) Study research papers related to deep-learning-based side-channel attacks; (2) Explore new architectures of neural networks that can be more robust in side-channel attacks; (3) Examine different target devices, including microcontrollers and FPGAs; (3) Learn cybersecurity and machine learning knowledge and skills related to this project; (4) Have access to GPU machines in Dr. Wang’s lab for training neural networks; (5) Have access to data collection platform (Chipwhisperer) and corresponding microcontrollers in Dr. Wang’s lab to collect power and EM (electromagnetic) traces of AES encryption for analysis. This opportunity is open to students in Electrical Engineering, Computer Engineering, Computer Science, or Cybersecurity Engineering.