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

SUMMER RESEARCH OPPORTUNITIES FOR UNDERGRADUATE students

APPLICATION DEADLINE: April 27, 2025

PROJECT TITLE: Pre-Silicon Side Channel Analysis

Physical Requirement : No physical requirement
Project's Technical Skills Requirement : C, assembly, embedded systems (microcontrollers or FPGAs), Hardware Description Languages (Verilog or VHDL), RTL verification, or cybersecurity
Project's Available Positions : 1 or 2

Boyang Wang
Rhodes 806A
Cincinnati, OH, 45221
boyang.wang@uc.edu

Project Description

Side-channel analysis 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.

This project aims to investigate pre-silicon side-channel analysis over hardware design, e.g., RISC-V CPU, written in Hardware Description Languages (e.g., Verilog) to identify security vulnerability of software/hardware implementation of encryption algorithms. The students in this project will have the opportunities to (1) Study research papers related to side-channel analysis (including deep learning side-channel analysis); (2) Examine different hardware designs of encryption algorithms, such as AES, written in Verilog or VHDL; (3) Learn cybersecurity 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 and hardware in Dr. Wang’s lab to collect power traces of AES encryption for pre-silicon side-channel analysis. Undergraduate researchers who previously worked with Dr. Wang have received UC undergrad research fellowship awards and have published multiple research papers.