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

RESEARCH OPPORTUNITIES FOR UNDERGRADUATE students

APPLICATION DEADLINE: April 27, 2025

PROJECT TITLE: Hardware Design Security Analysis with Large Language Models

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

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

Project Description

Hardware design is complicated and often comes from untrusted third parties. To ensure the security and trust of the hardware design is critical. Traditional approaches often perform simulations to detect vulnerable code in Hardware Description Languages (Verilog or VHDL), which is time-consuming for the verification team.

This project aims to utilize Large Language Models to automatically detect HDL code that is vulnerable to known hardware CWEs (Common Weakness Enumerations). The students in this project will have the opportunities to (1) Study research papers related to Large Language Models and hardware CWEs; (2) Examine different hardware designs 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 Large Language Models; (5) Build robust datasets for this type of automatic detection. Undergraduate researchers who previously worked with Dr. Wang have received UC undergrad research fellowship awards and have published multiple research papers.