DEPARTMENT OF
COMPUTER SCIENCE
TEXAS TECH
Whitacre College of Engineering

Constructing Secure Hardware Datasets to Support the Application of Large Language Models in Hardware Domain

Xiaolong Guo, Ph.D.
Kansas State University

Tuesday, November 26, 2024
3:30 p.m.
Zoom: https://texastech.zoom.us/j/99975231209?pwd=D2asbJrgAS71Zzf8uvHNkn2o4P1iRJ.1
Meeting ID: 999 7523 1209
Passcode: 566306

Abstract: The application of Large Language Models (LLMs) in hardware security represents a transformative step towards addressing challenges in hardware design and verification. This presentation explores various advancements, including the development of domain-specific LLMs like Hardware Phi-1.5B, tailored for semiconductor applications, and LLM4SecHW, fine-tuned for hardware debugging using curated datasets derived from version control systems. Addressing data scarcity and quality issues, a novel semi-synthetic data generation method leverages journalistic principles to enhance hardware debugging datasets. Additionally, this presentation investigates resilience against power side-channel attacks, proposing reinforcement learning (RL)-based solutions to secure hardware designs. To optimize Power, Performance, and Area (PPA) metrics, an LLM-based RL framework, PPA-RTL, integrates post-synthesis metrics into design generation. Finally, Dr. Guo will introduce an automated assertion generation framework that combines formal verification, hardware security knowledge, and version control data to create comprehensive security assertion datasets. These contributions highlight the potential of LLMs to enhance automation, resilience, and efficiency in hardware security and semiconductor design.

Bio: Dr. Xiaolong Guo is an Assistant Professor in the Department of Electrical and Computer Engineering at Kansas State University (K-State). He earned his Ph.D. in Electrical and Computer Engineering from the University of Florida in 2019. His research focuses on large language models, formal verification, and hardware security. Dr. Guo has received several accolades, including Best Paper Awards at DATE 2019 and AsianHost 2020, and a Best Paper Nomination at ASP-DAC 2021. He was honored with the Outstanding Assistant Professor Award from the Carl R. Ice College of Engineering at K-State, as well as the First Award and REI Award from Kansas NSF EPSCoR. Most recently, he is the recipient of the 2024 NSF CAREER Award.