Electrical & Computer Engineering

S E M I N A R

Louisiana State University

Advancing IoT Hardware Security and Data Augmentation Technique using MAGAN

Frederic Rizk

University of Louisiana at Lafayette

Abstract—This research talk delves into two significant advancements in hardware security and machine learning. Firstly, we explore the hardware security for Internet of Things (IoT) devices, presenting a novel Cost-Efficient Reliable Reconfigurable Ring Oscillator Physical Unclonable Function (CERRO PUF). CERRO PUF proves to be a promising solution, significantly reducing design overhead and power consumption while maintaining high efficiency and security. Through detailed analysis, we demonstrate its superiority over existing designs, showcasing improved challenge-response pair generation and heightened resistance against machine learning attacks.

In the second part of the talk, we shift our focus to data augmentation, a crucial strategy in overcoming the scarcity of training data for machine learning models. Generative Adversarial Networks (GANs) have emerged as powerful tools for data augmentation, producing realistic and diverse synthetic data. Our study introduces a two-player game approach to GAN training, iteratively refining the generator to create increasingly authentic samples. Furthermore, we present MAGAN, a Meta-Analysis method for GANs' latent space, shedding light on its influence on the generated image space. Quantitative results from MAGAN demonstrate its accuracy in tracing latent space changes, affirming the potential of GANs as parameterized data generators for data-driven augmentation, addressing the challenge of limited labeled datasets during model training.

When: **Friday, 1 March 2024, 13:30 - 14:30**
Where: **Room 3316E Patrick F. Taylor Hall**
Info: `https://www.lsu.edu/eng/ece/seminar`
Food: ***Brownies, Sandwiches, Drinks will be served.***