SEMINAR ANNOUNCEMENT

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
Faculty of Engineering
Website: https://www.eng.nus.edu.sg/ece/

Area: Communications & Networks

Host: Assoc Prof Bharadwaj Veeravalli

TOPIC	:	**Depth-Optimized, ReLu-Activated Fully Homomorphic Encrypted Neural Networks**
SPEAKER	:	**Mr Souhail Meftah** **Graduate Student, ECE Dept, NUS**
DATE	:	**Monday, 29 March 2021**
TIME	:	**10.00AM to 11.00AM**
WEBINAR	:	**Join Zoom Meeting** **https://nus-sg.zoom.us/j/88423701986?pwd=UUQ3djl1RExEQlpydEdBTmhZdCs1dz09** **Meeting ID: 884 2370 1986** **Password: 980931**

ABSTRACT

Fully homomorphic encryption (FHE) is a powerful cryptographic primitive to secure outsourced computations against an untrusted third-party provider. With the growing demand for AI and the usefulness of machine learning as a service (MLaaS), the need for secure training and inference of artificial neural networks is rising. However, the computational complexity of existing FHE schemes has been a strong deterrent to this. Prior works suffered from accuracy degradation, lack of scalability, and ciphertext expansion issues. Hence, we take the first step towards the problem of space-efficiency in evaluating deep neural networks through designing DOReN: a low depth, without approximations, batched neuron that can simultaneously evaluate multiple ReLU-activated neurons on encrypted data.

BIOGRAPHY

Mr. Souhail Meftah received his BS.Sc degree in Computer Science from Al Akhwayn University in 2016, he later received his MS.Sc in Information Systems Security from that same university. He served as an R&D research consultant in Leyton UK for a year before joining NUS as a PhD student in Electrical and Computer Engineering. His research interests include Applied Cryptography, AI, Cloud Security, and Intrusion Detection.