

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	:	Practical Inference on Encrypted Medium Resolution Images
SPEAKER	:	Mr Souhail Meftah Graduate Student, ECE Dept, NUS
DATE	:	Monday, 20 September 2021
TIME	:	10.00AM to 11.00AM
WEBINAR	:	Join Zoom Meeting https://nus-sg.zoom.us/j/89000572860?pwd=bHJ3U1MrMmxvZnJla1pUeWRFWWxwdz09 Meeting ID: 890 0057 2860 Password: 659075

ABSTRACT

Fully homomorphic encryption (FHE) is a powerful tool enabling secure outsourcing to untrusted third-parties. As AI technologies mature and companies start offering AI-as-a-service (AlaaS), the privacy of their customers' data needs to be considered but the high overhead of existing FHE schemes is a major limitation. Prior works tried to address this but suffered accuracy degradation, lack of scalability, ciphertext expansion, and impractical performance issues. In this talk, we explore the utility of High-Performance Computing systems for accelerating the secure evaluation of deep convolutional neural networks (CNN) with FHE. We examine previous encrypted neural network architectures and propose a holistic re-design for the HPC environment, which introduces a new consideration for the latency of inter-node communication. The new architecture was implemented with MPI and OpenMP and its performance benchmarked against state-of-the-art FHE-based CNN evaluation methods. We achieved improvements of between 6 to 34 folds for various CIFAR10 CNN architectures and more than 1500 times folds for AlexNet, bringing FHE-based evaluation of AlexNet down from several hundred days to within 14 hours. We believe that practical inference on encrypted medium resolution images is around the corner with the use of HPC systems.

BIOGRAPHY

Mr. Souhail Meftah received his BSc degree in Computer Science from Al Akhwayn University in 2016, he later received his MSc 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.

<https://www.eng.nus.edu.sg/ece/highlights/events/>