SEMINAR ANNOUNCEMENT

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
COLLEGE OF DESIGN AND ENGINEERING
Website: https://cde.nus.edu.sg/ece

Area: Communication and Networks (CN)

Host: Prof Biplab Sikdar

TOPIC	:	**Structure-Conditioned Membership Leakage in Quantum Neural Networks**
SPEAKER	:	**Mr Najeeb Ullah** **Graduate Student, ECE Dept, NUS**
DATE	:	**Thursday, 26 November 2026**
TIME	:	**10:00AM-11:00AM**
VENUE	:	**E4-05-39 ECE Conference Room**

ABSTRACT

Membership inference attacks use a model's predictions to determine whether a specific record was part of its training set. Although these attacks and their defenses have been widely studied in classical machine learning, less is known about how quantum neural network (QNN) design shapes this risk. In a QNN, a feature-map encoder prepares each input as a quantum state, a trainable circuit transforms that state, and measurements yield the outputs used for prediction. Even when fixed, the encoder determines the representation from which the variational circuit learns. We investigate whether altering that representation changes how easily an attacker can identify training records when the number of trainable parameters remains constant. Across four image and tabular datasets, increasing encoder repetition from one to five raised attack AUC in all 16 dataset–attack comparisons, and this effect persisted under noisy simulation. Greater repetition altered the geometry of the encoded states before training, while models with larger train–test accuracy gaps tended to exhibit higher leakage afterward. We further evaluate whether existing defenses can narrow this encoder-associated leakage gap. Among four defenses tested on Fashion-MNIST, differentially private training reduced the high-risk, five-repetition model's attack AUC by 0.186 under our primary attack, yet a repetition-associated gap of 0.043 remained. These findings show that QNN privacy audits should assess both how much a defense reduces leakage for a given model and how much leakage still varies across encoder choices. They also motivate the development of defenses that account for encoder design to better protect training data while preserving predictive performance.

BIOGRAPHY

Mr Najeeb Ullah is a PhD candidate in Electrical and Computer Engineering at the National University of Singapore, supervised by Prof. Biplab Sikdar. His research focuses on membership inference attacks and privacy defenses in classical and quantum machine learning. He received his bachelor's and master's degrees in computer science from the National University of Computer and Emerging Sciences (FAST-NUCES) in Peshawar, Pakistan.