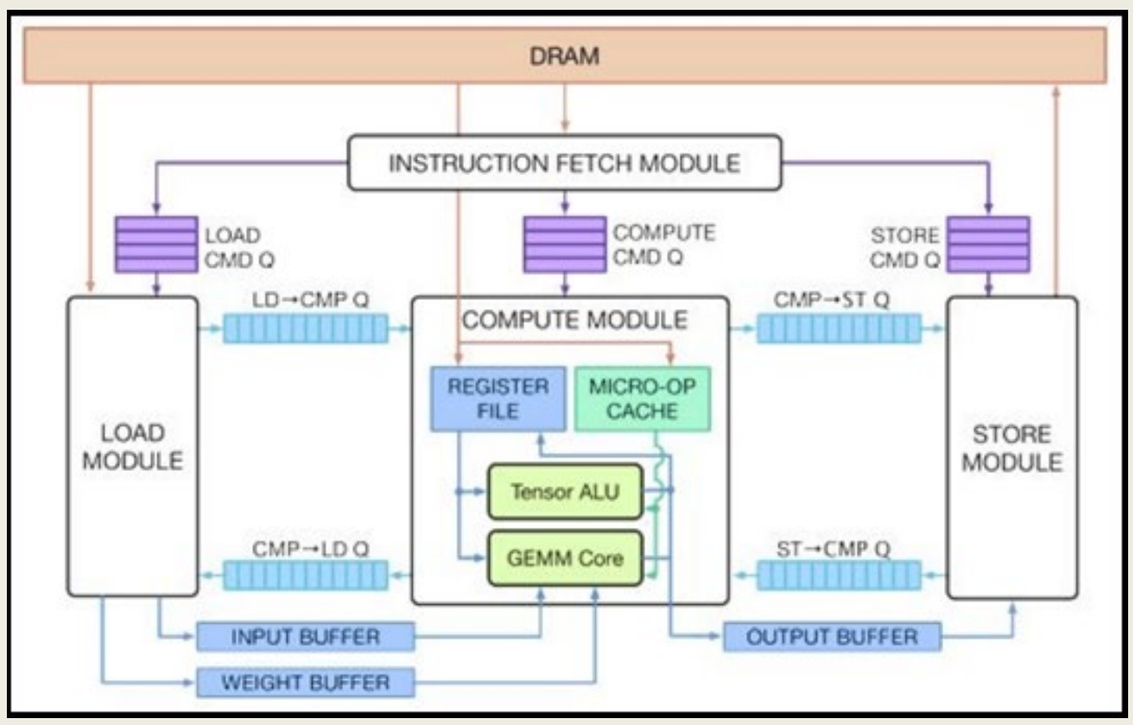
NANYANG TECHNOLOGICAL UNIVERSITY
SINGAPORE

School of Computer Science and Engineering
College of Engineering

Reverse Engineering Deep Learning Algorithms

Student: Muhammad Irfan Bin Norizzam **Supervisor: Assoc Prof Lam Siew Kei**



Project Objectives:

As the demand for edge computing grows, Deep Neural Networks (DNNs) are increasingly deployed on edge devices to enable real-time processing and decision-making. There is a need to address cybersecurity concerns in edge FPGA accelerators hosting DNNs due to vulnerability to side-channel reverse engineering attacks (SCAs). Proposed defense mechanisms in this project build upon prior research, aims to thwart the attackers attempts to leverage information leakage via SCAs to prevent the theft of proprietary information.

Scheduling Measures: Variability in the computation order is introduced while minimizing changes to the underlying mathematical logic.

Dummy Layer Obfuscator: Dummy convolutional layers are inserted into the DNN architecture to obscure its structure.

Technologies used

PyTorch

tvm