Side-Channel Attacks against Memristor Computing Systems and Countermeasures

In this project, we reveal the vulnerability of memristor computing systems by developing novel side-channel attacks to reverse engineer the NN structures of the NN models. To mitigate the vulnerability, we also propose efficient countermeasures. Both the attacks and countermeasures will be experimented on simulation models or physical platforms.

Background:

Memristor computing systems have demonstrated great potential in improving the energy efficiency of neural network (NN) algorithms. The NN weights are stored in the memristor crossbars of memristor computing systems. However, the memristor computing systems may face side-channel attacks. Specifically, during the NN inference, the memristor crossbars consume considerable power. The power profile could hint the insightful information about the NN structures, including each NN layer's dimension. The structure of a NN model primarily determines its perception performance. Thus, exploiting the side-channel attacks to extract the NN structures from memristor computing systems could be a severe problem, which has not yet been touched or addressed.

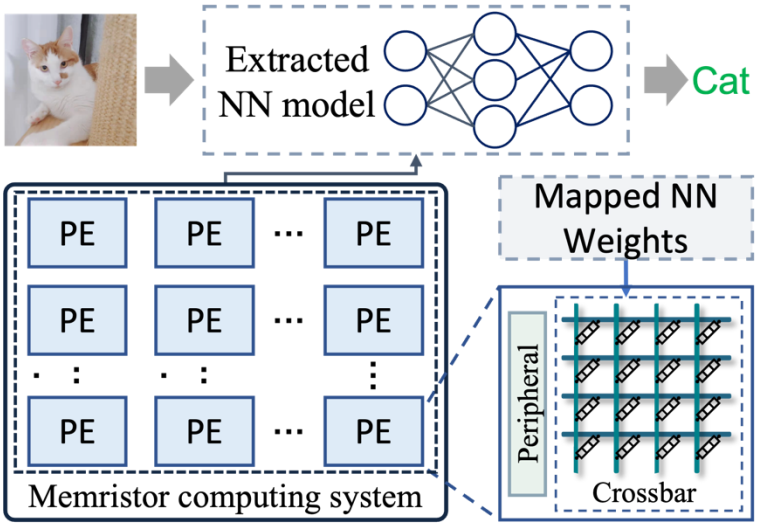

Figure: The basic structure of memristor computing systems and extraction threat through side-channel attacks

Prerequisites:

- **Courses:** Circuits and Architectures with Memristors or Introduction to VLSI
- **Skill:** programing, hack-style thinking

For more information: Minhui Zou minhui@campus.technion.ac.il