PhD Thesis Title: Investigation of Security Vulnerabilities in Emerging Compute Architectures

Abstract:

Emerging non-volatile memory (NVM) technologies such as Ferroelectric RAM (FRAM) are revolutionizing energy-efficient edge and neuromorphic computing systems. However, their susceptibility to hardware-level security threats, including side-channel and fault-injection attacks, poses significant challenges. This thesis experimentally investigates electromagnetic (EM)-based side-channel and fault-injection vulnerabilities across a range of next-generation compute paradigms all the way from commercial FRAM memories to TinyML (Tiny Machine Learning) accelerators and neuromorphic spiking networks—thereby presenting a comprehensive security analysis framework for NVM-based intelligent hardware.

In the first part of this thesis, commercial FRAM devices are analyzed as black-box systems to evaluate their susceptibility to electromagnetic side-channel attack (EM-SCA) and EM fault injection (EMFI) attacks. The study demonstrates that memory operations such as read/write can be distinguished and manipulated through EM emanation analysis, revealing exploitable information leakage and controlled data corruption pathways. Building on this foundation, the second part of the thesis explores vulnerabilities in persistent TinyML hardware. Through localized EM-SCA, critical model parameters such as neural network weights are statistically extracted, enabling the model cloning of some TinyML models with as little as 0.5% of the training dataset for some cases.

Extending this threat model, the third part experimentally investigates EMFI-induced corruption of neural network weights during model loading in NVM-based TinyML or lightweight neural network systems, showing that EM perturbations at specific chip regions can degrade inference accuracy by up to 40%, particularly in lightweight architectures like ResNet and MobileNet. The final part focuses on neuromorphic spiking neural networks (SNNs) realized on Field Programmable Gate Array (FPGA) platforms. By applying differential power analysis (DPA), the study successfully decodes internal network activity, such as the number of active neurons, and demonstrates the potential for denial-of-service (DoS) attacks in battery-powered neuromorphic systems.

Collectively, the research establishes the first holistic experimental framework for analyzing and benchmarking side-channel and fault-injection vulnerabilities in NVM-based computing systems—from memory and TinyML accelerators to spiking neuromorphic platforms—bridging the gap between device-level physics and system-level security. The insights derived from this thesis will aid in designing robust countermeasures for future low-power, intelligent, and secure edge hardware.
