Opportunities and Challenges for Resistive Random Access Memory Devices in Hardware Security and Trust

Rashmi Jha, University of Cincinnati

https://eecs.ceas.uc.edu/MIND

Supported by NSF Award # CNS 1556301

- Emerging non-volatile memory devices, such as Resistive Random Access Memory (RRAM) devices, Spin Torque Transfer RAM (STTRAM) devices, and Phase Change Memory (PCM) devices have caught significant research attention for on-chip embedded memory, storage class memory, and in-memory computing.
- From hardware security perspective, these devices have been investigated for applications as Physically Unclonable Functions (PUFs), programmable vias and switch boxes in split manufacturing.

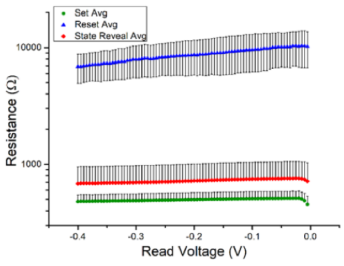
The ***major challenge*** this project aims to address pertains to accomplishing low-power data-encryption and data-storage in power-constrained systems such as Internet of Things (IoTs).

- Conventional techniques of keys-based data encryption are power consuming and compute resource intensive making them unsuitable for data encryption and storage in power constrained devices.
- Cryptographic keys can be leaked via side-channel attacks that an attacker can use to reveal the stored data.

The project aims to have ***significant scientific impacts*** by providing the following solutions:

- Fast and low-power integrated data-encryption and storage in embedded systems.
- Tamper-resistant self-encrypted memory devices that can also be used for in-memory computing applications, such as neuromorphic computing.
- High-density self-encrypted non-volatile memory devices that can be used to store keys for achieving IC design obfuscations in ASICs, and FPGAs.

The ***central approach*** will be to capitalize on the switching physics in RRAM devices and tailor the filament geometry such that the stored data will be encrypted into the filament geometry and history of the device. Our approach is based on recent results obtained using our NSF SaTC funded project.



Broader Impact on Society:

- The stealing and hacking of data, crypto-keys, and IC designs impose major threat to our society. The proposed project will provide solutions for data encryption and storage in tamper-resistant memory at ultra-low power which will have *transformative impact*.

Broader Impacts on Education and Training:

- Project will train undergraduate and graduate students in the area of crypto memory, emerging non-volatile memory, and IC design for trust with self-encrypted memory.

Broader Impacts Quantifications:

- Demonstration of prototype with self-encrypted memory.
- Establishing collaboration with microelectronics industry and government lab for technology translation.