Hardware Security

Chongxi Bao, Yang Xie, Abhishek Chakraborty, Ankit Mondal, Yuntao Liu
Prof. Ankur Srivastava

Hardware Trojan Detection

May be inserted at:
- Design-Time
- Fab-Time
- Test-Time

Foundry-inserted Trojans

RE-based Trojan Detection Flow

Reverse-engineering (RE)

SVM Classifier

Final Step

- Detect three kinds
- Accuracy > 99.6%
- False positive <1%

Hardware IP Protection

1. IC supply chain attack

2. 2.5D Split Fabrication

- 2.5D Split fabrication: The interposer layer can be fabricated separately in a trusted foundry
- Security-aware Design Flow
- Secure partitioning: function obfuscation
- Secure Placement: layout obfuscation

3. Logic Locking

Side-channel Attack on Emerging Technology

1. Magnetic Tunnel Junction

2. MTJ Switching Characteristics

Spin polarized current can switch states through spin-torque transfer (STT)

3. Proposed Power Model

(a) Vertical alignment of power traces
(b) Net variation in power of an MRAM cell:

4. Correlation Power Analysis Attack

LP Based Attack on Physical Unclonable Functions

Target PUFs

The Arbiter PUF

Memristor Crossbar PUF

The response is

\[ f = \begin{cases} 1 & \text{if } \phi \cdot \hat{D} > 0 \\ 0 & \text{otherwise} \end{cases} \]

subject to

\[ -r \sum_j d_j \leq d_{\text{th}} \leq r \sum_j d_j \]

for \( j = 1, \ldots, n + 1 \)

This work was supported by NSF under Grant No. 1223233
and AFOSR under Grant FA9550-14-1-0351.