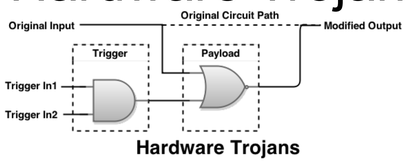
Hardware Security

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

UNIVERSITY OF MARYLAND 18 56
INSTITUTE FOR SYSTEMS RESEARCH
A. JAMES CLARK SCHOOL OF ENGINEERING

Hardware Trojan Detection



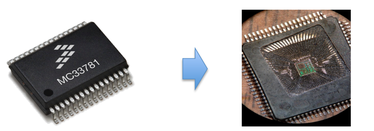
Hardware Trojans

May be inserted at:

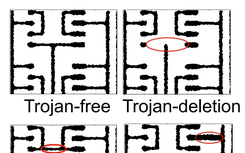
- Design-Time
- Fab-Time
- Test-Time

Foundry-inserted Trojans

Reverse-engineering (RE)

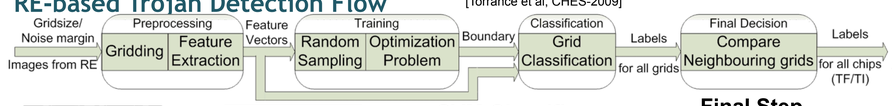


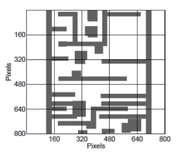
[Torrance et al, CHES-2009]

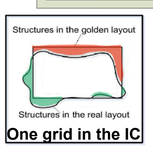


Trojan-free Trojan-deletion Trojan-addition Parametric

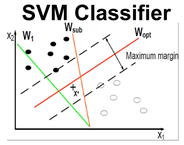
RE-based Trojan Detection Flow



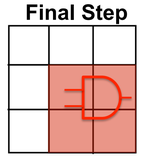




SVM Classifier



Final Step

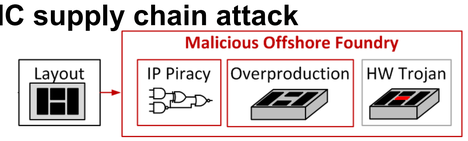


Results

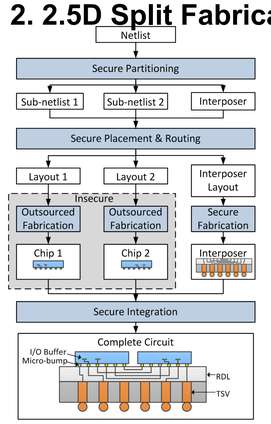
- Detect three kinds
- Accuracy > 99.6%
- False positive <1%

Hardware IP Protection

1.IC supply chain attack

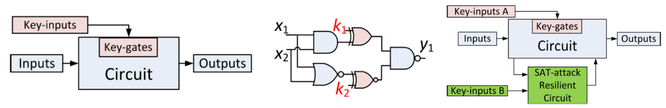


2. 2.5D Split Fabrication



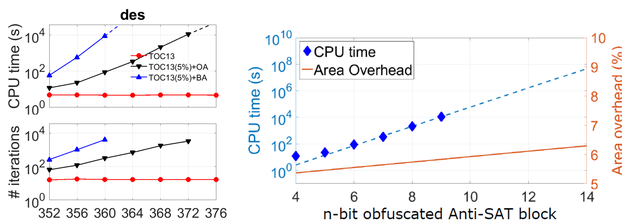
- **2.5D Split fabrication:** The interposer layer can be fabricated separately in a trusted foundry
- **Security-aware Design Flow**
- **Secure partitioning:** function obfuscation
- **Secure Placement:** layout obfuscation

3. Logic Locking



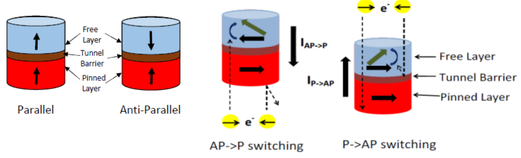
Anti-SAT block: the number of SAT attack iteration λ is an exponential function of key-size k

$$\lambda \geq \lambda_l = \frac{2^{2n}-2^n}{p(2^n-p)} \approx \frac{2^{2n}-2^n}{1\times(2^n-1)} \approx 2^n$$



Side-channel Attack on Emerging Technology

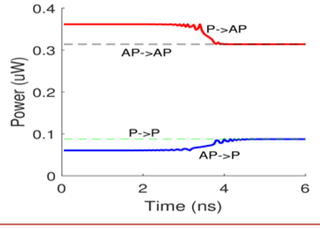
1. Magnetic Tunnel Junction



2. MTJ Switching Characteristics

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

Power profiles due to AP to P & P to AP are different !



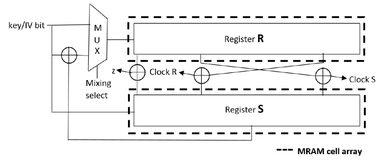
3. Proposed Power Model

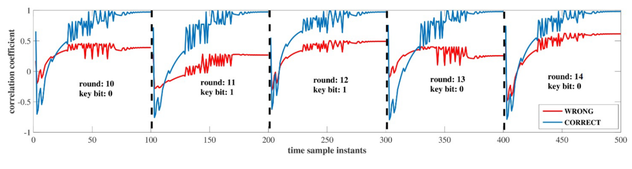
(a) Vertical alignment of power traces

(b) Net variation in power of an MRAM cell:

$$\Delta P_{total}^{align} \propto at_{10} - bt_{01}$$

4. Correlation Power Analysis Attack

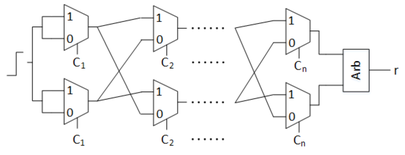




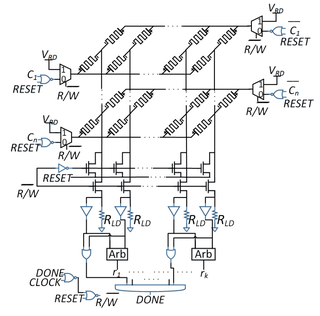
LP Based Attack on Physical Unclonable Functions

Target PUFs

The Arbiter PUF



Memristor Crossbar PUF

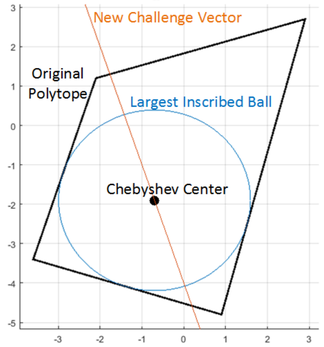


The response is

$$r = \begin{cases} 1 \text{ if } \vec{\Phi}^T \cdot \vec{D} > 0 \\ 0 \quad \text{otherwise} \end{cases}$$

$\vec{\Phi}$: the *feature vector,*

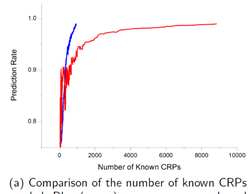
$\vec{D}$: the *weight vector.*



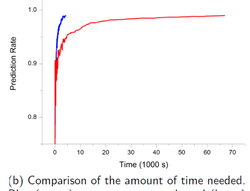
$$\max_{\hat{D},\rho} \rho$$

$$\text{subject to} \quad -r_j \hat{\Phi}_j^T (\hat{D} + \rho \frac{\hat{\Phi}_j}{\| \hat{\Phi}_j \|}) \leq 0$$

$$d_{lb,j} \leq \hat{d}_j \leq d_{ub,j} \quad \text{for} \quad j = 1, 2, \ldots, n+1$$



(a) Comparison of the number of known CRPs needed. Blue (upper) curve: our approach; red (lower) curve: ML approach.



(b) Comparison of the amount of time needed. Blue (upper) curve: our approach; red (lower) curve: ML approach.

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

IDEAlab INTELLIGENT DEPENDABLE EFFICIENT & ADAPTABLE electronic systems lab