MPA: Model-assisted PCB Attestation via Board-level RO and Temperature Compensation

Zimu Guo, Xiaolin Xu, Mark M. Tehranipoor and **Domenic Forte**
Electrical and Computer Engineering, University of Florida
Email: zimuguo@ufl.edu; {xiaolinxu,tehranipoor,dforte}@ece.ufl.edu

Motivation

Consumer electronics

IoT devices

Military applications

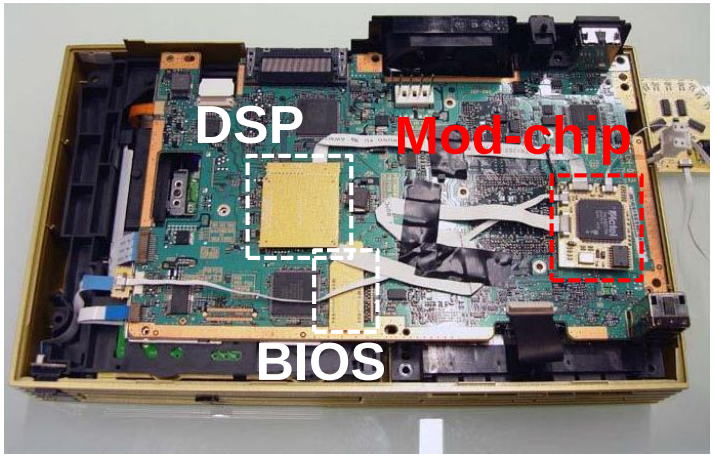
PCB security issues

- In-field Alternation
  - Test/Debug Interface/ Peripheral Exploitation
  - Re-routing internal paths
  - Add/replace components
- Rev. Eng./ Recycling
  - Recycling
  - Cloning/Counterfeiting

Mod-chip

Real-life Examples

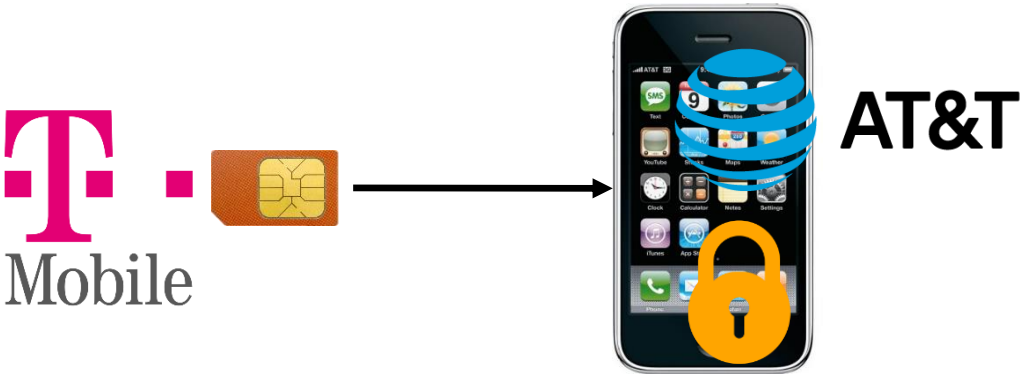
- Xbox 360 copyright bypass via **mod-chip**.



Run **third-party** operating system and run **application without purchasing**

Hundreds of online vendors
Thousand of device sold

- iPhone hacking: crack the carrier restrictions.

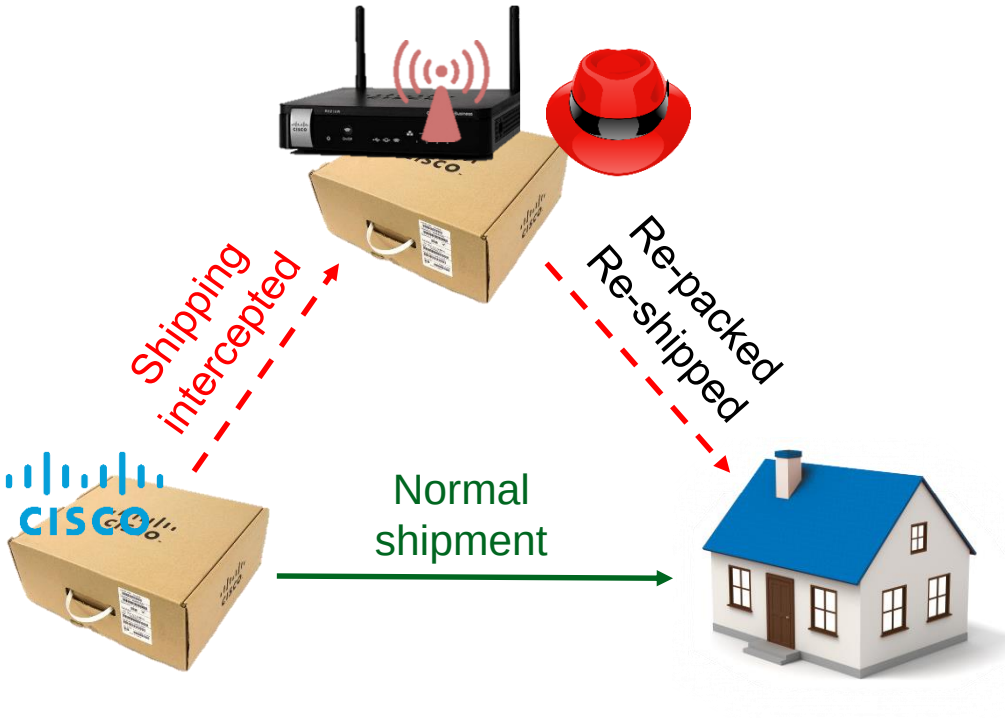


Motivation – Cisco Router "Upgrade"

"Attacker": National Security Agency (NSA) employees

Target: Cisco servers, routers, and other network devices

Activity: install beacon firmware with a "load station"



Current Solutions and Limitations

System-level tamper protection framework (*TI*)

Opening switch

Tamper mesh from the IBM 4758 cryptoprocessor

Vibration sensor

Temperature sensor

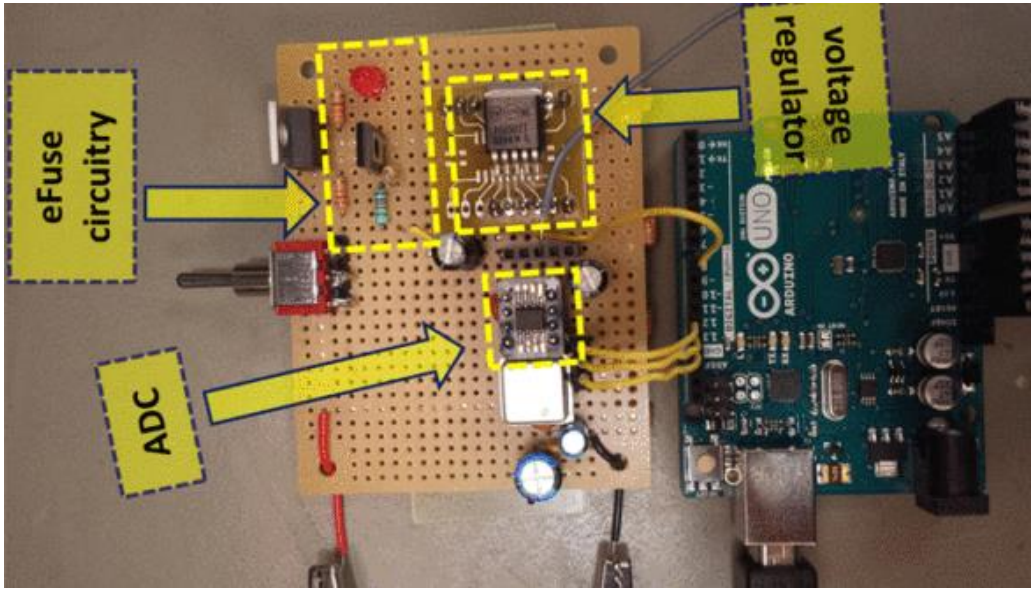
Limitations:

- Sensors can be removed.
- Should be handled carefully.
- Expensive for the system level.

Current Solutions and Limitations

Circuit path resistance monitoring (*S. Bhunia et al, 2016*)

Requires high resolution analog-to-digital converter (**ADC**) and **constant current source.**



Not always applicable!

Objective – Desired Properties

Universality

- Applicable for most PCB designs
- Compatible with existing design/fabrication steps

Low cost

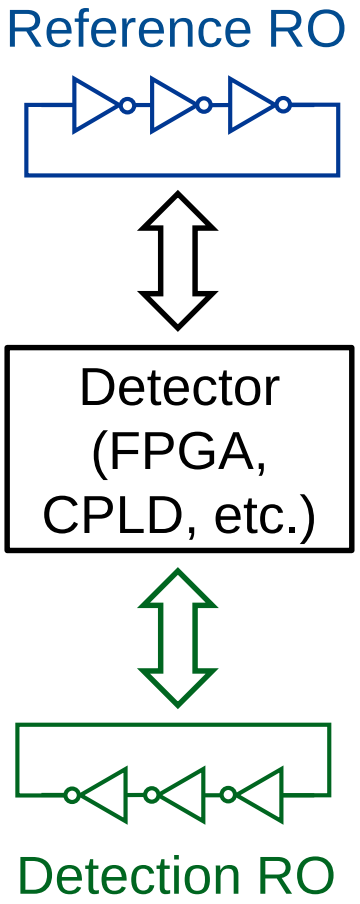
- Minimal additional components
- Simple to implement / Low design effort

Robustness

- Difficult to deactivate
- Accurate in presence of environmental noise

Framework Overview

MPA: **M**odel-assisted **P**CB **A**ttestation



- Refer temperature by the RO frequency.

- Collects the frequencies of the ROs.
- Compute the boundaries based on the **model**.
- Makes tampering decision.

- Covers the board-level critical paths.
- Monitors the impedance changes.

Model Enrollment

Why model enrollment?

- Both the detection and reference ROs are *sensitive to temperature variations.*

Model expression:

$$f_{det} = G(f_{ref})$$

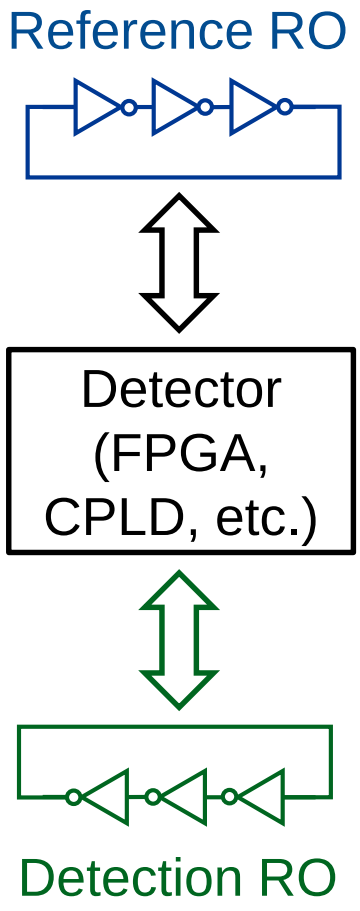
Frequency of each detection RO

Frequency of each reference RO

Collect multiple (f_{det}, f_{ref}) pairs and apply polynomial fitting.

$$G(x) = p_3x^3 + p_2x^2 + p_1x + p_0$$

$$\sigma_{max} = std(f_{det})$$



In-field Detection

- Generate decision boundaries during the **testing mode**.

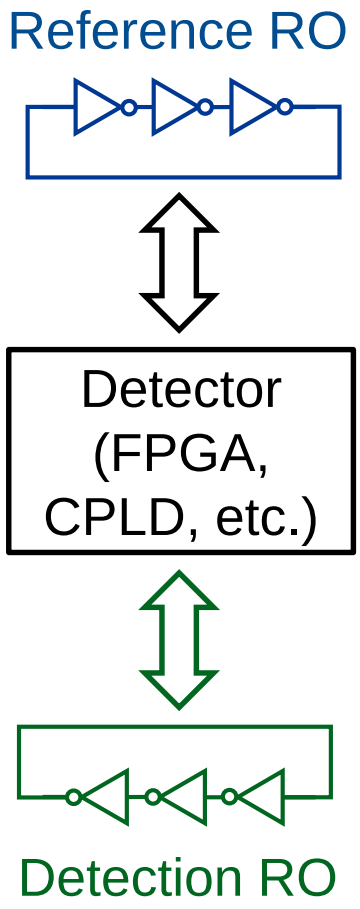
Lower boundary $b_{lo} = G(f_{ref}) - 3 \times \sigma_{max}$

Upper boundary $b_{up} = G(f_{ref}) + 3 \times \sigma_{max}$

- Compare the detection RO frequency with the boundaries.

$f_{det} \in [b_{lo}, b_{up}]$ ⟶ System safe!

$f_{det} \notin [b_{lo}, b_{up}]$ ⟶ System tampered!



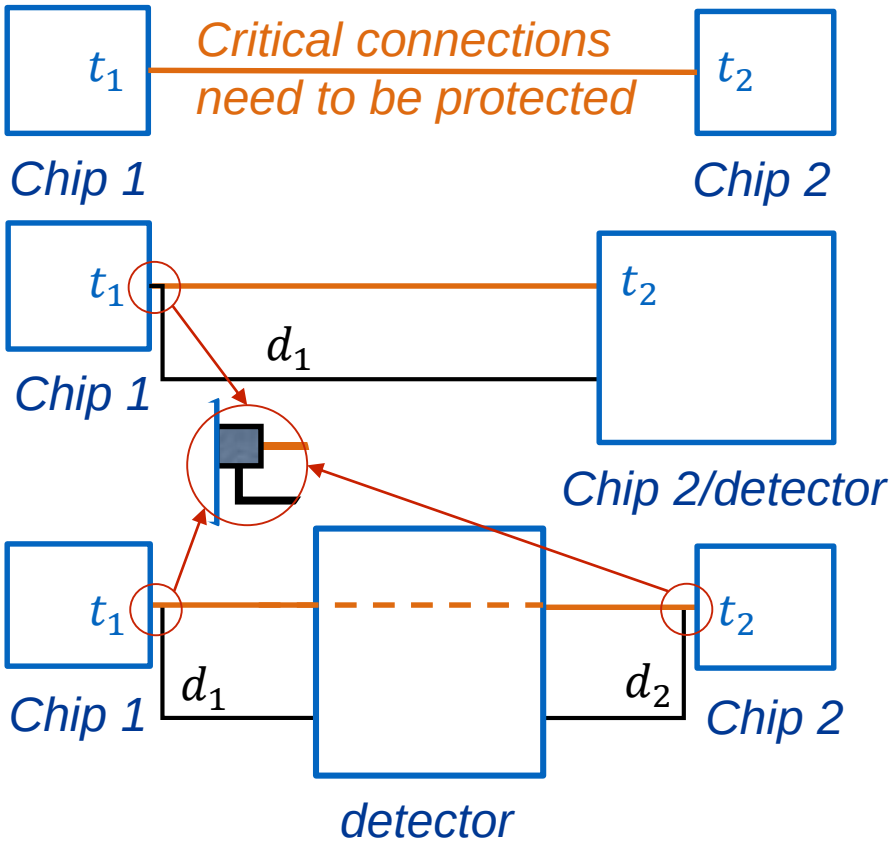
MPA Implementation

Design Modification Scenarios

Original design

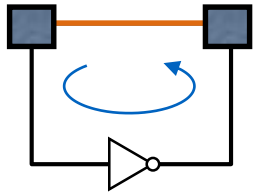
Embedded mode detector scenario
E mode

Standalone mode detector scenario
S mode



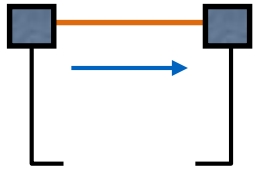
JTAG in HIGHZ mode

Testing mode



JTAG Disabled

Normal mode



MPA Implementation: Detector Design

Inverter bank

- Achieve reference and detection ROs
- Configured by the controller

Controller

- Central controller and processor of the detector
- Configures the counter and inverter bank

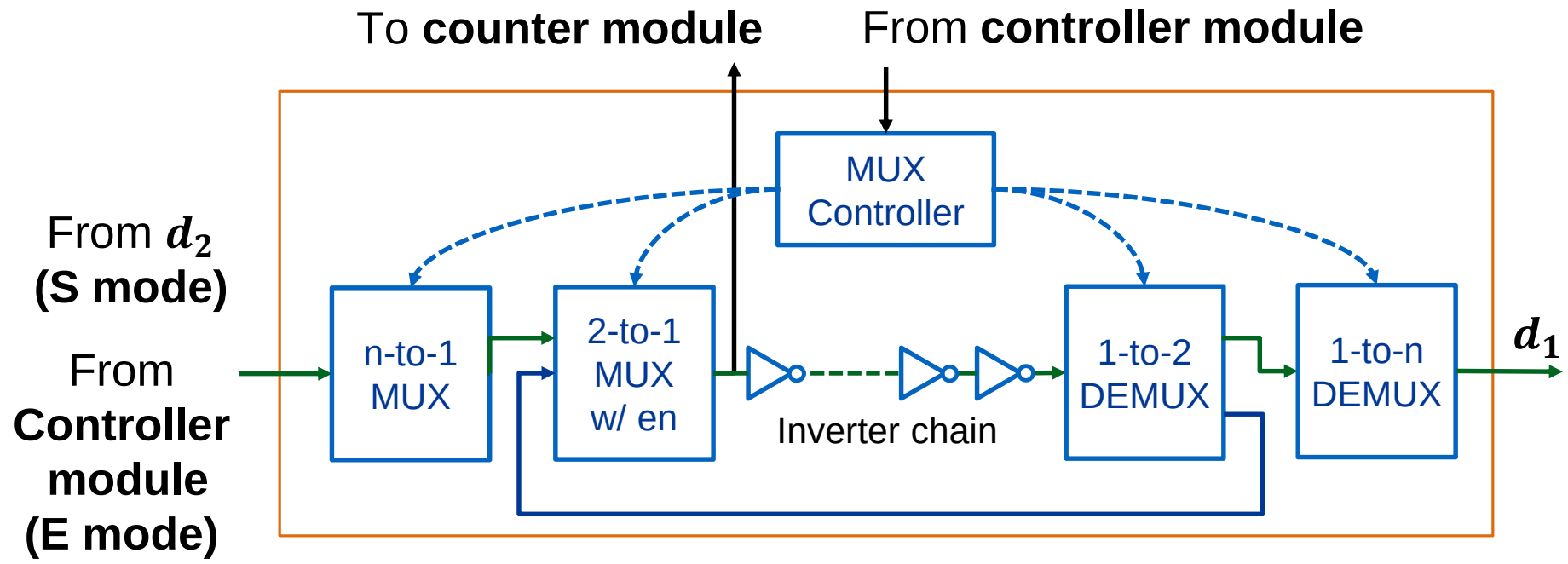
Counter

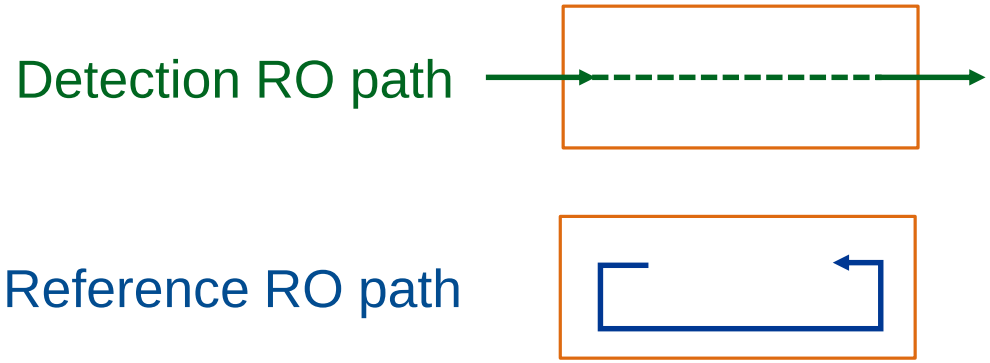
- RO frequencies measurements
- Controller defines time instants

Permutation Network

- Only in S-mode detector
- Key controlled permutation
- Tampering response

MPA Implementation: Inverter Bank





The inverter bank composes part of the RO

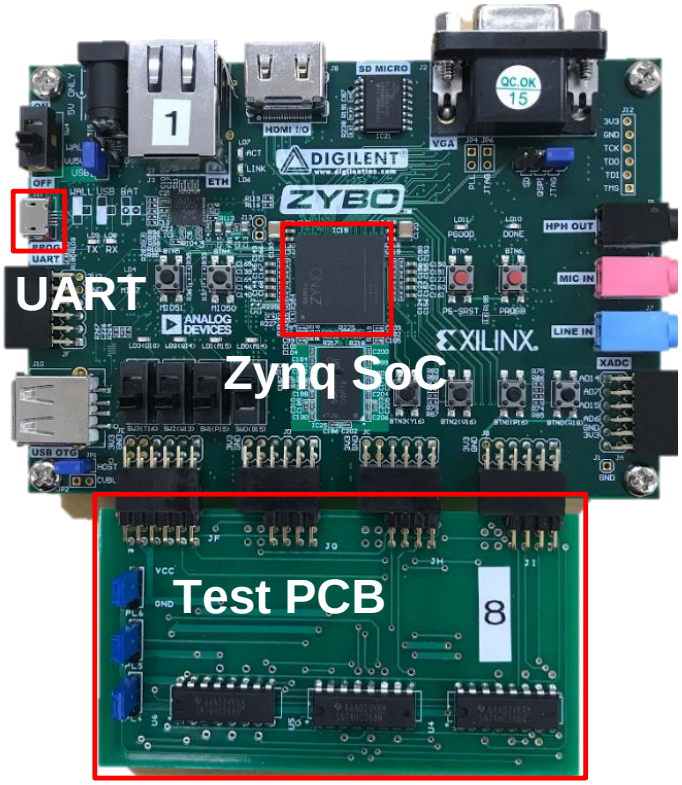
The inverter bank composes the full RO

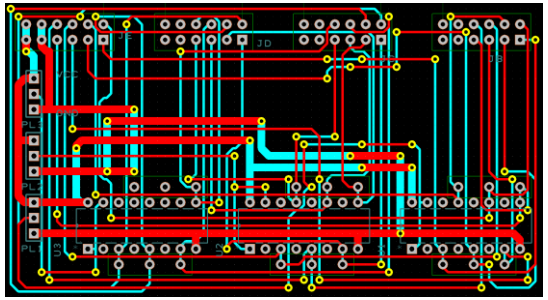
Experimental Setup

- Detector implementation
  - ARM Cortex-A9 + Artix-7 FPGA
  - UART data transmission to PC
  - FPGA utilization (0.016W)

Primitive type	Count	Percentage
Flip-Flops	363	1.03%
Look-up tables	757	4.30%
Carry logic	78	1.12%
Other	4	0.20%

- Test PCB consists of 8 ROs
- Probe specification
  - Tektronix TDP1000
  - $< 1\ pF$ input capacitance





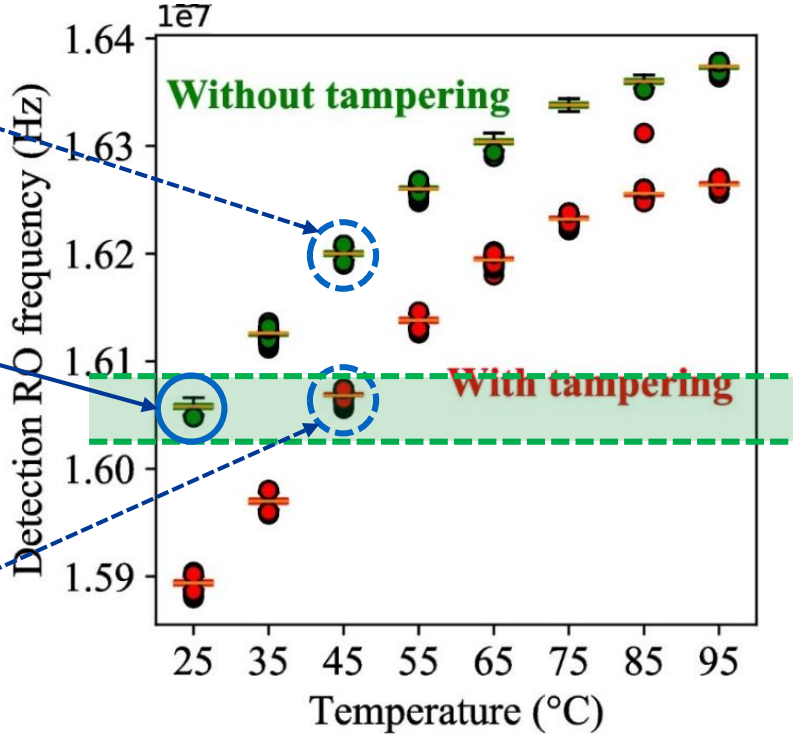
Results: Temperature Effect

- Measurement conditions: **25**℃ : 10℃ : **95**℃
- **1,000** detection RO frequencies are collected from:
  - each temperature condition
  - with and without tampering cases

Detection RO measured at 45℃.
Not tampered detected as tampered

Genuine RO enrolled at 25℃.

Detection RO measured at 35℃.
Tampered detected as not tampered



Results: Model and Detection Example

- **Enrollment conditions**: 25℃, 65℃, and 95℃.
- **Measuring target**: reference and detection ROs.
- **Model**:

  $f_{det} = \boldsymbol{G}(f_{ref})$

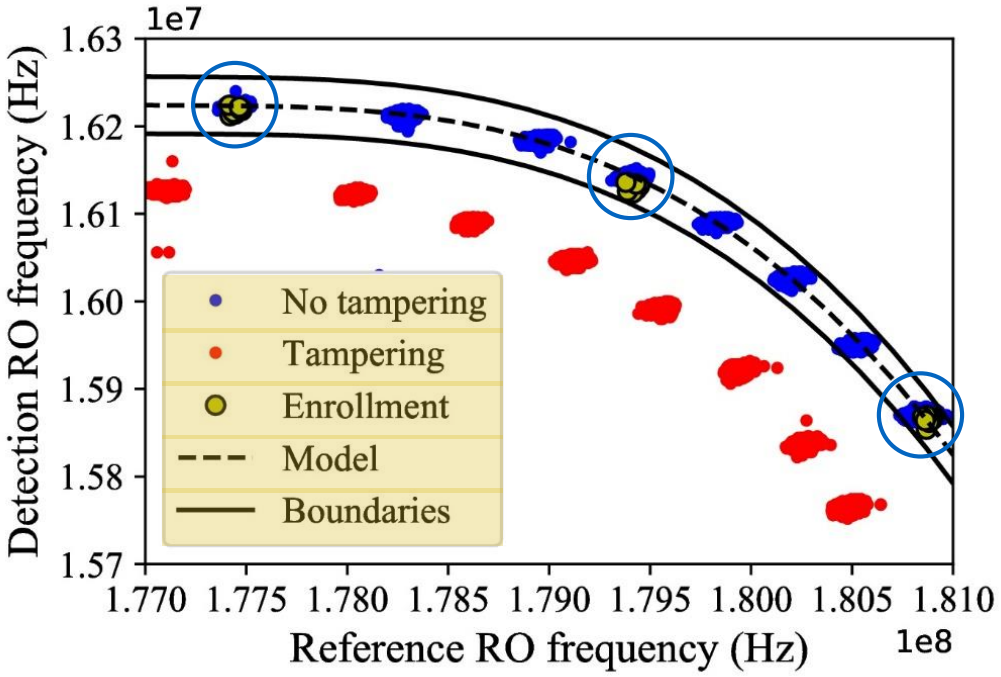
- **Detection boundaries**:

  $b_{lo} = G(f_{ref}) - 3 \times \sigma_{max}$

  $b_{up} = G(f_{ref}) + 3 \times \sigma_{max}$

- **Evaluation**:

  Test $f_{det} \in [b_{lo}, b_{up}]$



Results: Detection Performance

Metric

$$Success\ rate = \frac{TPR + TNR}{2}$$

TPR: true positive rate
TNR: true negative rate

	RO0	RO1	RO2	RO3	RO4	RO5	RO6	RO7
25℃	99.77%	100%	99.99%	100%	100%	99.99%	99.93%	99.99%
35℃	99.81%	100%	100%	100%	100%	100%	100%	100%
45℃	99.97%	99.99%	99.98%	99.99%	100%	100%	99.98%	99.99%
55℃	100%	100%	100%	100%	100%	100%	100%	100%
65℃	100%	100%	100%	100%	100%	100%	100%	100%
75℃	100%	100%	100%	100%	100%	100%	100%	100%
85℃	100%	100%	100%	100%	100%	99.99%	100%	100%
95℃	100%	100%	100%	100%	100%	100%	100%	100%

Conclusion and Future work

Model-assisted PCB Attestation (MPA) Framework

- Plug-in-play style tamper detection
- Low FPGA utilization
- High detection accuracy ($> 99.7\%$) across a large temperature range

Future work

- Eliminate the multi-condition enrollment
- Investigate the feasibility of unique board ID generation from the MPA framework
- Analyze the impact of board-level trace design on tamper detection and unique ID generation
- Develop a run-time tamper detection approach

Acknowledgements and Questions

This work is made possible though the grants, gifts, and partnerships with

Contact Information

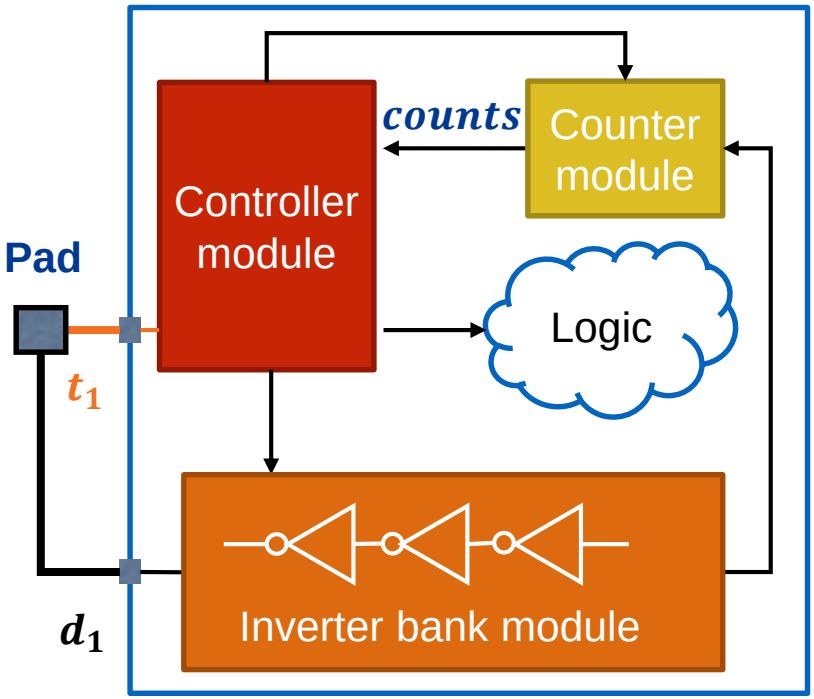
- Prof. Domenic Forte, University of Florida, ECE
- Webpage: http://dforte.ece.ufl.edu
- E-mail: dforte@ece.ufl.edu
- Phone: 352-392-1525

Backup slides

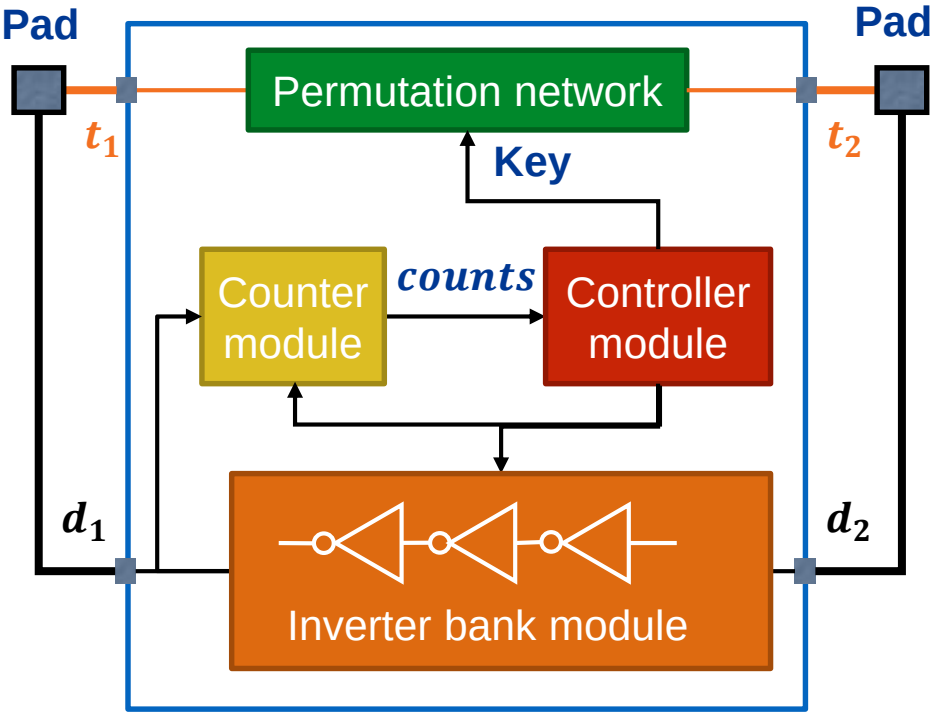
MPA implementation: detector design

Permutation network | Counter | Inverter bank | Controller

Embedded mode detector



Standalone mode detector



MPA Implementation: Controller Module

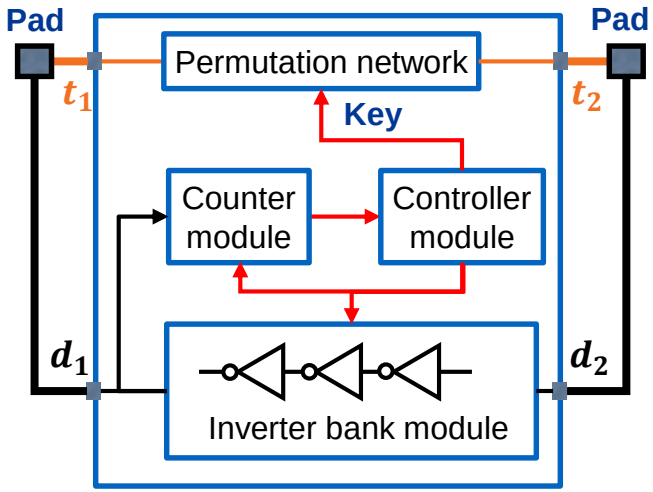
- Send the correct **key** to the **permutation network** when no tampering is detected.

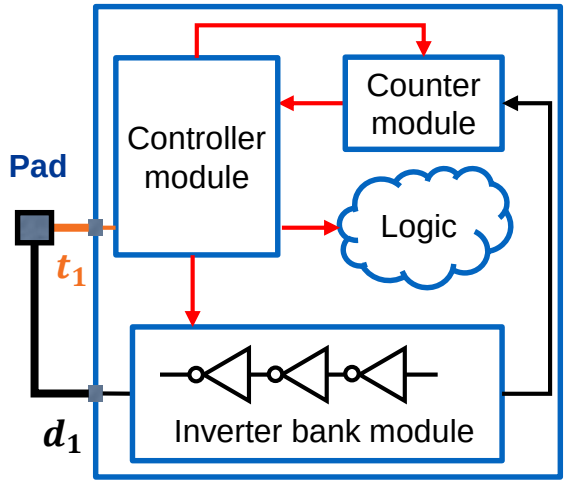
S-mode detector

- Configure the **invert bank** module and select RO.
- Configure the **counter** module and collect the counts.
- Compute the RO frequency.

E-mode detector

- Connect t_1 to the internal logic if no tampering is detected.





Results: Temperature Effect

- Theoretically, high temperature slows down the transistor's switching speed. Thus, the RO frequency should decrease.
- **1,000** detection RO frequencies are collected from
  - Each temperature condition, without tampering
  - Different length of detection ROs

This "irregular" observation is possibly due to the impact which derives from the pad of the SoC port.