VERNAM LAB
Worcester Polytechnic Institute

WPI

Toward High-Confidence System-Level Tamper Detection using Impedance Sensing

Tahoura Mosavirik, Patrick Schaumont, Fatemeh (Saba) Ganji, and Shahin Tajik,

Zero Trust Hardware Architectures Workshop (ZTHA), 3 November 2022

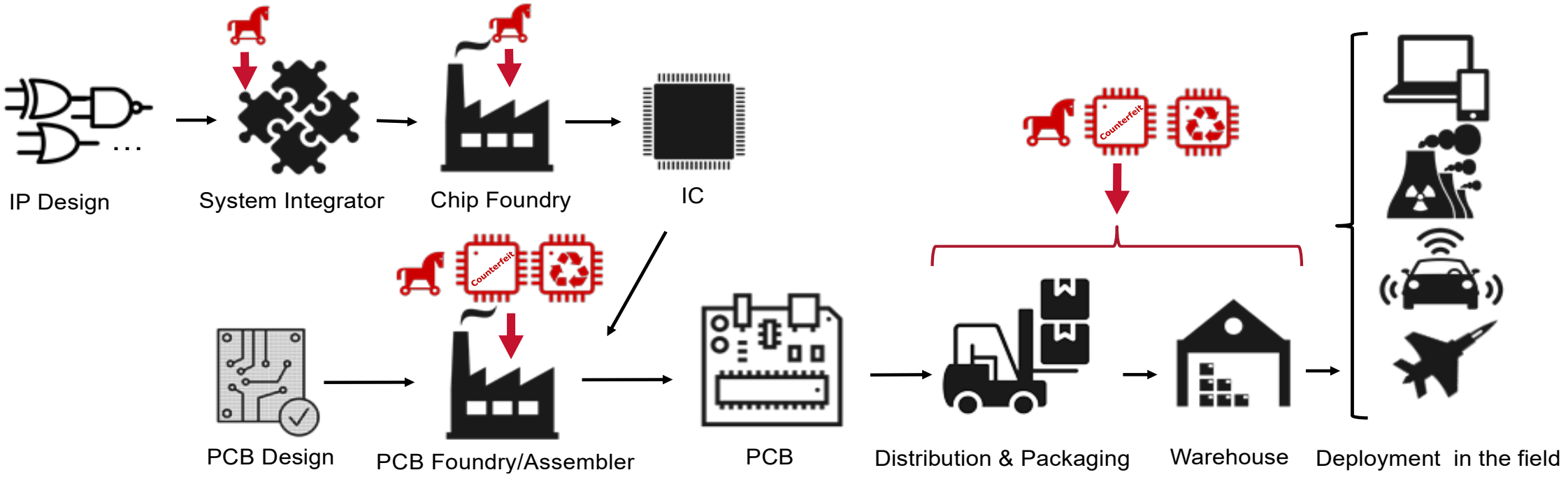
NSF
EPRI ELECTRIC POWER RESEARCH INSTITUTE
CISCO

Supply chain security

Electronic device supply chain security

VERNAM LAB
Worcester Polytechnic Institute

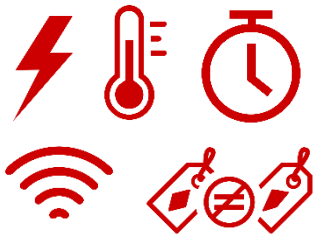
Motivation

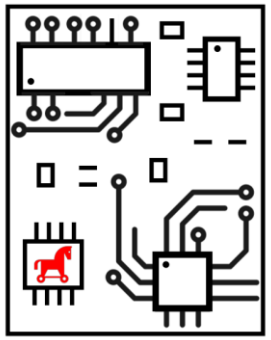


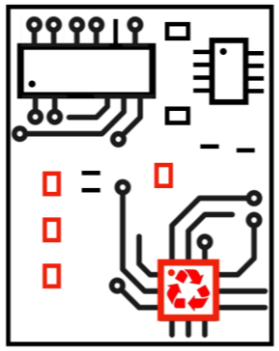
Existing verification methods

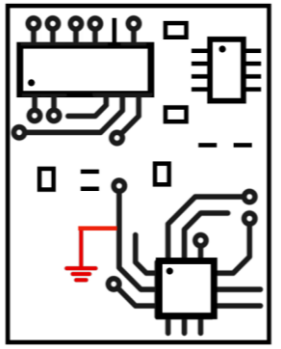
Impacts of threats on physical characteristics

VERNAM LAB
Worcester Polytechnic Institute

	Spy chips or HW Trojan on PCB	Counterfeit Components or Removing/adding components	Reliability Issues, Ageing, etc.
Impacts on physical characteristics of the system: 	• PCB Visual patterns • PCB Traces & vias • PCB impedance • PCB timing • PCB power • PCB temperature	• PCB visual patterns • Components' package • PCB Traces & vias • PCB impedance • PCB freq. response • IC side-channel leakages	• PCB Traces & vias • PCB impedance • PCB freq. response • PCB power • PCB temperature • IC side-channel leakages

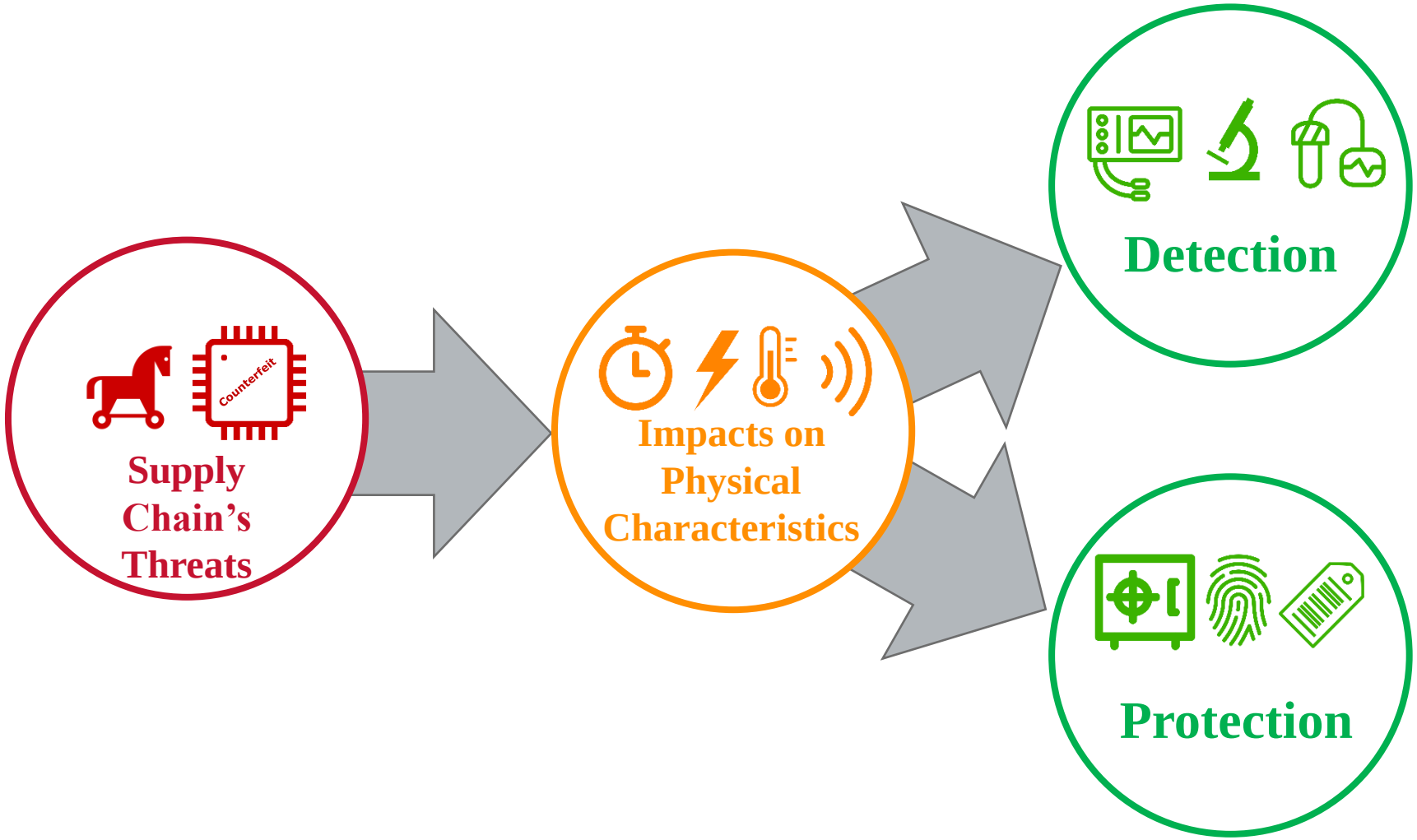




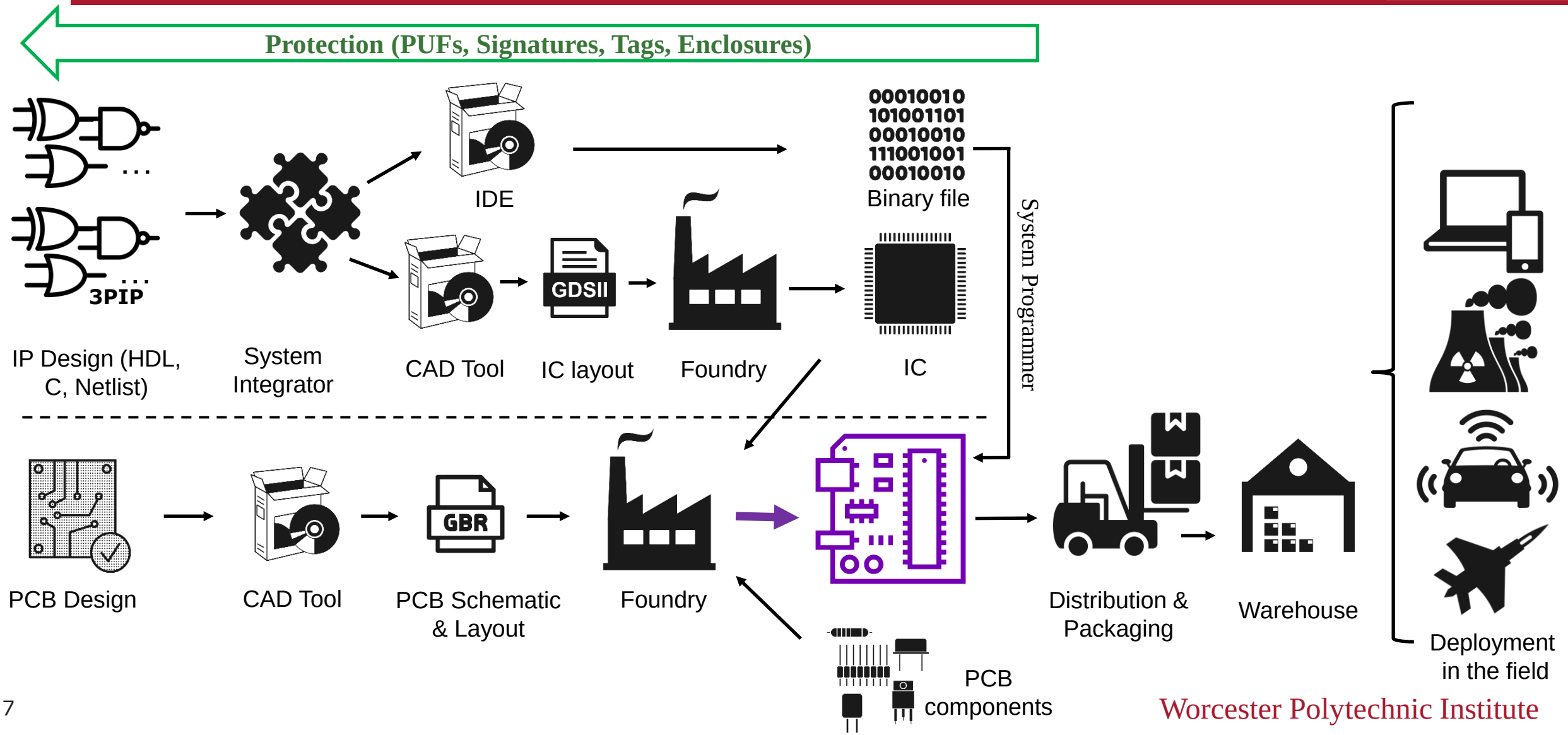


serve as backdoors and kill switches.

Verification approaches

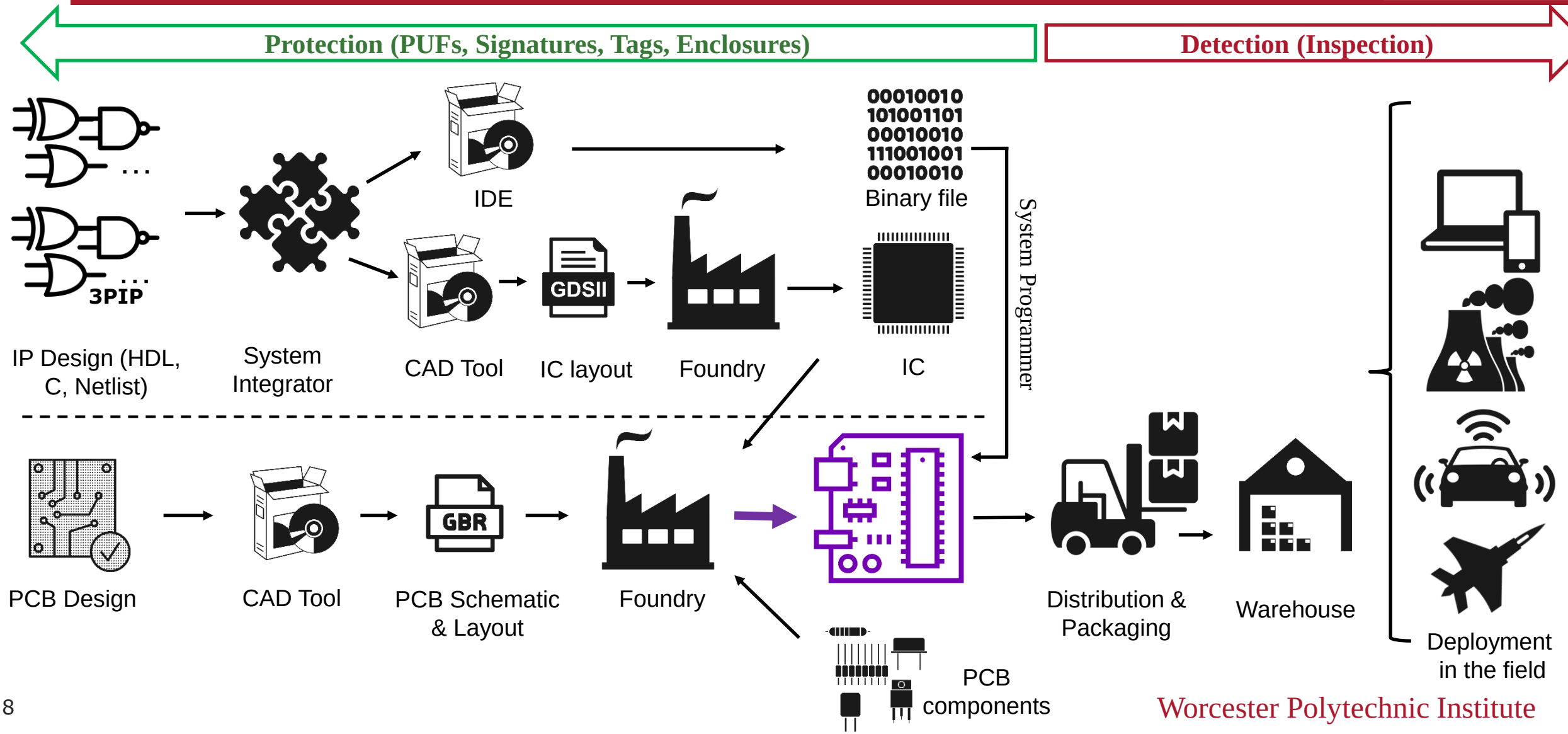


Protection vs. detection approaches



Protection vs. detection solutions

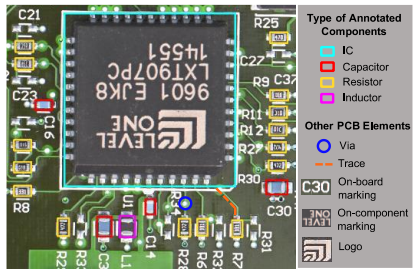
VERNAM LAB
Worcester Polytechnic Institute

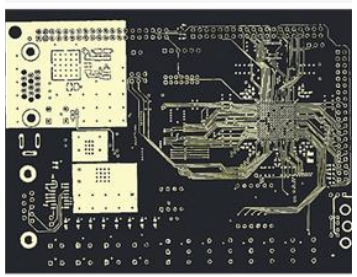


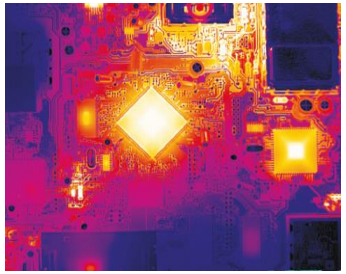
Available Inspection Tools

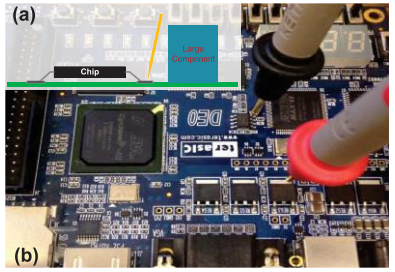
VERNAM LAB
Worcester Polytechnic Institute

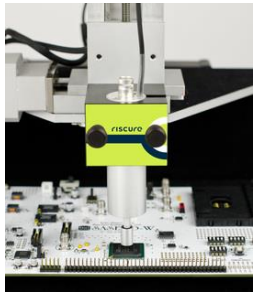
	Visual Inspection	X-ray Tomography	Thermal Analysis	Electrical Analysis	EM (Microwave & Terahertz) Analysis
Detectable Features:	• PCB Visual layout • PCB Traces & vias (top & bottom layers) • PCB visual artifacts • Components' package	• PCB layout (all layers) • PCB Traces & vias (all layers)	• PCB/IC thermal emissions • PCB/IC timing • Short/open circuits	• PCB/IC impedance • PCB/IC timing • PCB/IC power consumption	• PCB/IC impedance • PCB/IC timing • PCB/IC EM emissions







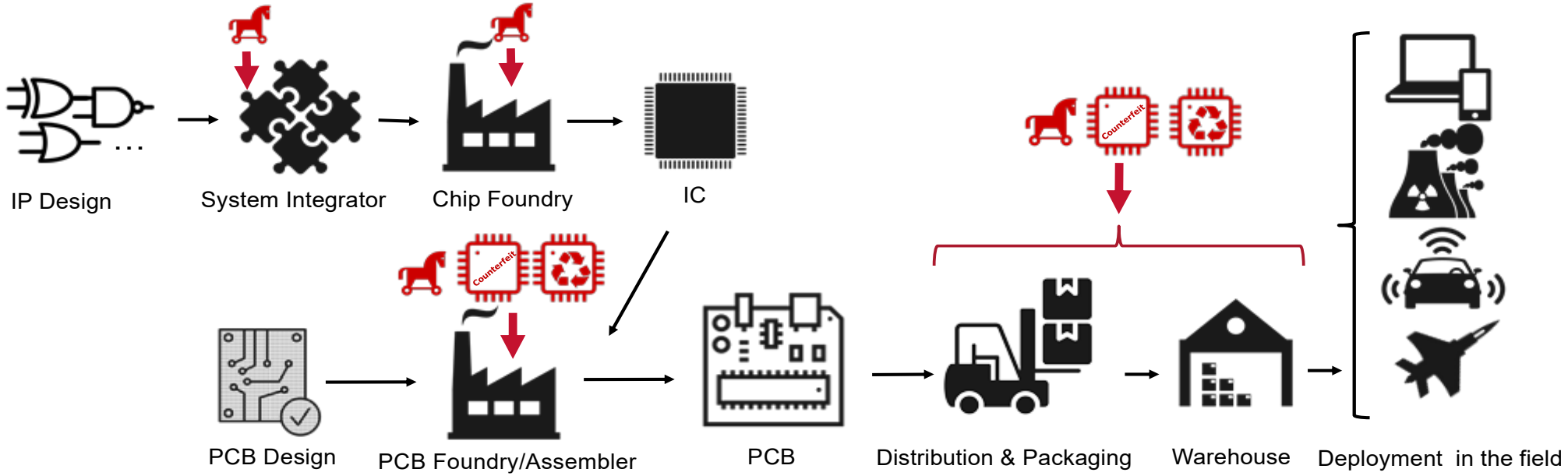




Electronic device supply chain security

VERNAM LAB
Worcester Polytechnic Institute

Motivation



Goal

- Generating **hardware signatures** to differentiate between Genuine and counterfeit boards by monitoring the physical behavior of the system.

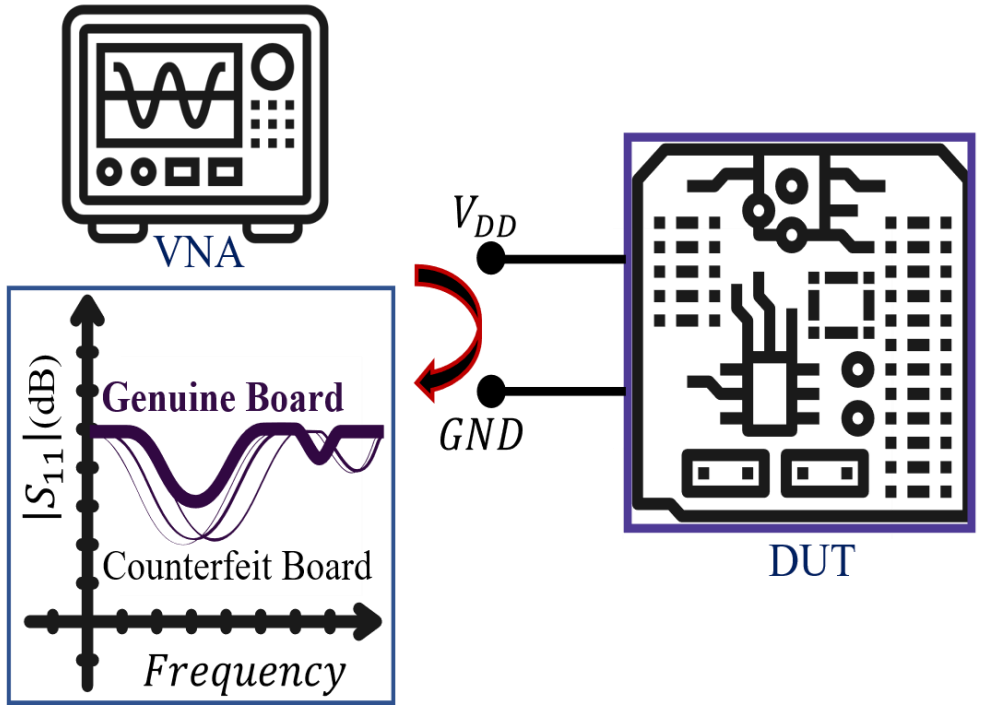
First solution

Threat model

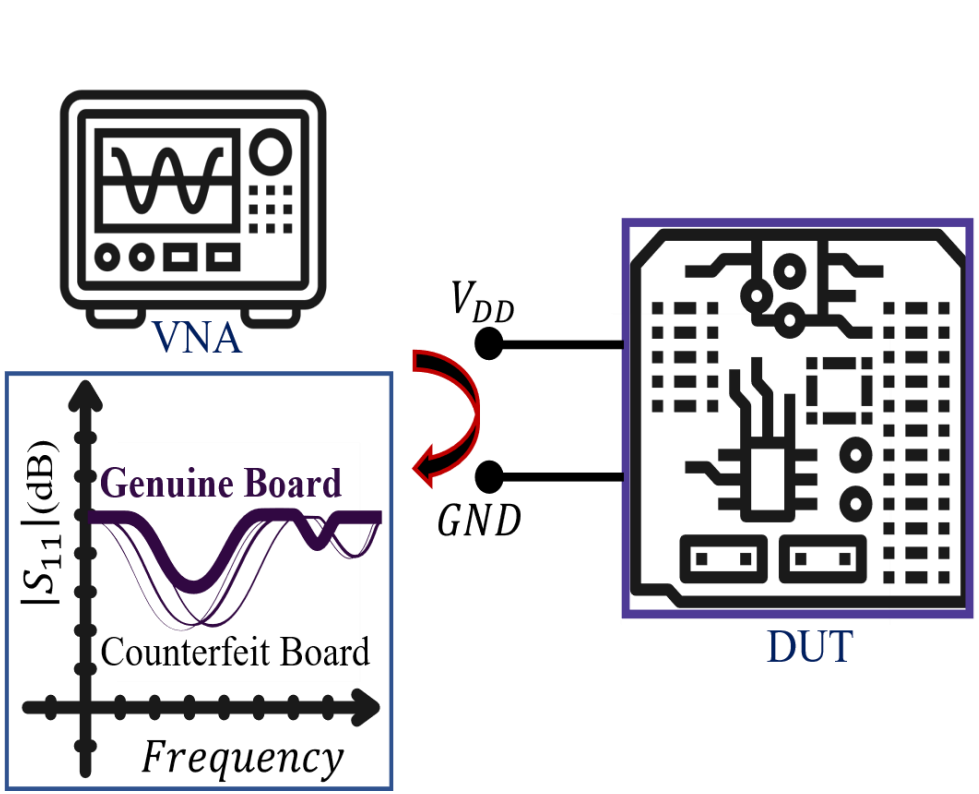
- We assume that the adversary can physically tamper with all components of the PCB prior to the verification.
- For different verification scenarios, we assume that the verifier possesses a golden sample to compare the measurements.
- The goal is that before deploying the PCB in the field, the designer or the end user verifies the authenticity of the devices.

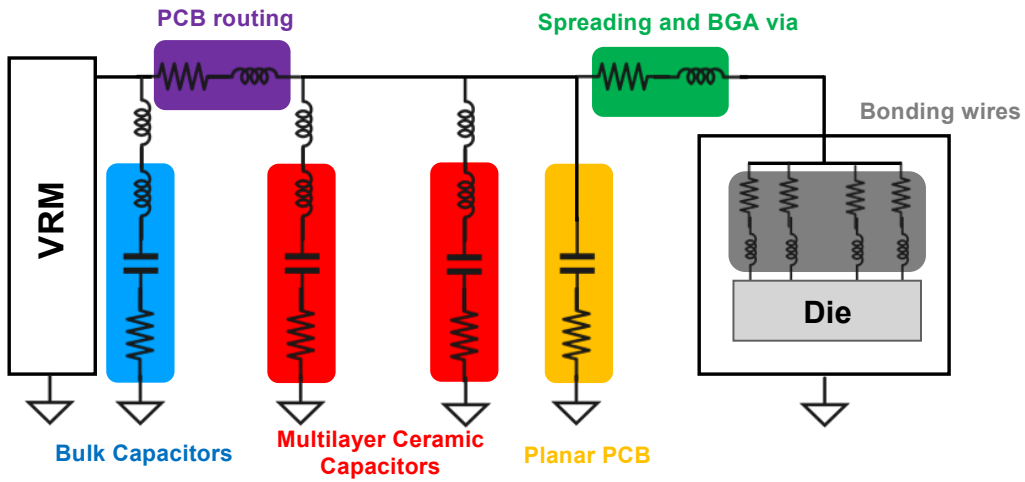
Verification methodology

- Converting the unique properties in the **power distribution network** (PDN) of a PCB into physical signatures.



Power distribution network (PDN)

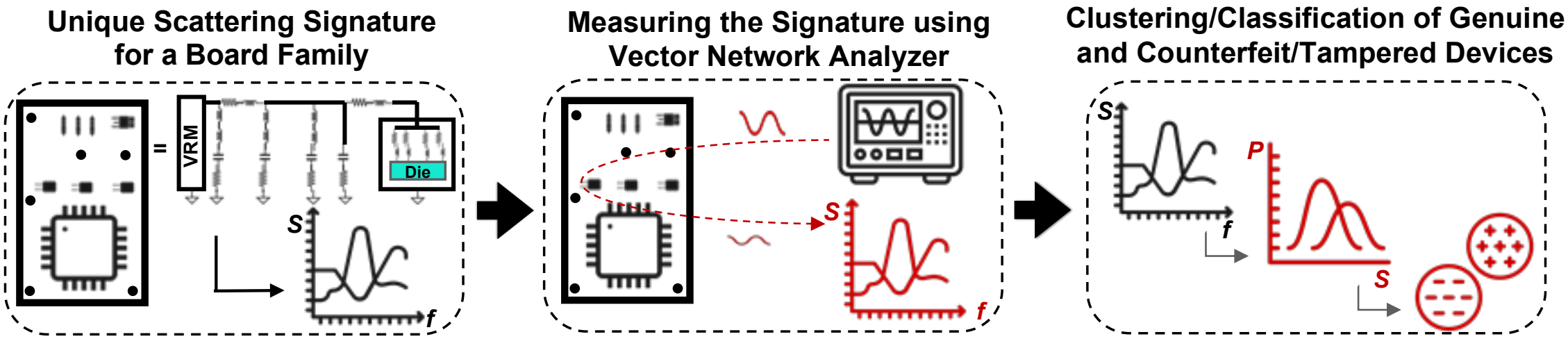




Equivalent circuit of PCB's PDN

1) Stimulate the device under test (DUT).
2) Measure the electrical 'echo' of the system to the applied stimulus.
3) Compare the resultant electrical 'echoes' of the counterfeit and genuine samples.

ScatterVerif [1]

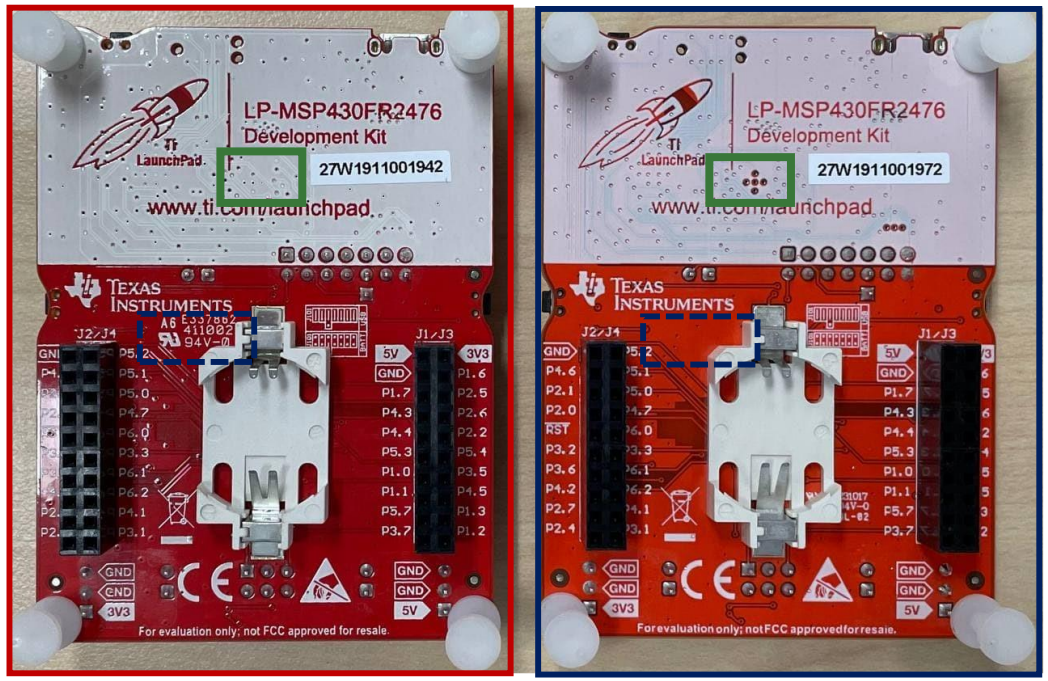


[1] T. Mosavirik, F. Ganji, P. Schaumont, and S. Tajik, "Scatterverif: Verification of electronic boards using reflection response of power distribution network", ACM Journal on Emerging Technologies in Computing Systems, 18(4):1–24, 2022.

Case studies and results (inter-genuine signatures)

10 PCBs

10 PCBs



Group 2

Group 1

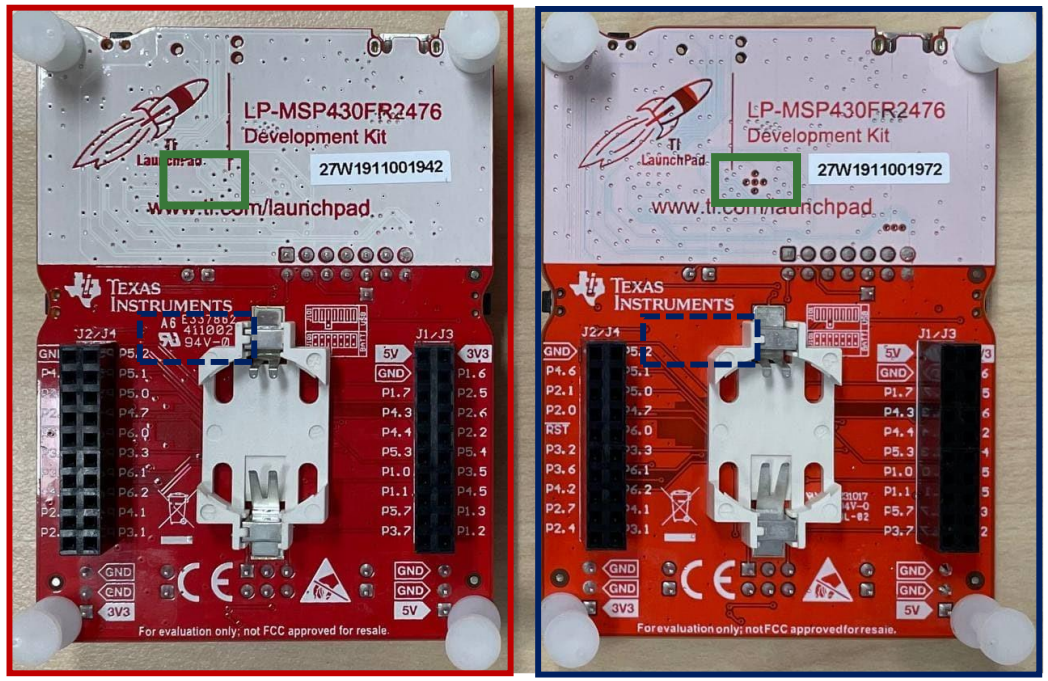
Backside of 2 different groups of MSP430FR2476 development kits

[1] T. Mosavirik, F. Ganji, P. Schaumont, and S. Tajik, "Scatterverif: Verification of electronic boards using reflection response of power distribution network", ACM Journal on Emerging Technologies in Computing Systems, 18(4):1–24, 2022.

Case studies and results (inter-genuine signatures)

10 PCBs

10 PCBs

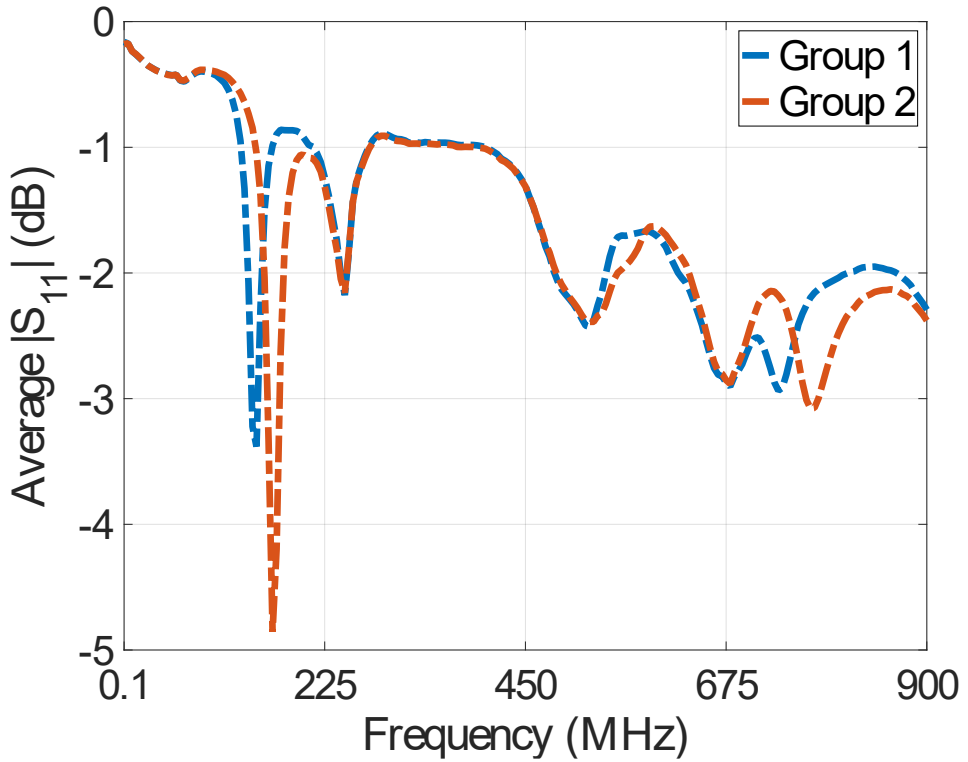


Group 2

Group 1

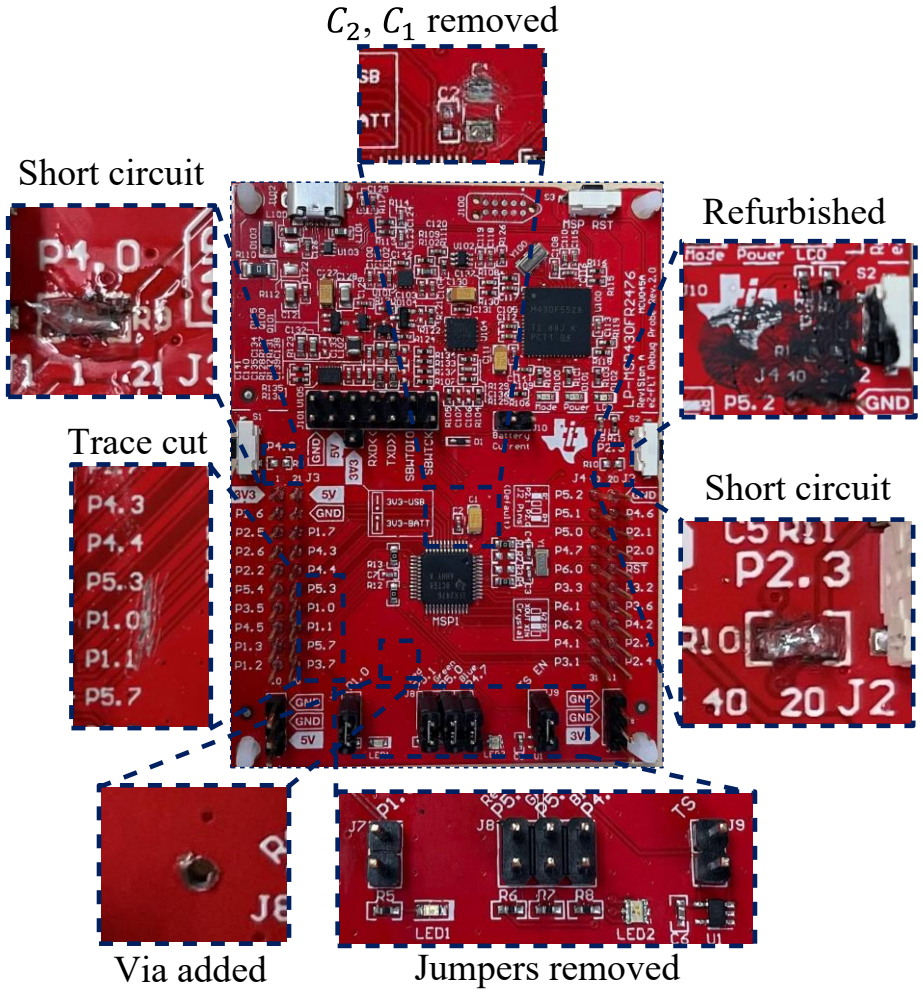
Backside of 2 different groups of MSP430FR2476 development kits

Manufacturing process variation



[1] T. Mosavirik, F. Ganji, P. Schaumont, and S. Tajik, "Scatterverif: Verification of electronic boards using reflection response of power distribution network", ACM Journal on Emerging Technologies in Computing Systems, 18(4):1–24, 2022.

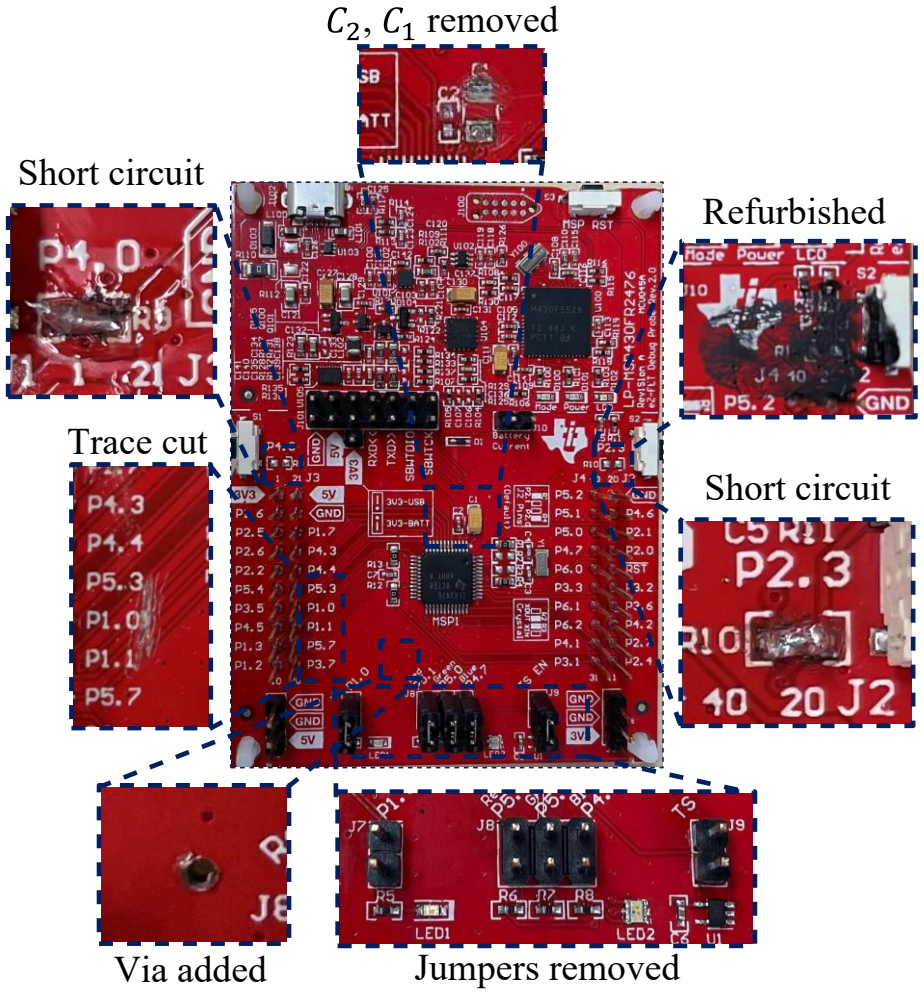
Case studies and results (tampering on MSP boards)

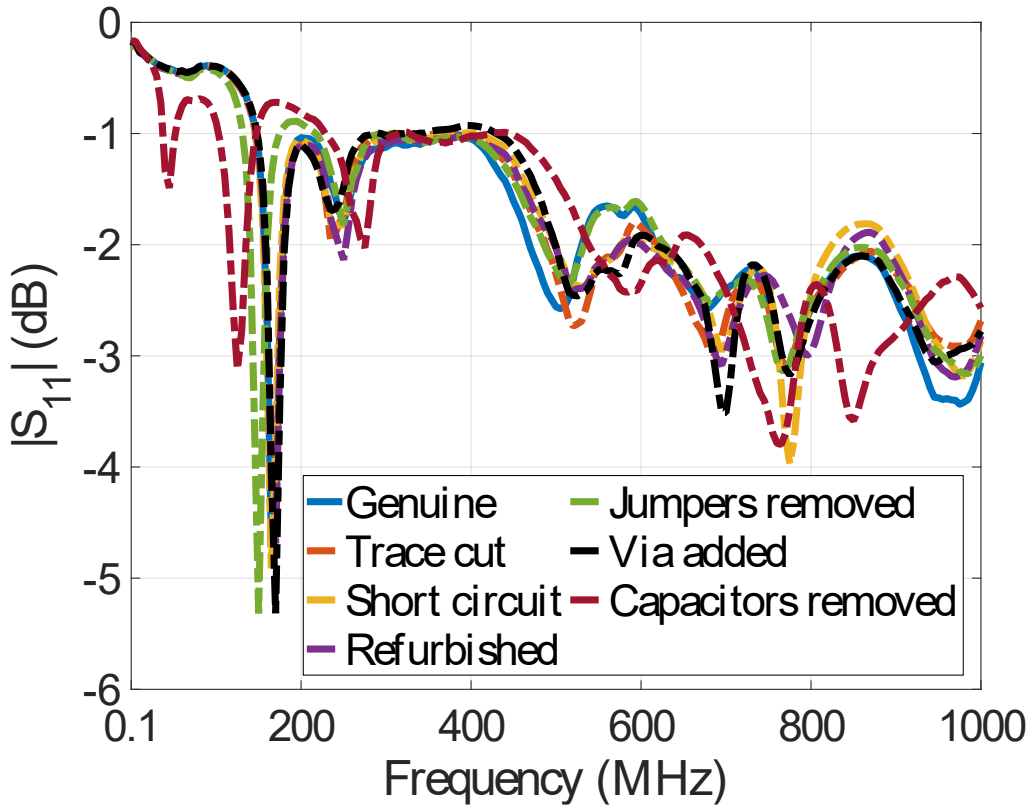


[1] T. Mosavirik, F. Ganji, P. Schaumont, and S. Tajik, "Scatterverif: Verification of electronic boards using reflection response of power distribution network", ACM Journal on Emerging Technologies in Computing Systems, 18(4):1–24, 2022.

Case studies and results (tampering on MSP boards)

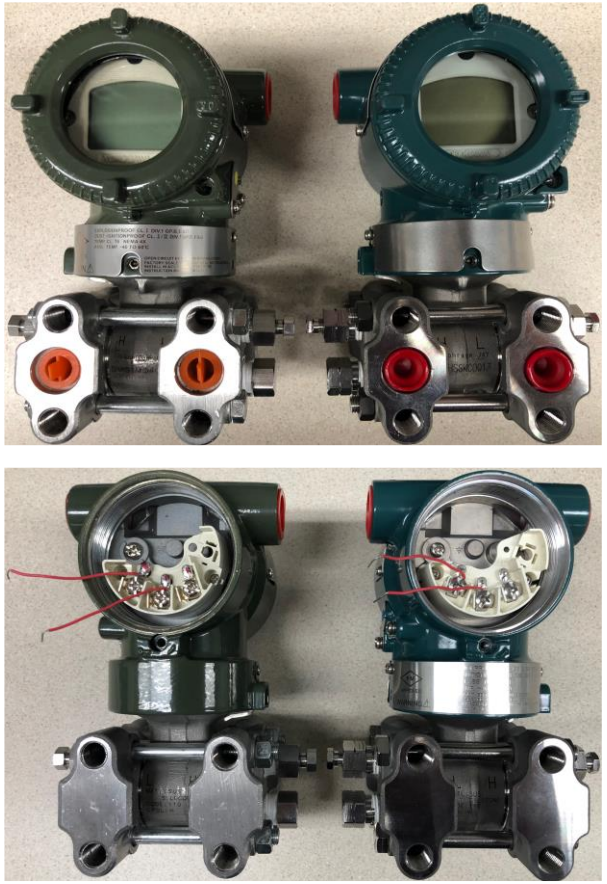
VERNAM LAB
Worcester Polytechnic Institute

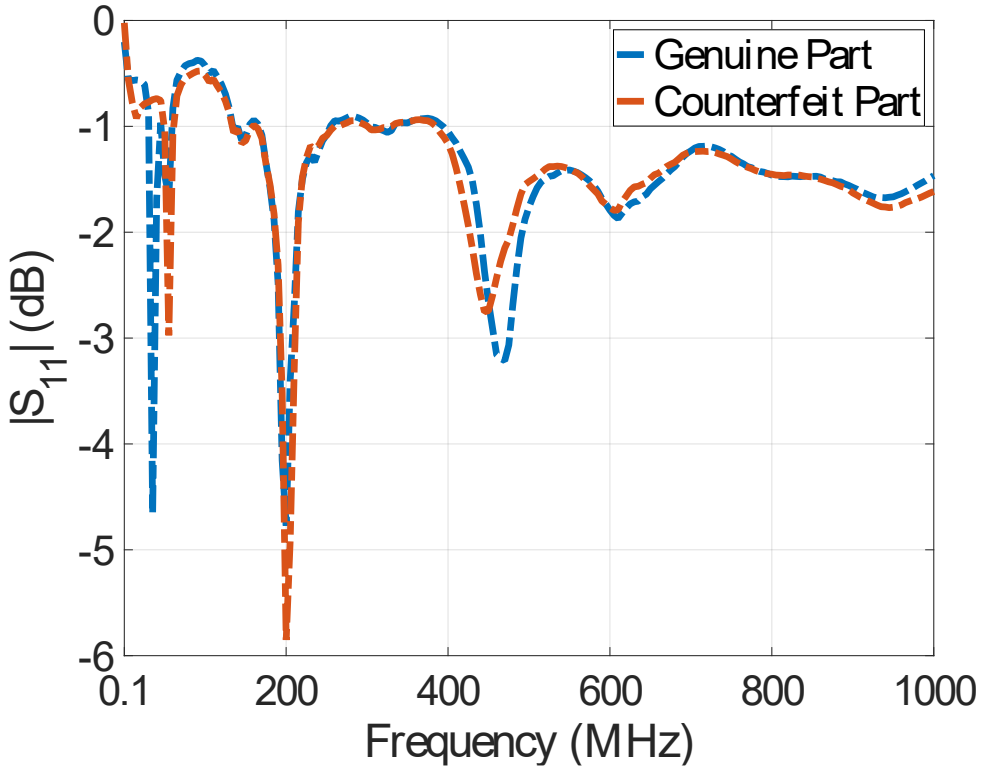




[1] T. Mosavirik, F. Ganji, P. Schaumont, and S. Tajik, "Scatterverif: Verification of electronic boards using reflection response of power distribution network", ACM Journal on Emerging Technologies in Computing Systems, 18(4):1–24, 2022.

Case studies and results (pressure sensors)





DUTs: a counterfeit (left) and genuine (right) pressure sensors

[1] T. Mosavirik, F. Ganji, P. Schaumont, and S. Tajik, "Scatterverif: Verification of electronic boards using reflection response of power distribution network", ACM Journal on Emerging Technologies in Computing Systems, 18(4):1–24, 2022.

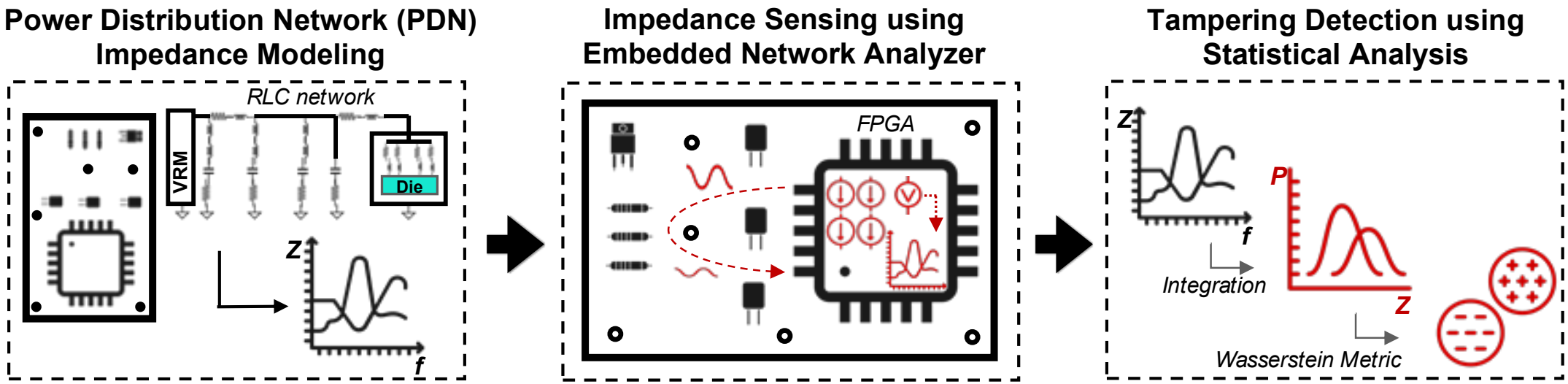
Second solution

Threat model

- we assume that the victim's electronic board is operated in an untrusted field and the attacker has physical access to it.
- The goal is to detect the attacker's tampering attempt on the system before she can mount SCA or FI attacks.
- We assume that the adversary can physically tamper with all components on the core and I/O PDNs of the board connected to the victim chip, including adding/removing/replacing other components.
- The proposed sensing countermeasure works on powered-on systems.
- We assume that the PDN's impedance profiles of genuine samples have been collected in an enrollment phase in a trusted environment and stored on the same chip, which performs the impedance characterization.

ImpedanceVerif [2]

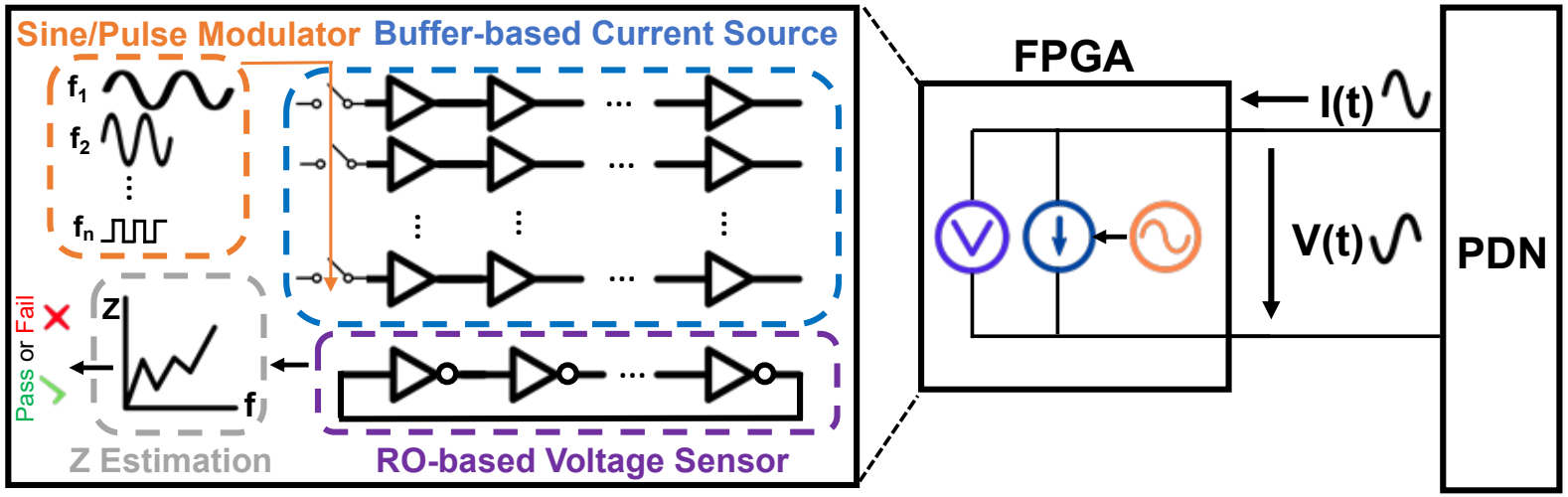
On-chip impedance sensing



[2] T. Mosavirik, P. Schaumont, and S. Tajik, "ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection", IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2023).

An embedded VNA on FPGA

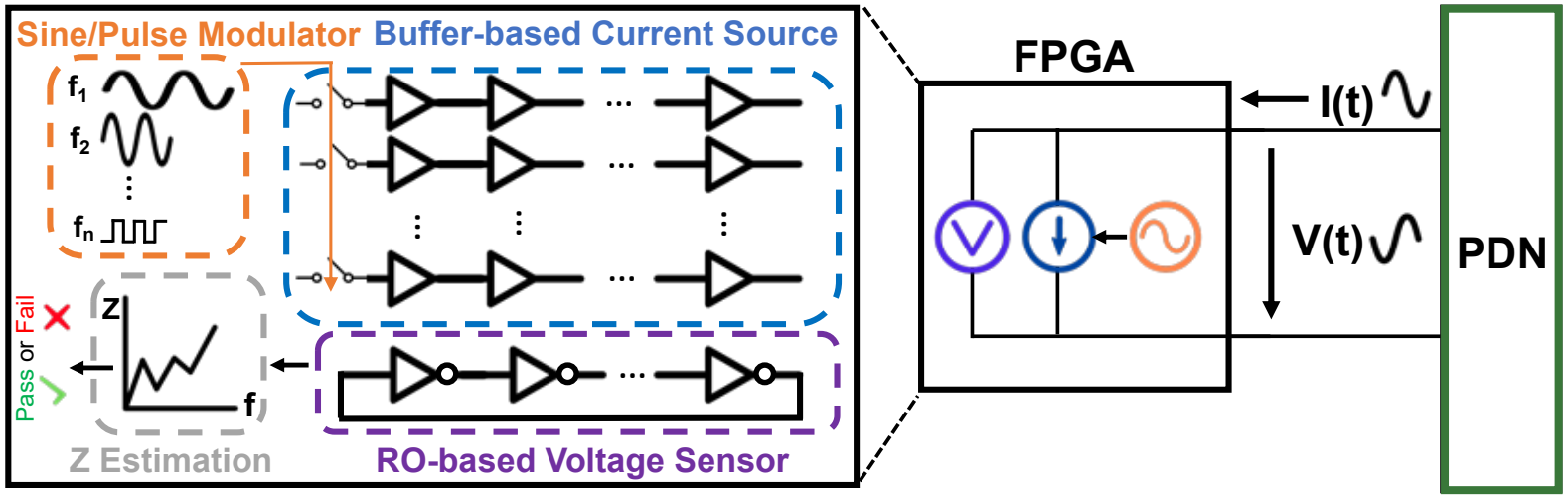
Main building blocks of an embedded VNA on FPGA



Cosmin Iorga, "Solve Power Integrity Problems in FPGA Systems Using an Embedded Vector Network Analyzer", Signal Integrity Journal, 2018.

An embedded VNA on FPGA

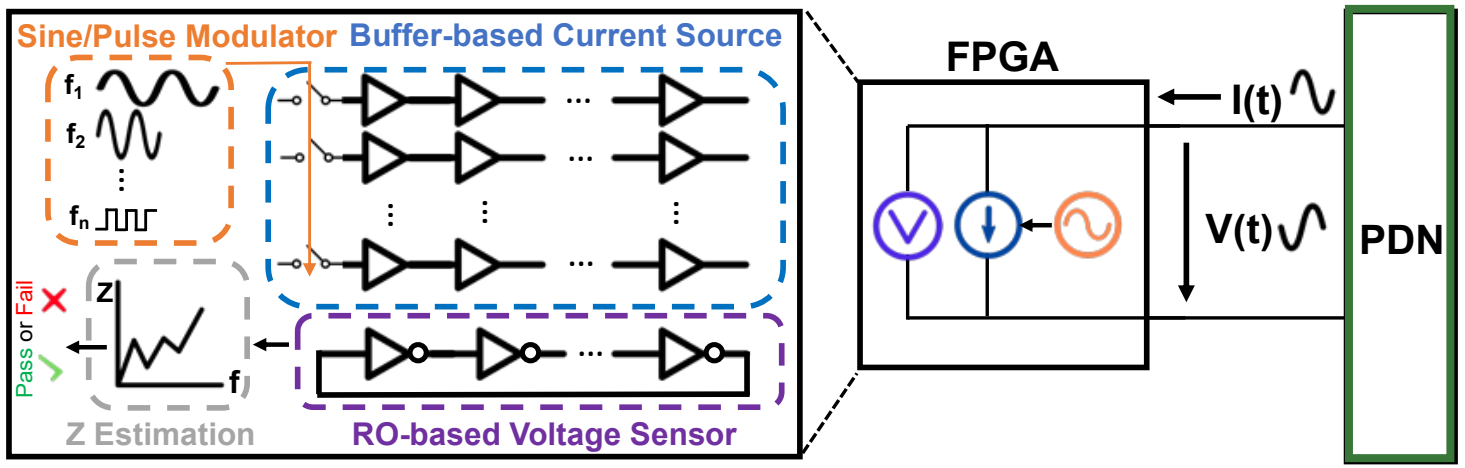
Main building blocks of an embedded VNA on FPGA

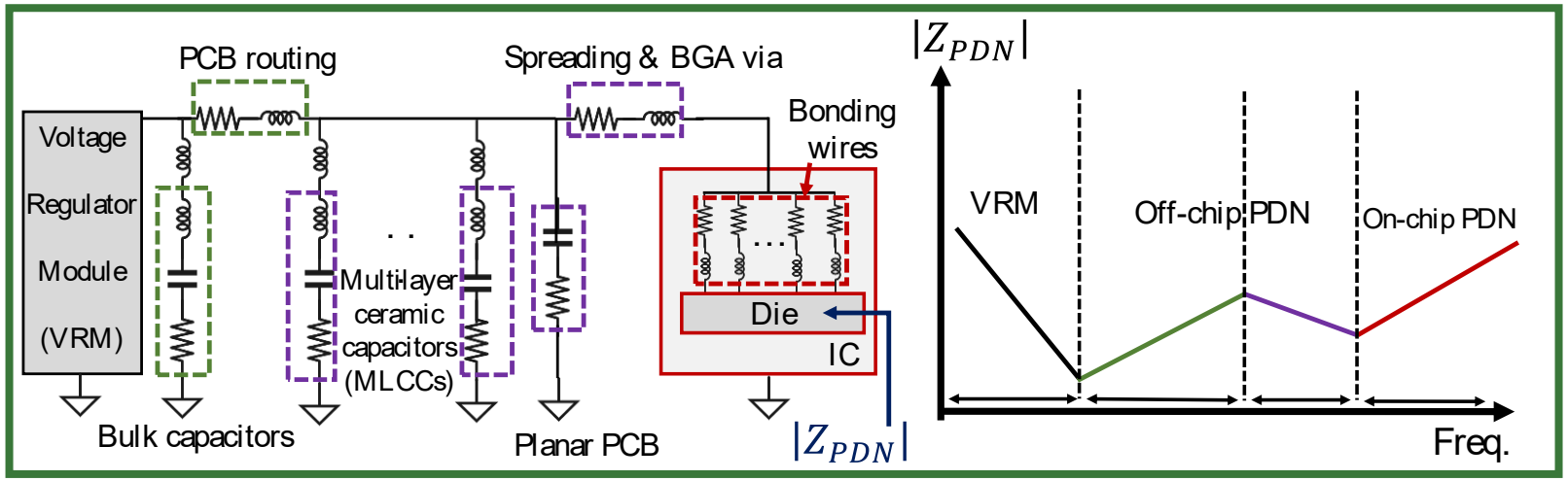


Cosmin Iorga, "Solve Power Integrity Problems in FPGA Systems Using an Embedded Vector Network Analyzer", Signal Integrity Journal, 2018.

An embedded VNA on FPGA

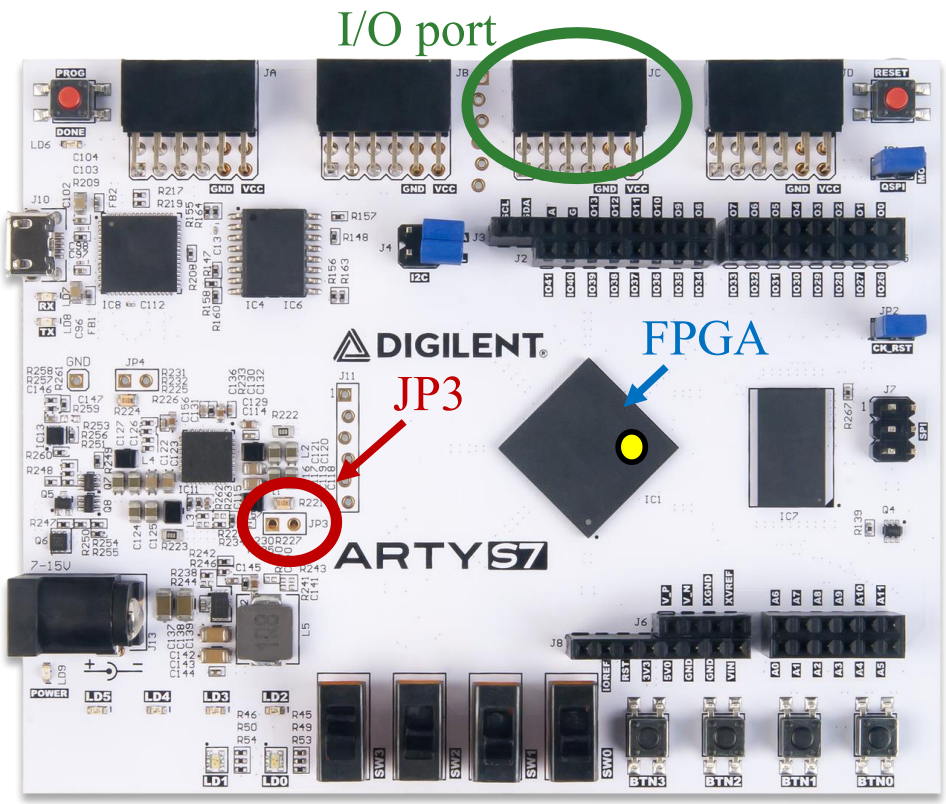
Main building blocks of an embedded VNA on FPGA



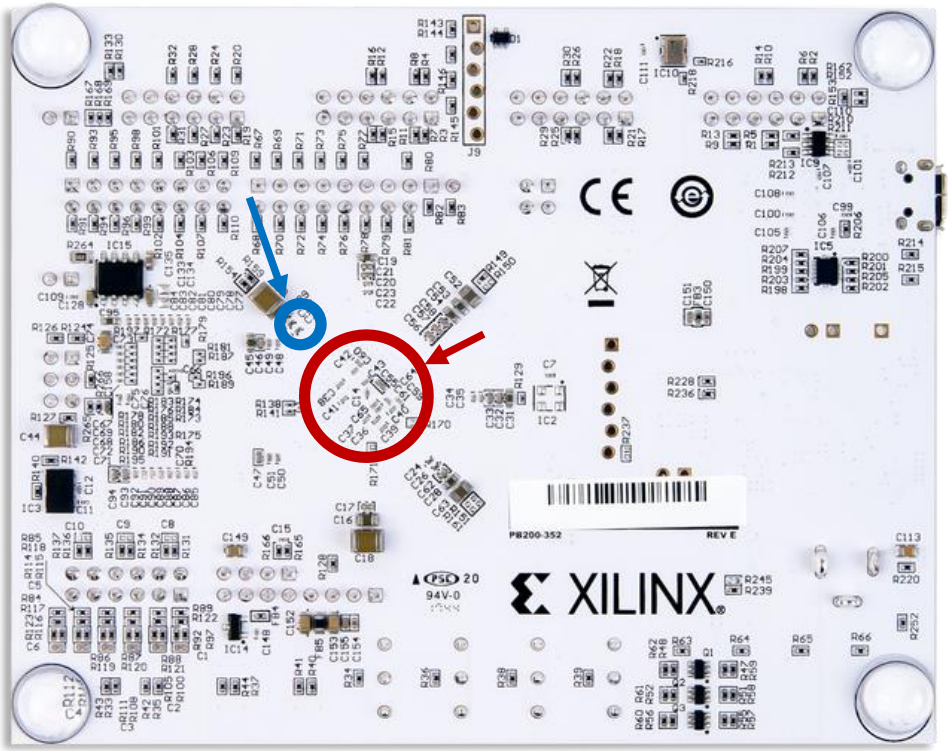


[2] T. Mosavirik, P. Schaumont, and S. Tajik, "ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection", IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2023).

Device under test



Front

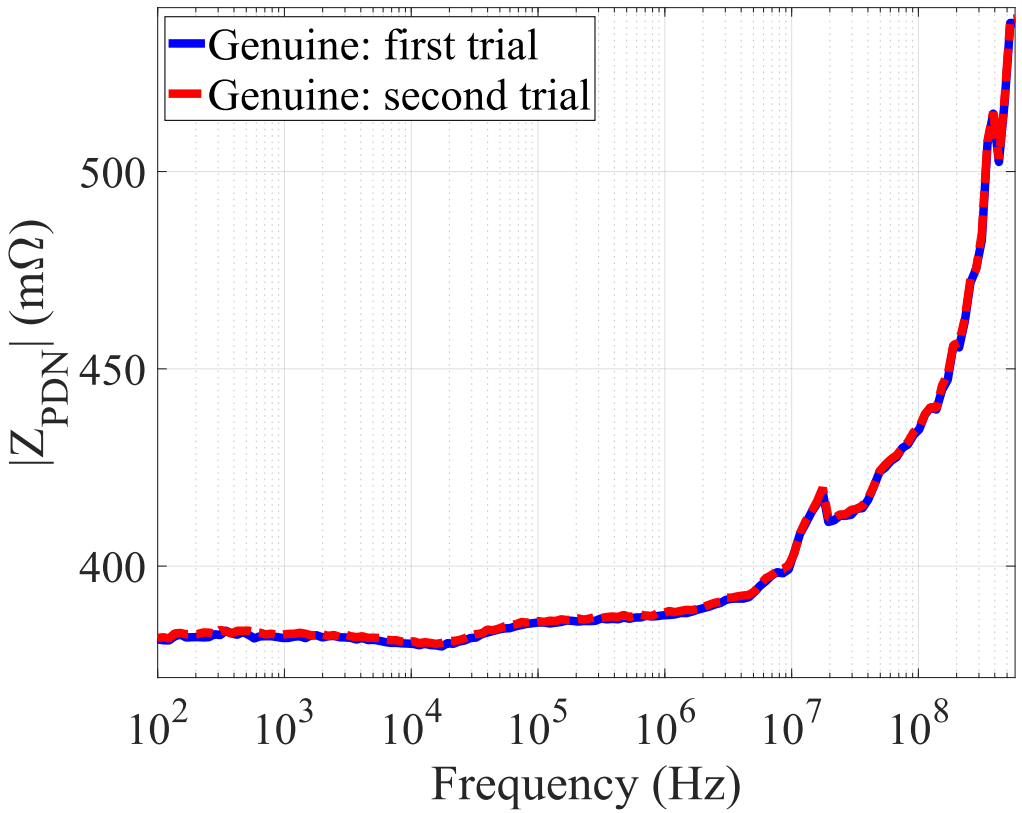


Backside

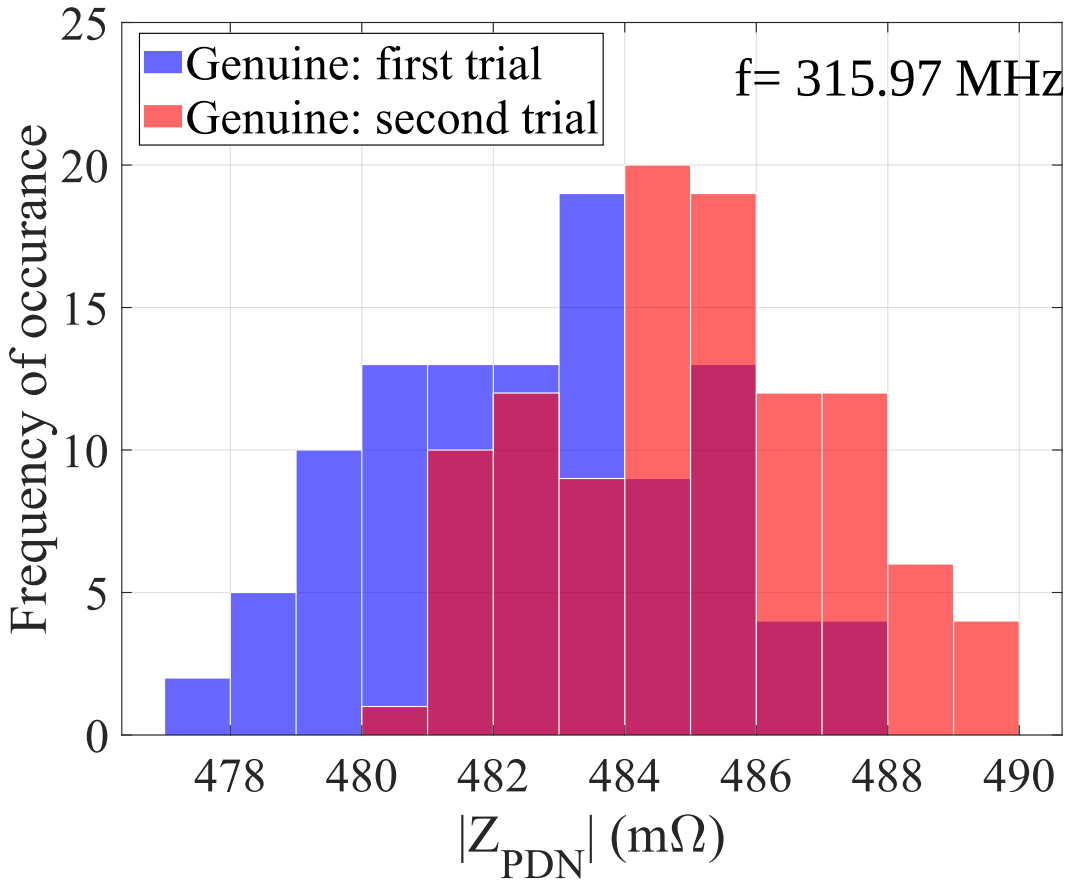
[2] T. Mosavirik, P. Schaumont, and S. Tajik, “ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection”, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2023).

Results for intra-genuine PCBs

The averaged impedance value of 105 measurement

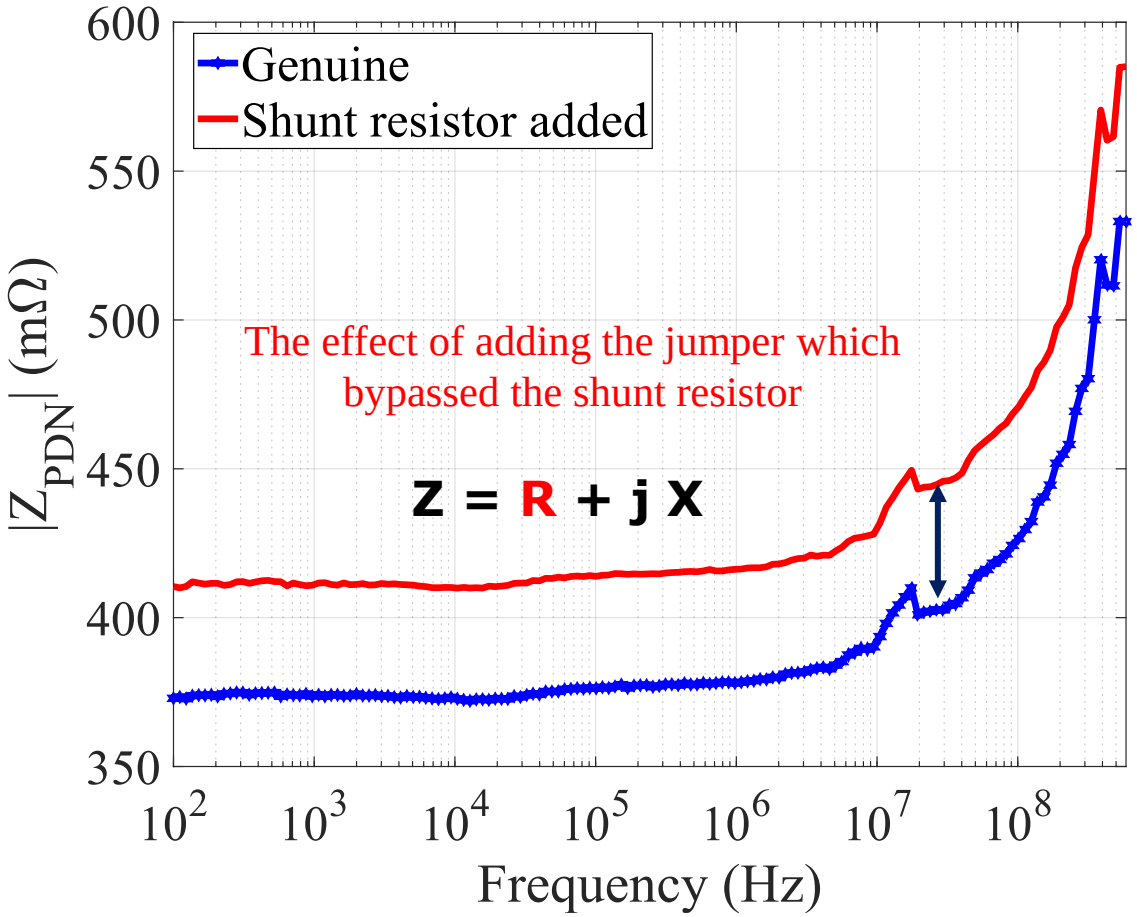


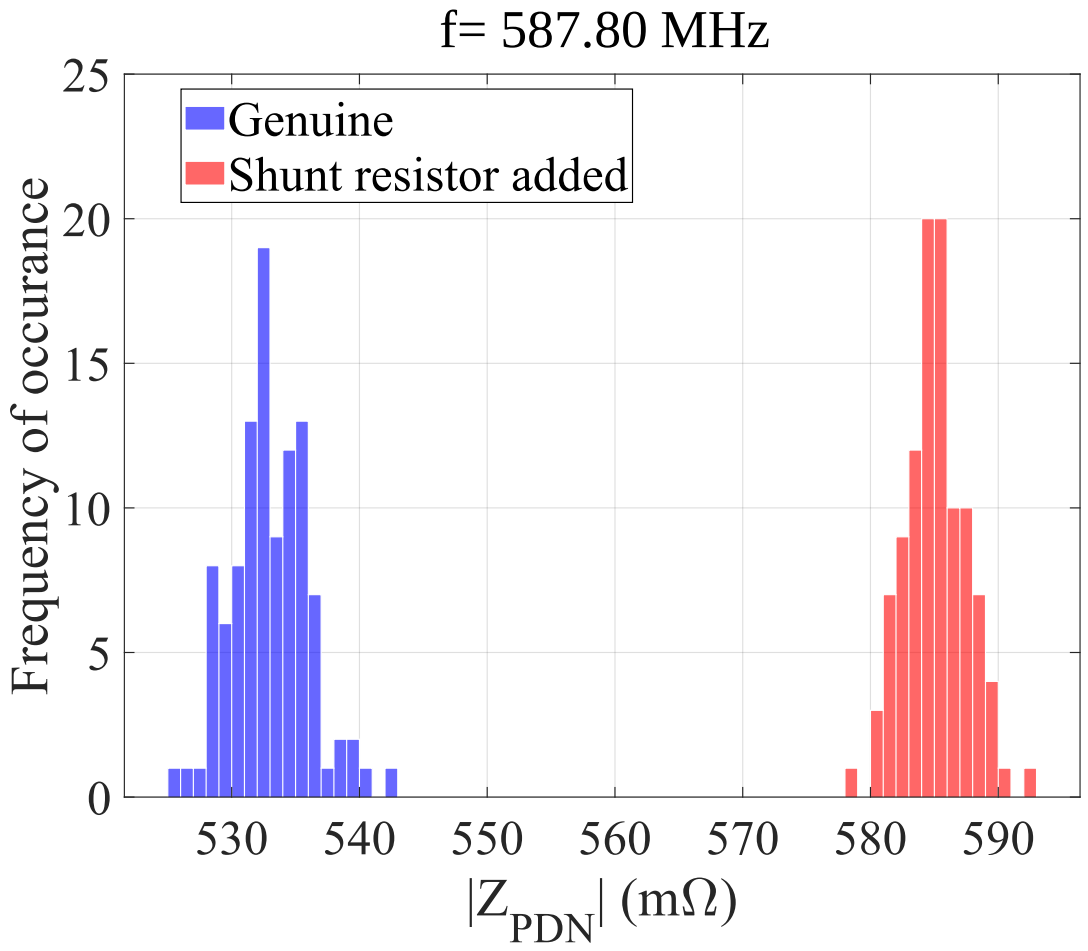
Maximum deviation between means of the measurements



[2] T. Mosavirik, P. Schaumont, and S. Tajik, "ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection", IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2023).

Results for adding a shunt resistor

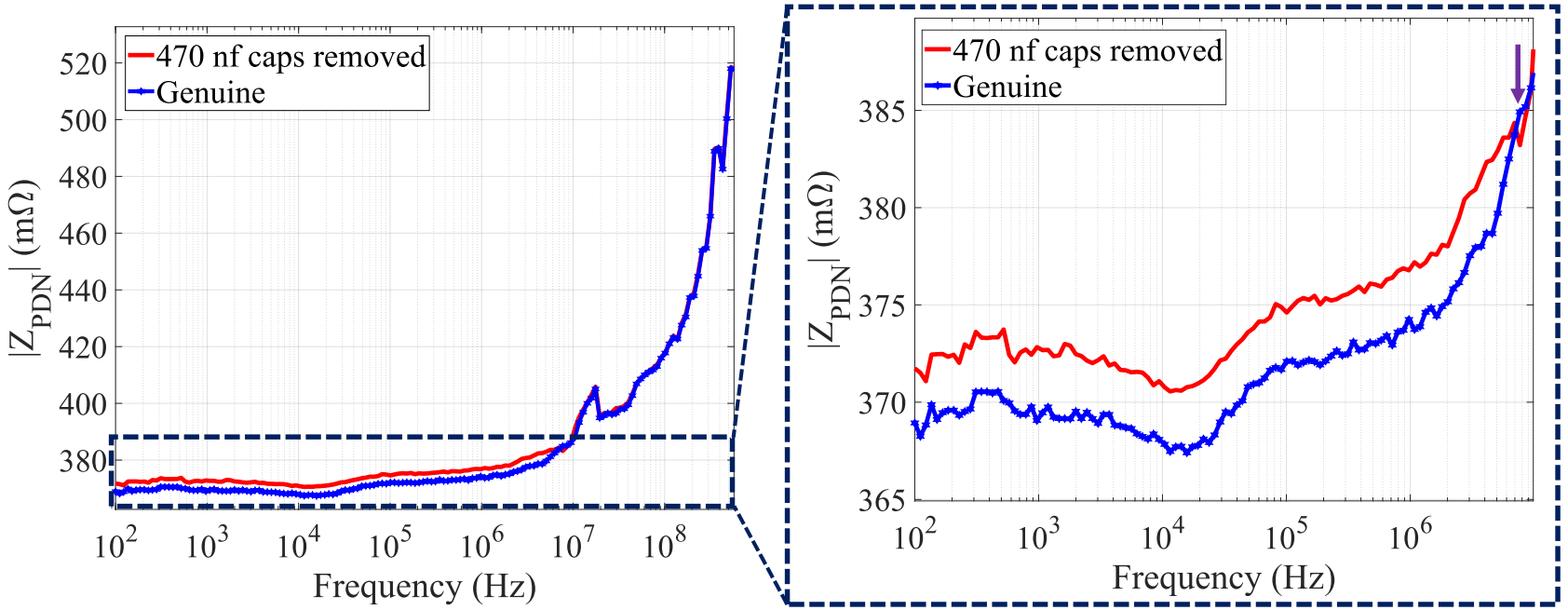


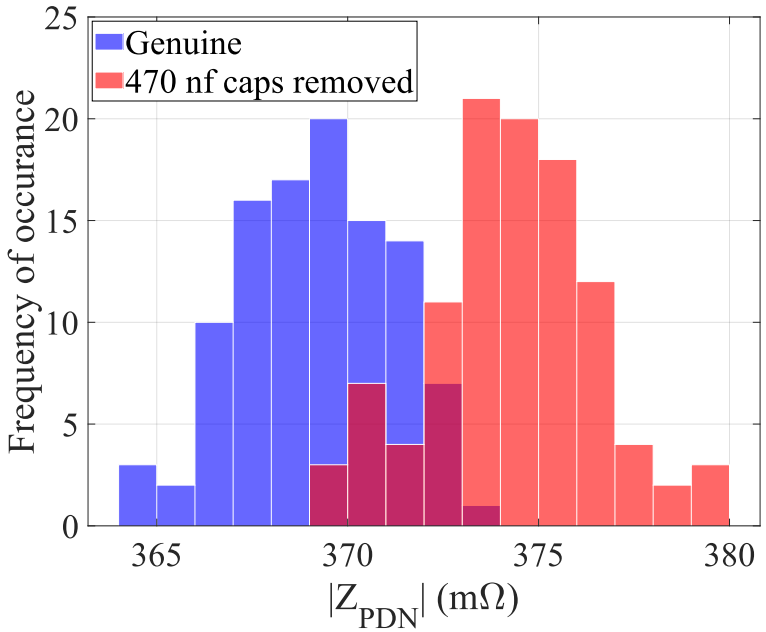


[2] T. Mosavirik, P. Schaumont, and S. Tajik, "ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection", IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2023).

Results for removing 470 nF capacitors

f= 1.57 kHz

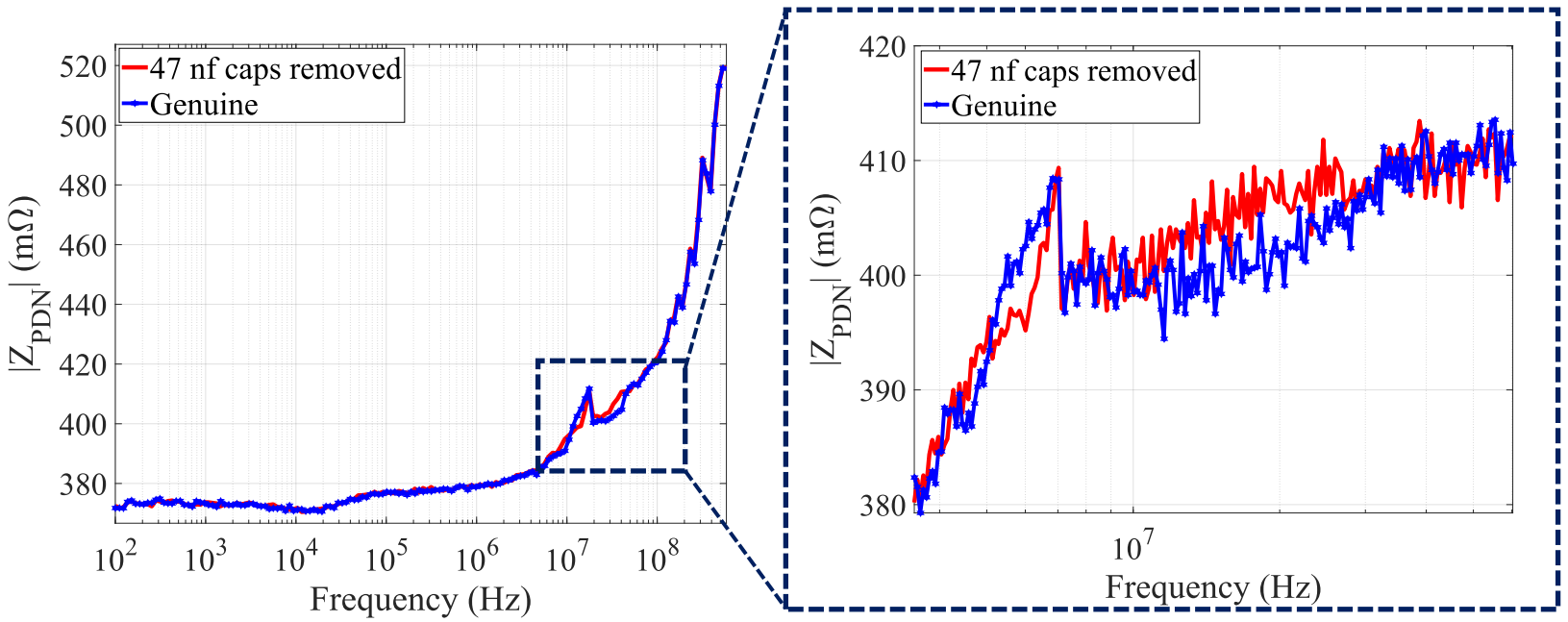




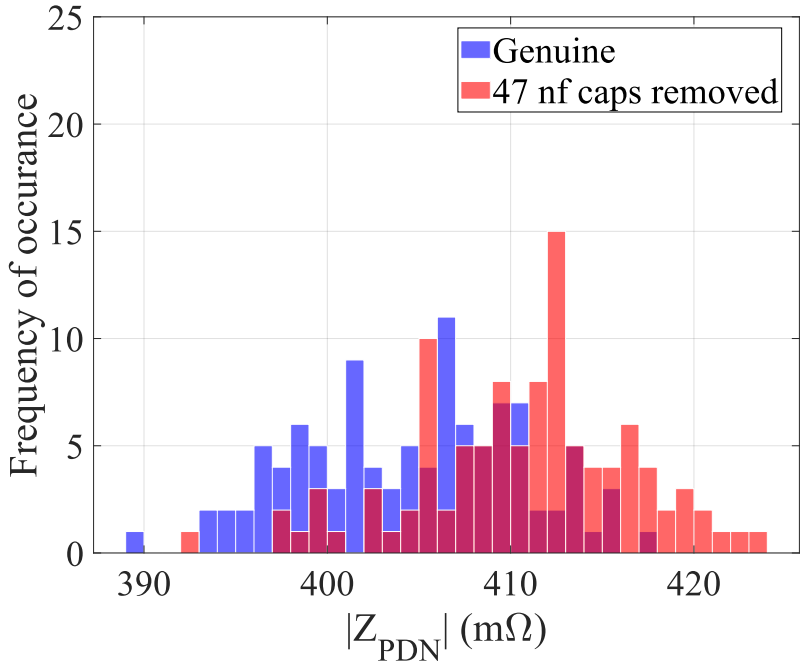
[2] T. Mosavirik, P. Schaumont, and S. Tajik, "ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection", IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2023).

Results for removing 47 nF capacitors

VERNAM LAB
Worcester Polytechnic Institute

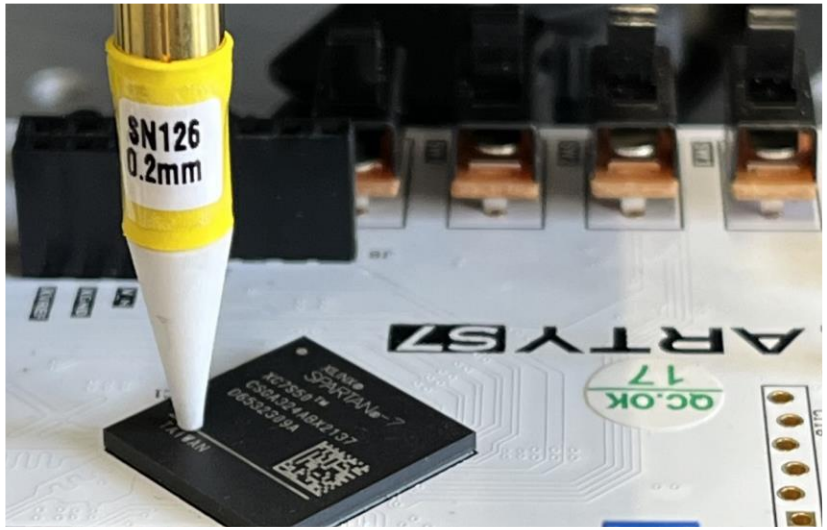


f= 39.90 MHz

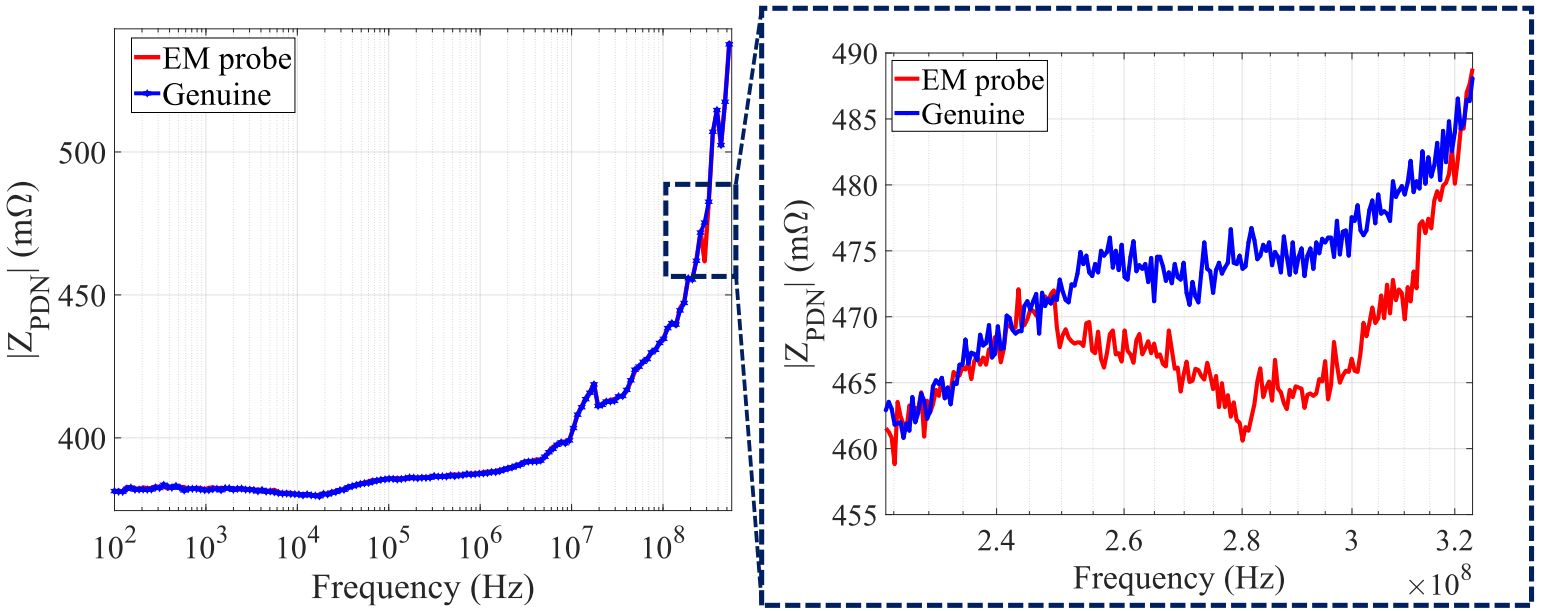


[2] T. Mosavirik, P. Schaumont, and S. Tajik, "ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection", IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2023).

Proximity of an EM Probe



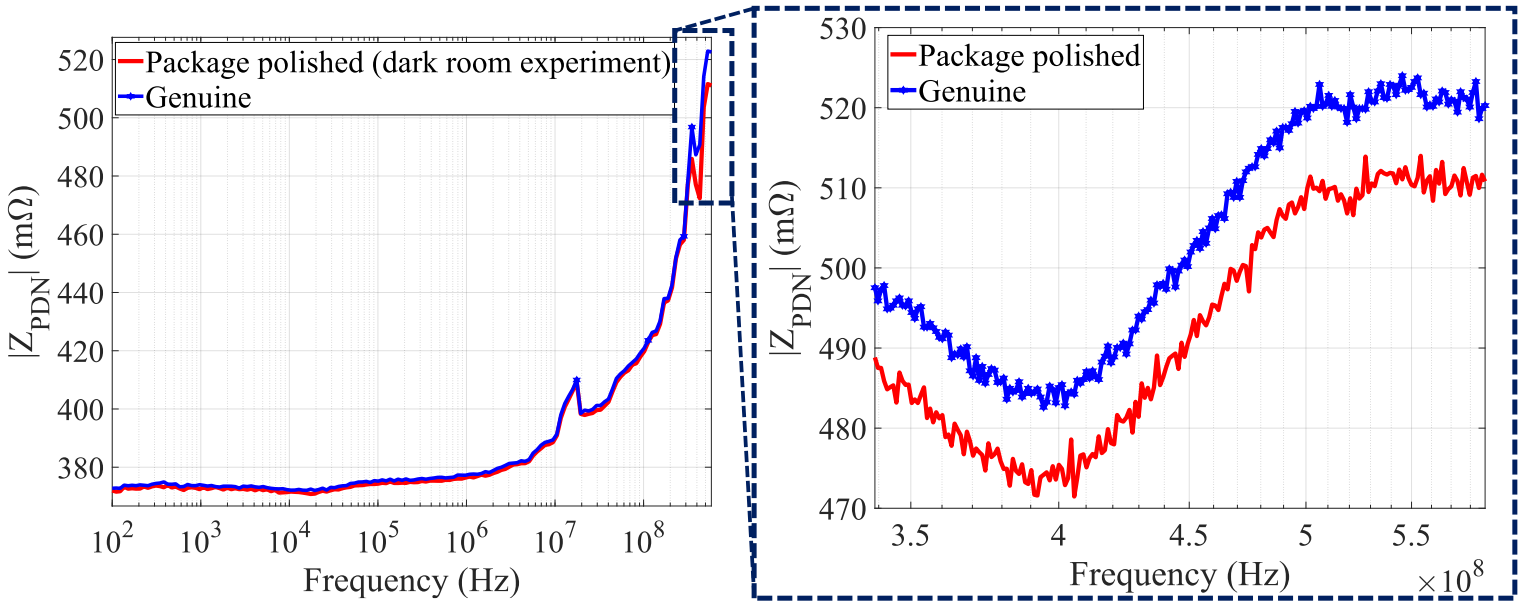
Placing an EM probe on top of the FPGA package.



[2] T. Mosavirik, P. Schaumont, and S. Tajik, "ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection", IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2023).

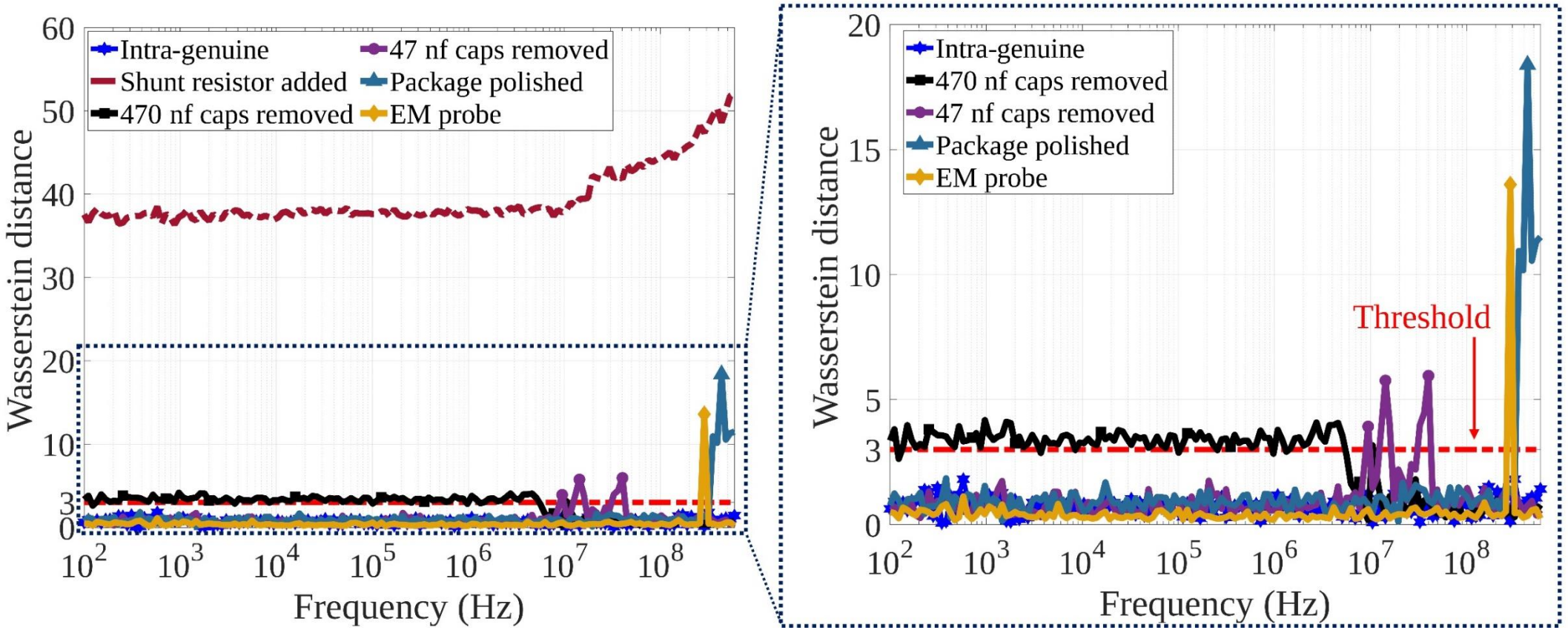
IC Package Polishing

Polished FPGA package



[2] T. Mosavirik, P. Schaumont, and S. Tajik, "ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection", IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2023).

Wasserstein metric



[2] T. Mosavirik, P. Schaumont, and S. Tajik, “ImpedanceVerif: On-Chip Impedance Sensing for System-Level Tampering Detection”, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES 2023).

Summary

Conclusion

- Our solutions make the verification generic and applicable to virtually all electronic systems.
- We converted the unique properties in the **power distribution network** (PDN) of a PCB into physical signatures.
- We used these hardware signatures, we can characterize the **entire system** from **board to chip level**, in different portions of the frequency band.
- The first solution, "ScatterVerif," is a holistic PCB verification framework based on the characterization of the PCBs' PDN. We show that different classes of physical attacks affect the overall impedance of a PCB differently in various frequency ranges. Hence, **the reflection response** of the PCB provides a unique hardware signature to differentiate between genuine and counterfeit/tampered samples by **a single measurement**.
- Experimental results from "ScatterVerif" show that even **genuine samples**, manufactured at **different facilities**, can be identified using the proposed approach.
- The on-chip impedance sensing (ImpedanceVerif) reveals different classes of tamper events from board to chip level, even environment-level tampering activities, such as the proximity of contactless EM probes to the IC package or slightly polished IC package.
- Self-contained verification method

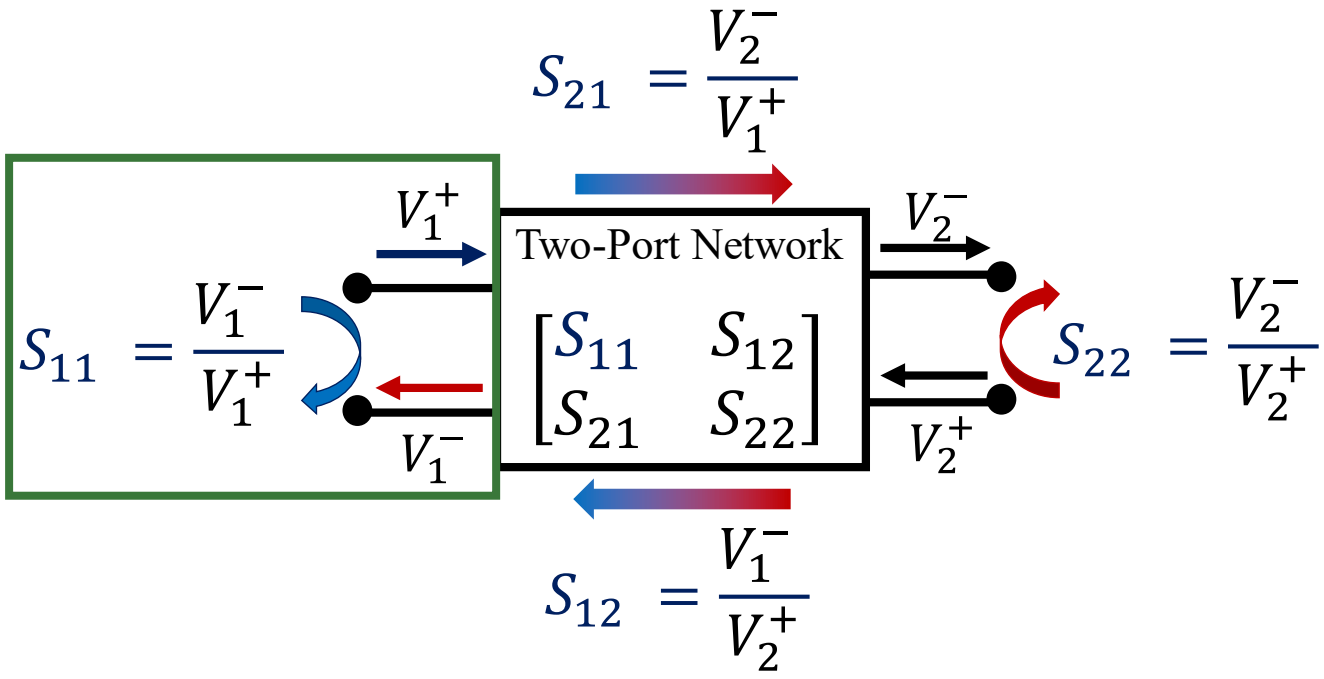
Acknowledgement

VERNAM LAB
Worcester Polytechnic Institute

- Dr. Shahin Tajik
- Dr. Patrick Schaumont
- Dr. Fatemeh (Saba) Ganji

Thank you for your attention!

Electrical echo



Scattering parameters measurement