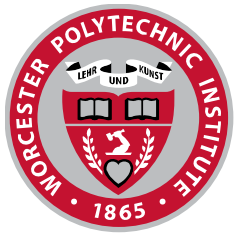
VERNAM LAB
Worcester Polytechnic Institute



WPI

BackMon: IC Backside Tamper Detection using On-Chip Impedance Monitoring

Tahoura Mosavirik
tmosavirik@wpi.edu

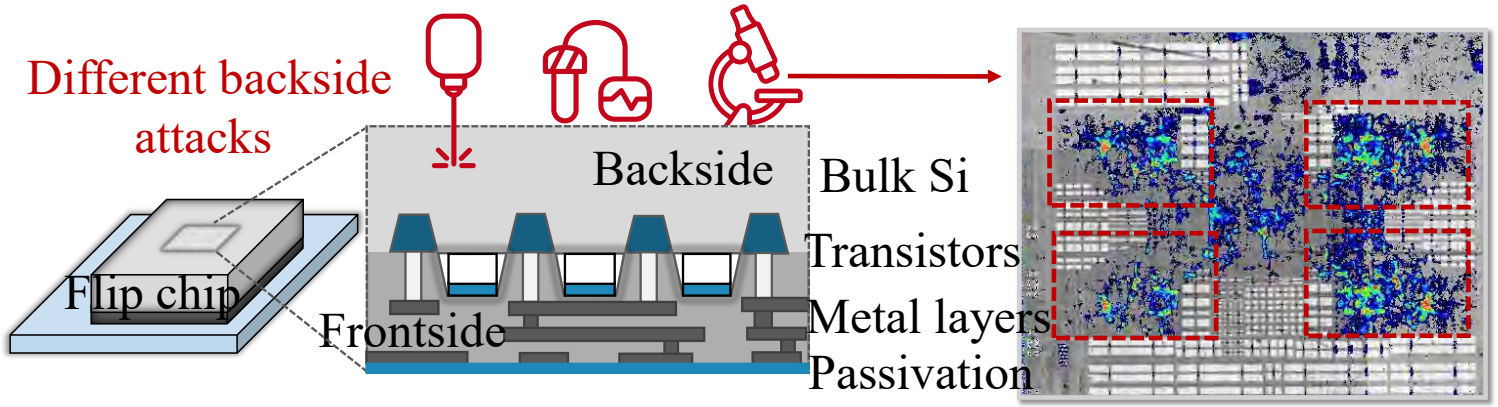
Advisor: Prof. Shahin Tajik

New England Hardware Security Day (NEHWS 2025),
April 18, 2025

IC backside security

Optical attacks

- More precision compared to conventional side-channel attacks
- Multiple interconnect layers obstruct the optical path to transistors on the IC frontside
- Active devices are directly accessible from the IC backside

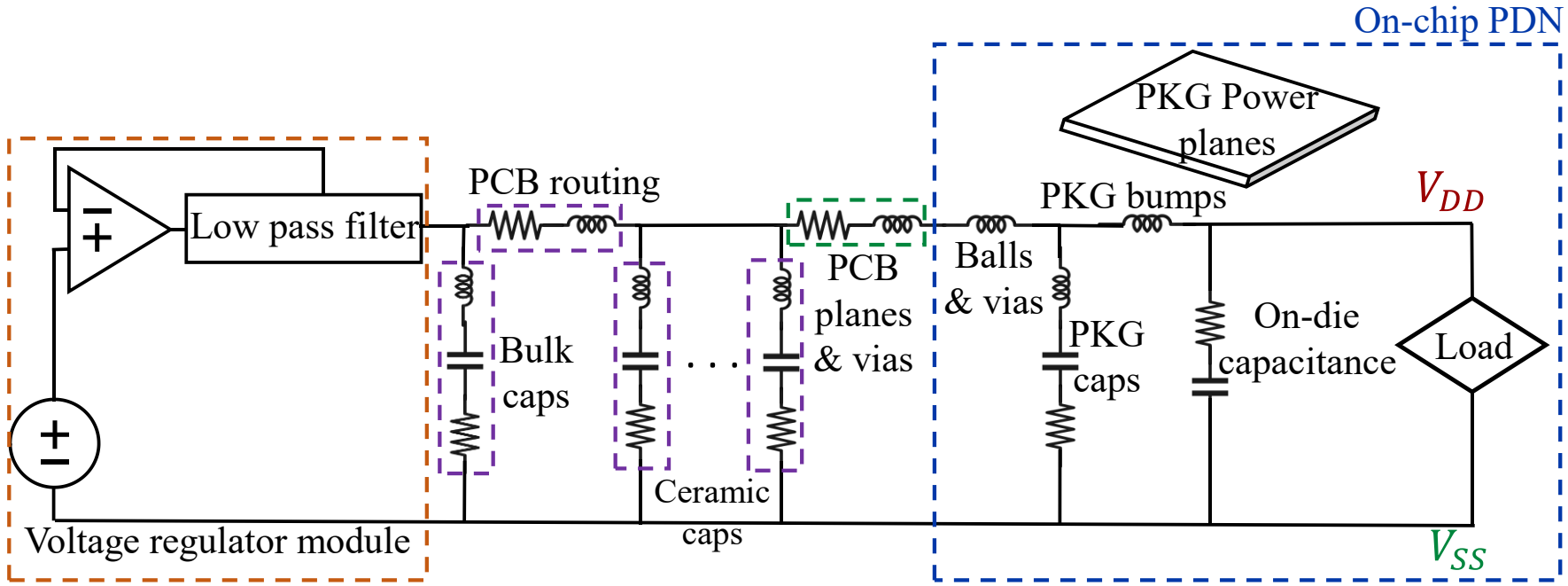


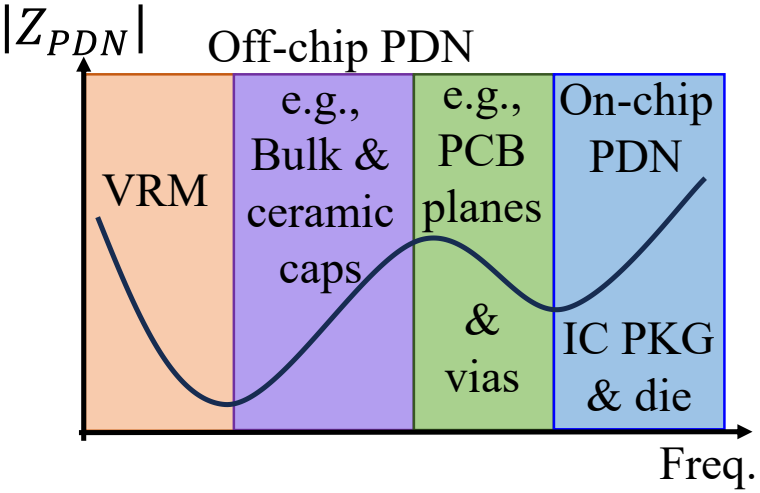
Cross-section view of a typical chip

Photon emission image of Zynq ultraScale+ processor

How the silicon backside can be used as an attack medium

Power distribution network (PDN)

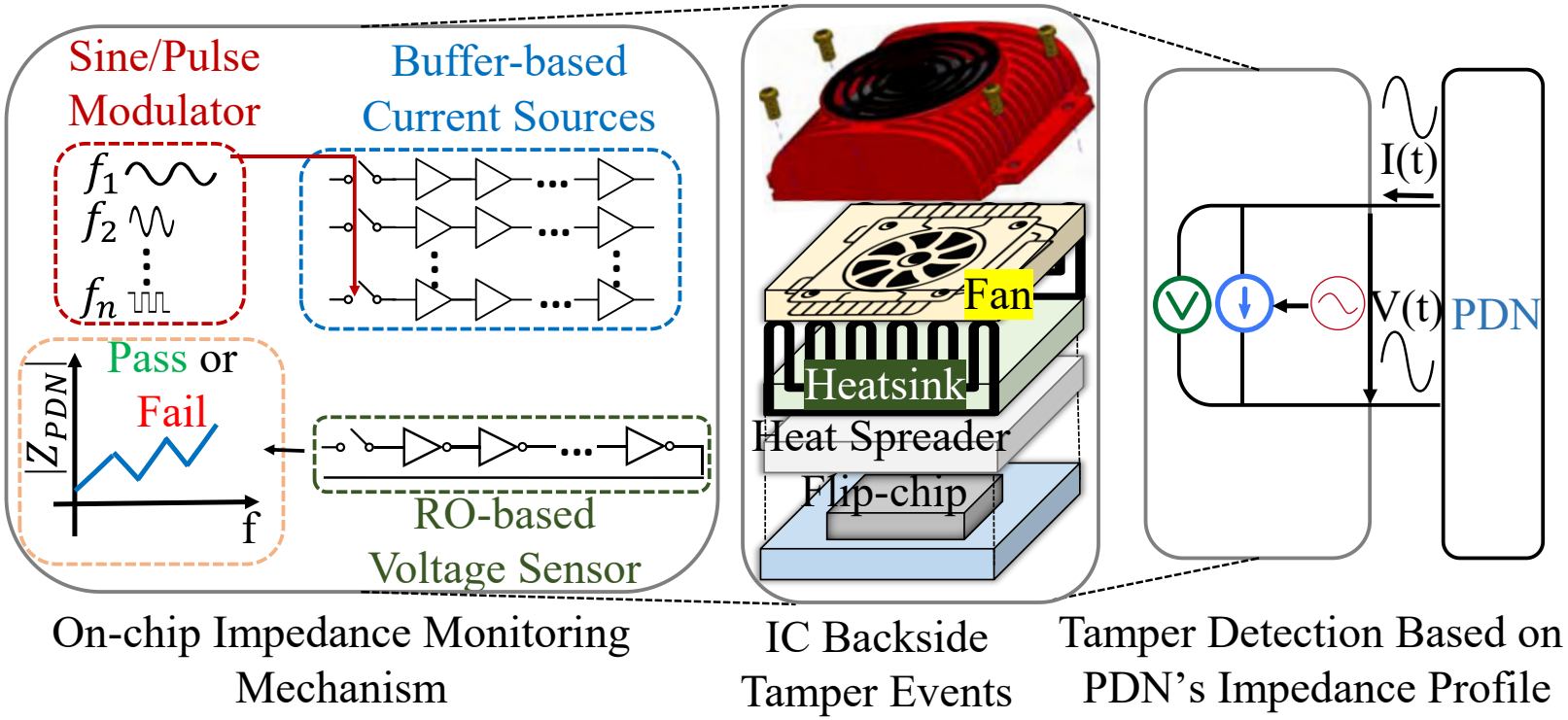




Equivalent RLC circuit model of the system's PDN and the contribution of different parts over frequency

Can we miniaturize this network analyzer on the chip?

Embedded network analyzer on FPGA



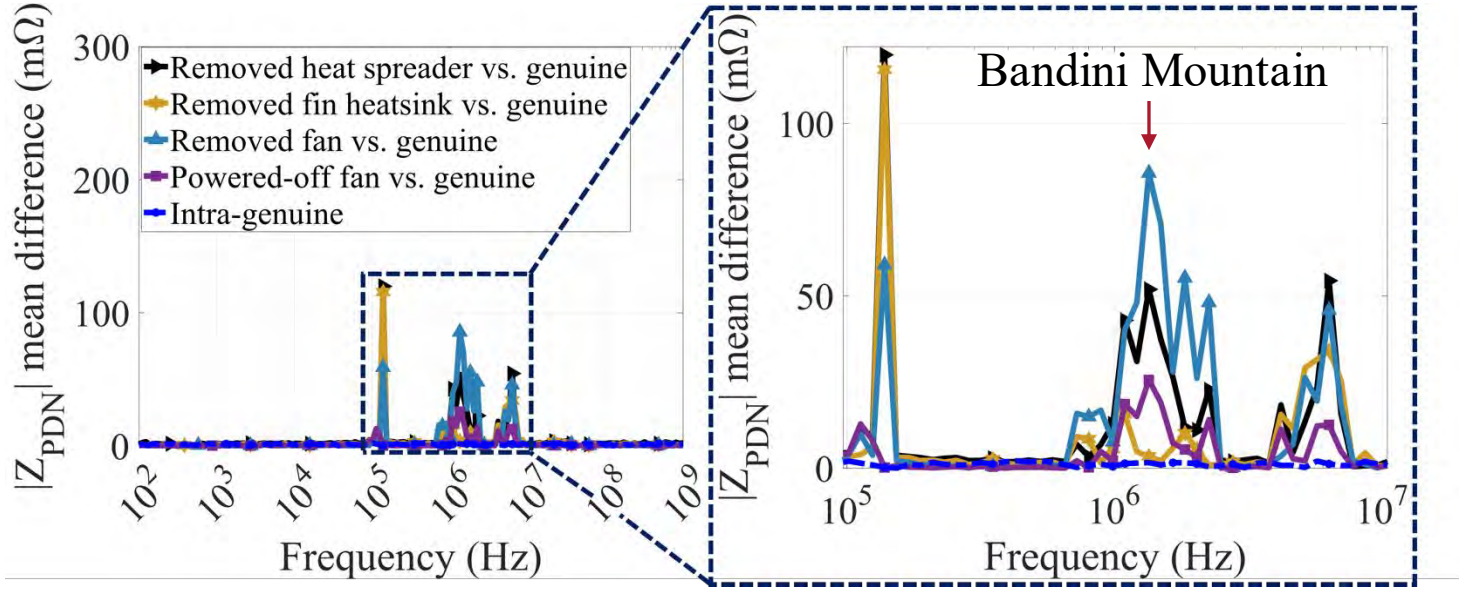
The proposed tamper detection methodology

Threat model

1) Genuine sample signatures are collected in an enrollment phase in a trusted environment at different temperatures and stored on the same chip
2) Detect the attacker's tampering attempt before performing optical attacks
3) Having physical access to the victim's board
4) Applicable to powered-on systems

IC backside tamper events

T= 25°C

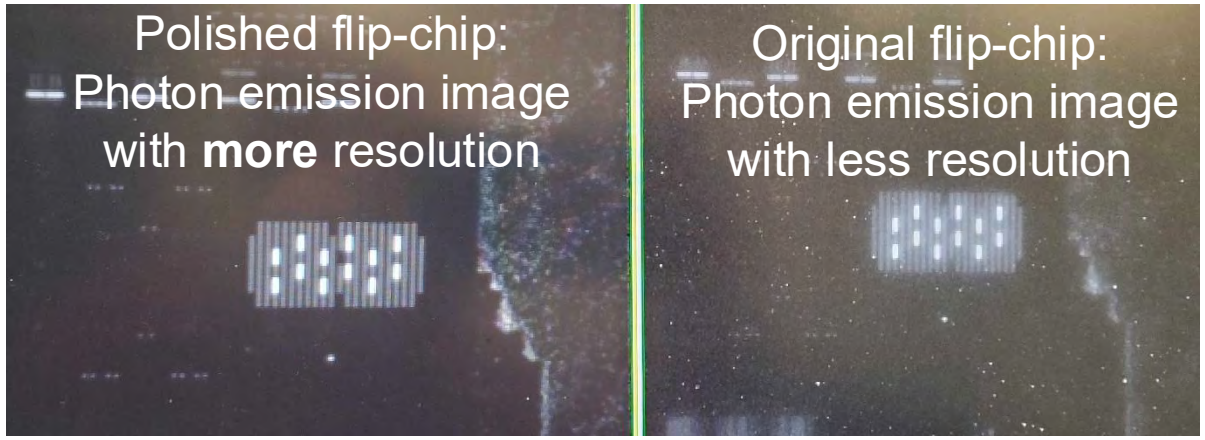


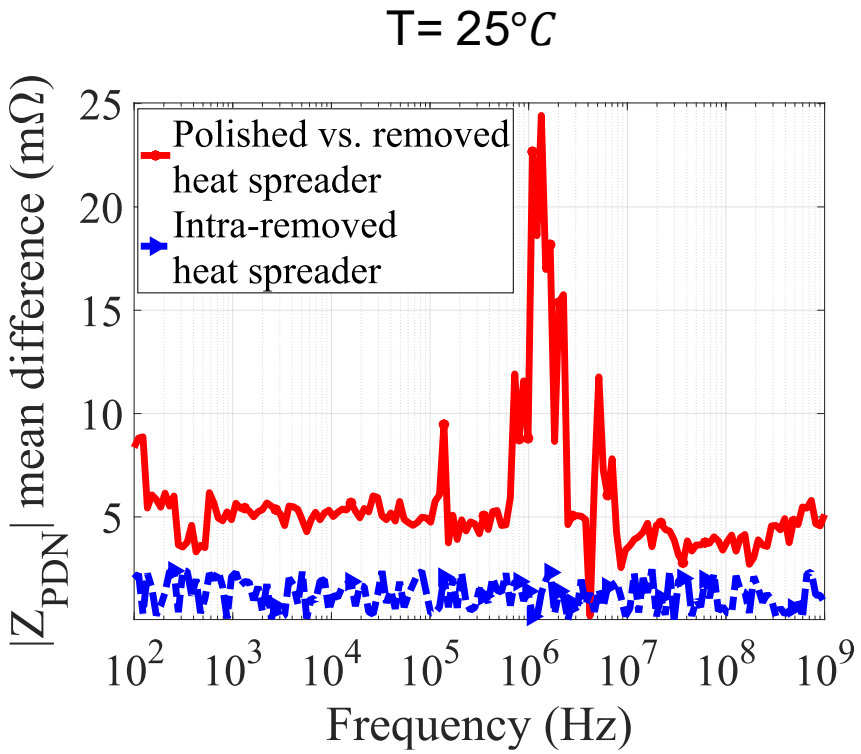
$$f_{Bandini} = \frac{1}{2\pi\sqrt{L_{PKG}C_{ODC}}}$$

Untouched sample (Genuine) | Removed fan | Removed fin heatsink | Removed heat spreader

Polishing IC backside

Polished IC backside (720 um thickness reduction)





Thank you for your attention!