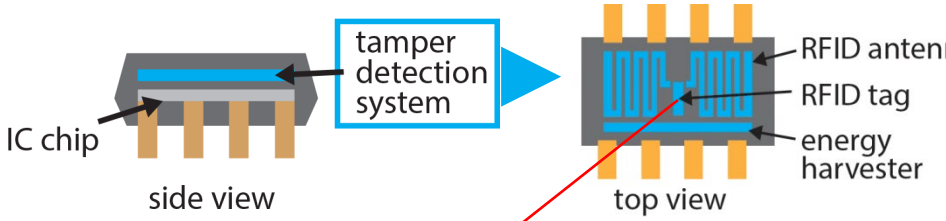
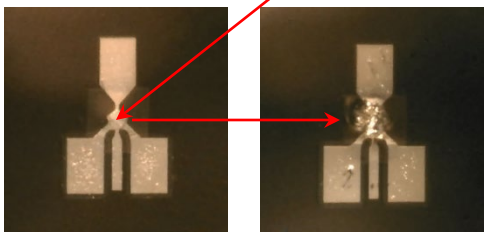
Wireless, Battery-less, Monolithic Tamper Detector for Semiconductor Chip Authenticity

USC Viterbi School of Engineering

Challenge:

- Loss of US Integrated Circuits (IC) industry due to counterfeiting ≈ $7.5 billion/yr
- Counterfeit ICs ← scavenged from printed circuit boards (PCBs) by heating PCBs to 250 – 400 °C (to melt the solder) and then banging PCBs against hard object (to dismount Ics
- lost revenue, increased failure risk in operationally critical systems, and security risks





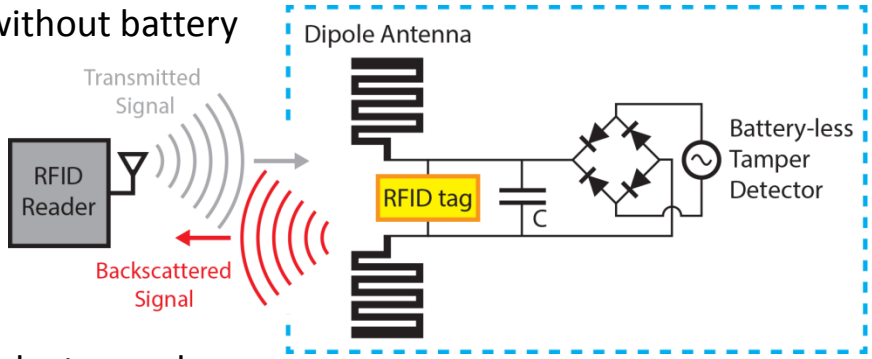
Cross-section of Tamper Detector

Scientific Impact:

- Piezoelectric voltage generators that produce voltage in response to tampering activities
- Film-bulk acoustic resonators (FBAR) that can be damaged by the voltage produced by the piezoelectric voltage generators and that can also be wirelessly interrogated
- Nozzle-less droplet ejectors capable of placing IC chips onto antenna-containing flexible substrates

Solution: Single-chip detector that can

- record any invasive semiconductor-chip-package tampering activity without battery
- be placed inside semiconductor chip packages through nozzleless droplet ejector
- be wirelessly interrogated without opening up semiconductor package



Broader Impact:

- Foundational technology for paradigm-shifting concept of individualized detection and recording of tampering activities to ensure authenticity of semiconductor chips
- Packaging technology based on droplet ejector
- Impacts semiconductor industry and high-value-product industries.

NSF CNS 1716953
Department of Electrical and Computer Engineering at University of Southern California
Prof. Eun Sok Kim (eskim@usc.edu)