SaTC:CORE: Medium: Introducing DIVOT: A Novel Architecture for Runtime Anti-Probing/Tampering on I/O Buses
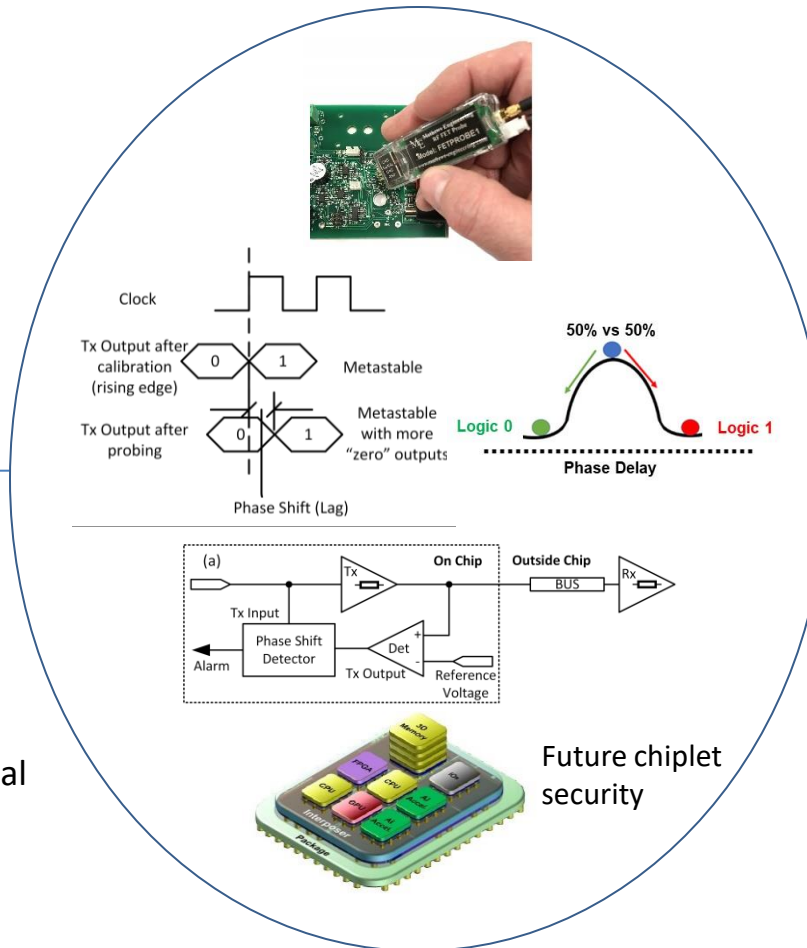
Challenge:

- Physical bus probing is a threat
- Encryption as a countermeasure imposes high overhead (latency and power)

Solution:

- Leverage existing data waveforms flowing on a bus to detect probing
- Detection works concurrently with normal data transfers on a bus

Future chiplet security

Scientific Impact:

- A runtime-accessible and CMOS-compatible hardware structure
- Integrating DIVOT with a variety of interconnecting buses will substantially reduce attack surface

Broader Impact and Broader Participation:

- Enhances hardware security of various computing platforms
- Design IPs will be generated that are likely to be transferred to the computer industry
- Enhance computer engineering curriculum