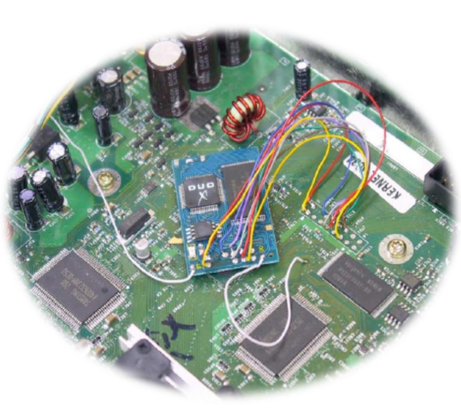
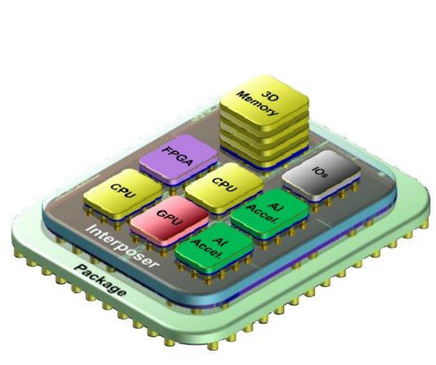
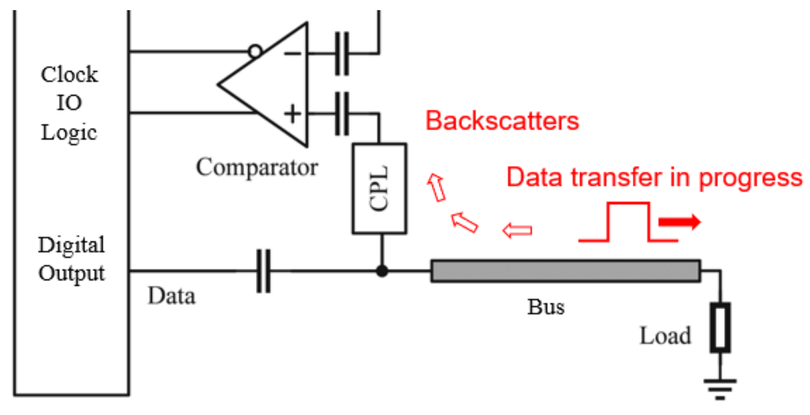
SaTC:CORE: Medium: Introducing DIVOT: A Novel Architecture for Runtime Anti-Probing/Tampering on I/O Buses

Tao Wei and Qing Yang, University of Rhode Island

https://www.nsf.gov/awardsearch/showAward?AWD_ID=2106750&HistoricalAwards=false







Key Problem:

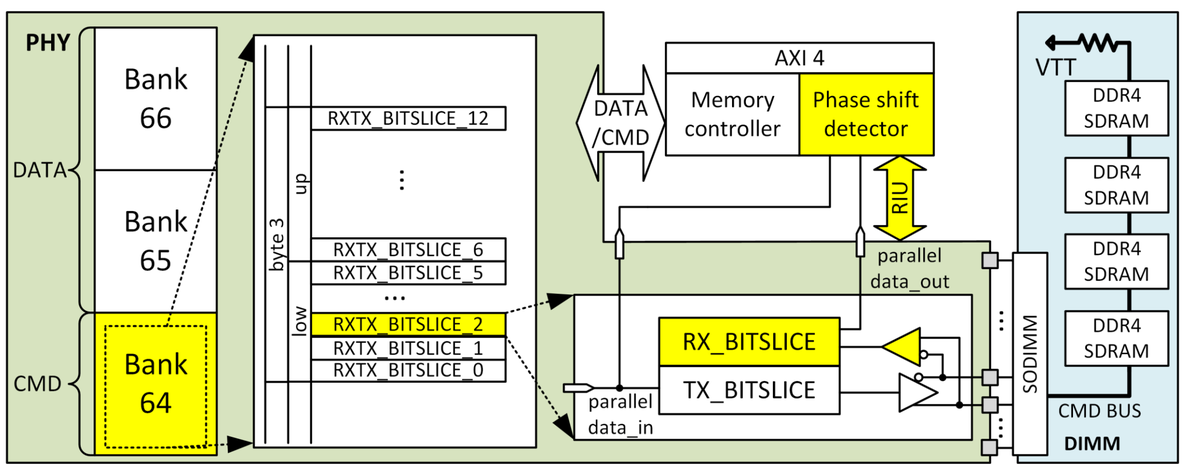
- An attacker can use physical probes to extract information from bus interconnections.
- Encryption technique (such as Intel SGX MEE) is effective but associated with high overhead in terms of latency and power.

Scientific Impact:

- A runtime-accessible and CMOS-compatible hardware structure in the form of silicon IP can be integrated into various IO circuitry for probing detection
- Integrating DIVOT with a variety of interconnecting buses will substantially reduce attack surface
- Could be used to protect future chiplet interconnections

Technical Approach:

- Leverage existing data waveforms flowing on a bus to detect probing
- Detection works concurrently with normal data transfers on a bus
- Detection circuit can be integrated in standard protocol (e.g., DDR4 shown on right)



Broder Impact:

It represents a universal countermeasure to fight against many physical probing/tampering threats and significantly enhances hardware security of various computing platforms ranging from servers to embedded computers in mobile devices and IoTs (Internet of things).

Broader Impact (Education and Outreach):

- Provide several undergraduate students summer intern opportunity to work on digital design
- Research results will be incorporated into our computer engineering curriculum.

Broader Impact and Broader Participation

- 5 undergraduate students were provided the opportunities to work on digital design
- 2 local high school students are involved in research activities