A Quantitative Framework for Analyzing and Mitigating Microarchitectural Side Channels

 # 2046359

Mengjia Yan (MIT EECS)

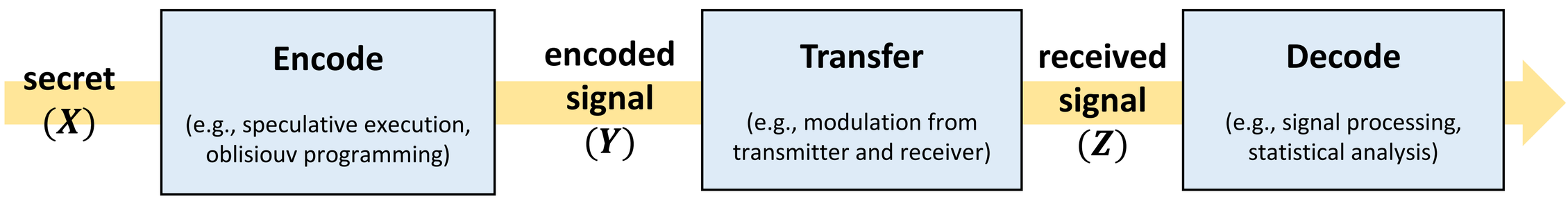
<u>Challenges:</u>

- uArch side-channel attacks breach processor security
- No existing tool for designing quantitative defense mechanisms

Solution:

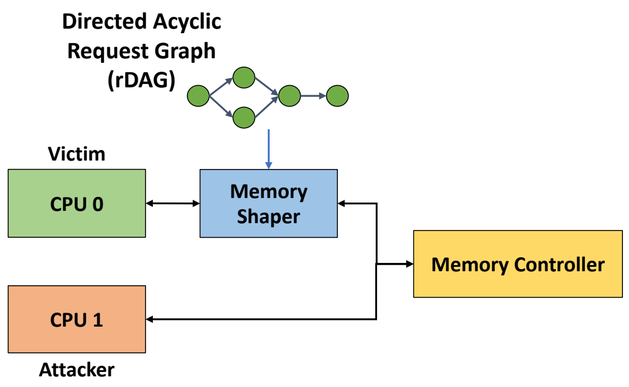
- A new way to formulate uArch side channels as a communication problem
- Construct precise quantitative models for uArch structures

uArch Side Channel Communication Model



Selected Projects:

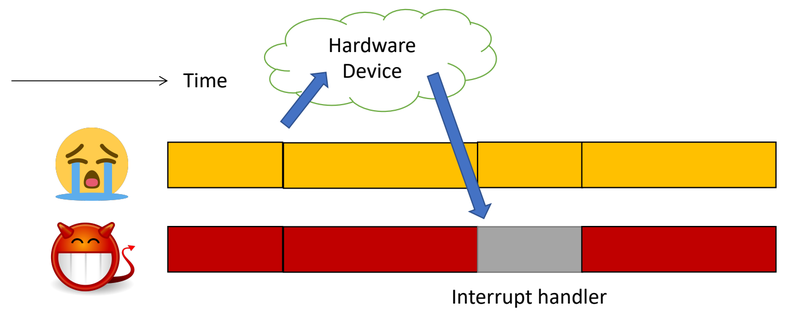
DAGguise: Mitigating Memory Controller Side Channels
(ASPLOS'22)



DAGguise achieves:

✓ **Formally-Verified Security**
and
✓ **Good Performance**

There's Always a Bigger Fish: A Clarifying Analysis of a Machine-Learning-Assisted Side-Channel Attack *(ISCA'22)*



- Discovered prior work misinterpreted the root cause of cache-occupancy attacks
- The actual root cause is interrupt side channels

Media Coverage: NSF Research News, MIT News

<u>Scientific Impact:</u>

- Bridge the gap between two research fields, computer architecture and information theory in studying side channels
- A quantitative framework to enable productive trade-offs between security and performance

<u>Broader Impact and Broader Participation:</u>

- Tutorials on uArch side channels @ISCA'22 (https://sites.google.com/view/mad-isca22)
- Advanced undergrad course on "Secure hardware Design" @MIT (http://csg.csail.mit.edu/6.888Yan/cal/)