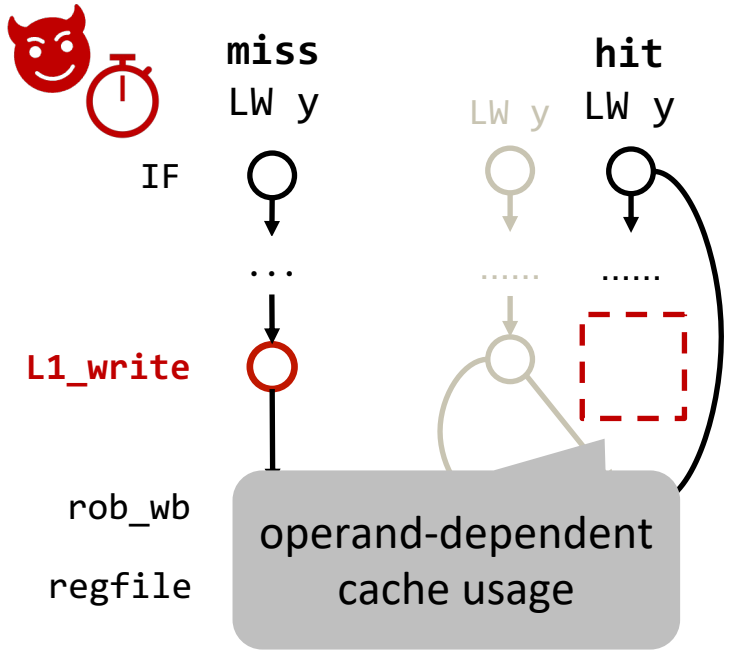
Formal Characterization of Hardware Transmitters for Secure Software and Hardware Repair

Yao Hsiao[1], Christopher W. Fletcher[2], Caroline Trippel[1]

[1]Stanford University, [2]University of Illinois Urbana-Champaign

- **Problem:**
  - Hardware side-channel attacks exploit unsafe instructions (i.e., transmitters) whose execution creates operand-dependent hardware resource usage that can be observed via some means (e.g., exec. time)



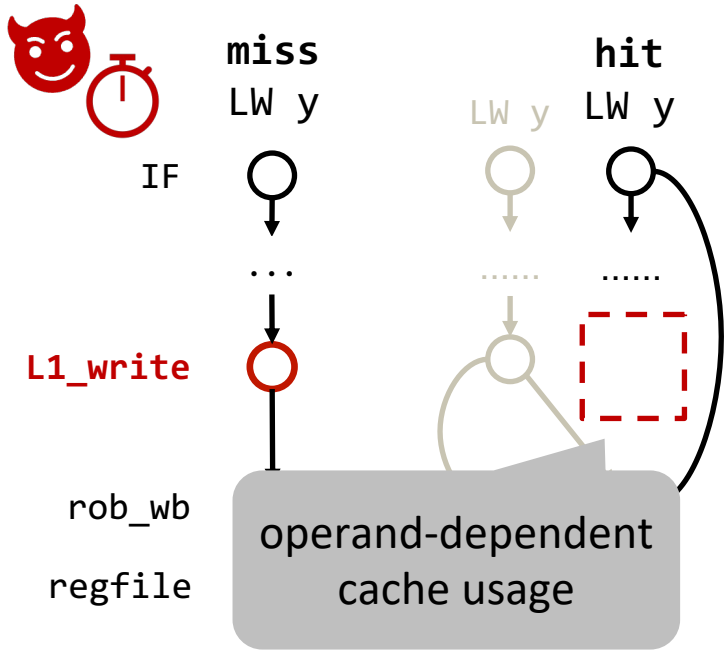
[1]Jose Vicarte et al. "Opening Pandora's Box: A Systematic Study of New Ways Microarchitecture Can Leak Private Data". In: *ISCA'21*.

Formal Characterization of Hardware Transmitters for Secure Software and Hardware Repair

Yao Hsiao[1], Christopher W. Fletcher[2], Caroline Trippel[1]

[1]Stanford University, [2]University of Illinois Urbana-Champaign

- **Problem:**
  - Hardware side-channel attacks exploit unsafe instructions (i.e., transmitters) whose execution creates operand-dependent hardware resource usage that can be observed via some means (e.g., exec. time)
  - Mitigating such attacks requires identifying all unsafe instructions on a given RTL design
  - Many unsafe instructions can be latent in microarchitecture[1]



[1]Jose Vicarte et al. "Opening Pandora's Box: A Systematic Study of New Ways Microarchitecture Can Leak Private Data". In: *ISCA'21*.

τsynth: Automated approach and tool for discovering and characterizing unsafe instructions on an input RTL design

- **Methodology:**
  - Exhaustive exploration of instruction execution paths using a combination of formal property generation and model checking
- **Results:**
  - Identifies 15 timing-differentiable transmitters on RISC-V CVA6
- **Ongoing work:**
  - Extracting data that a transmitter depends on to exhibit variable execution