Formal Characterization of Hardware Transmitters for Secure Software and Hardware Repair

Yao Hsiao¹, Christopher W. Fletcher², Caroline Trippel¹
¹Stanford University, ²University 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)

---

Formal Characterization of Hardware Transmitters for Secure Software and Hardware Repair

Yao Hsiao\textsuperscript{1}, Christopher W. Fletcher\textsuperscript{2}, Caroline Trippel\textsuperscript{1}

\textsuperscript{1}Stanford University, \textsuperscript{2}University of Illinois Urbana-Champaign

\textbf{Problem:}

\begin{itemize}
  \item 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)
  \item Mitigating such attacks requires identifying all unsafe instructions on a given RTL design
  \item Many unsafe instructions can be latent in microarchitecture\textsuperscript{1}
\end{itemize}

\textsuperscript{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

---

65 execution paths for division op → unsafe 😞