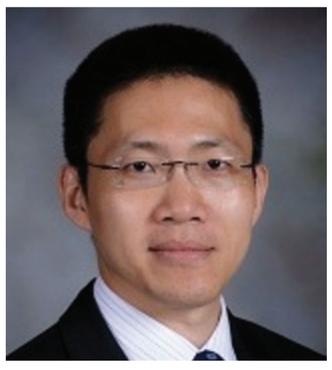
A Principled Approach to Modeling and Analysis of Hardware Fault Attacks on Embedded Software

Chao Wang
University Southern California

Patrick Schaumont
Worcester Polytechnic Institute



Project page: http://???

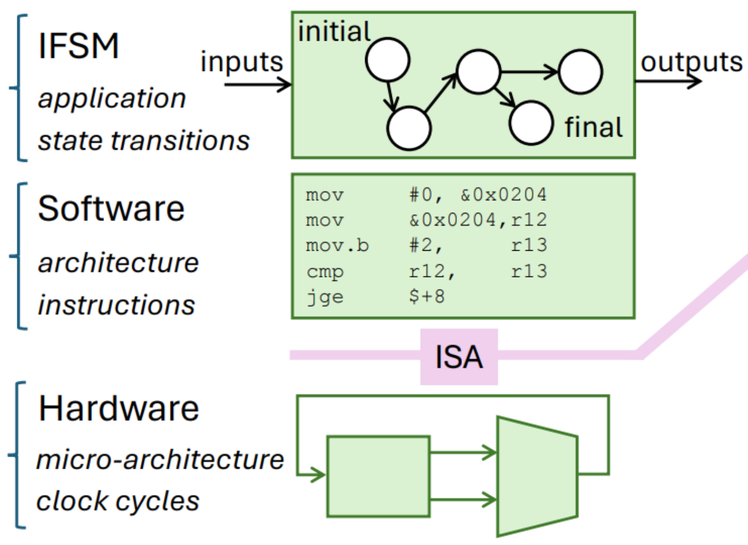
Problem Statement

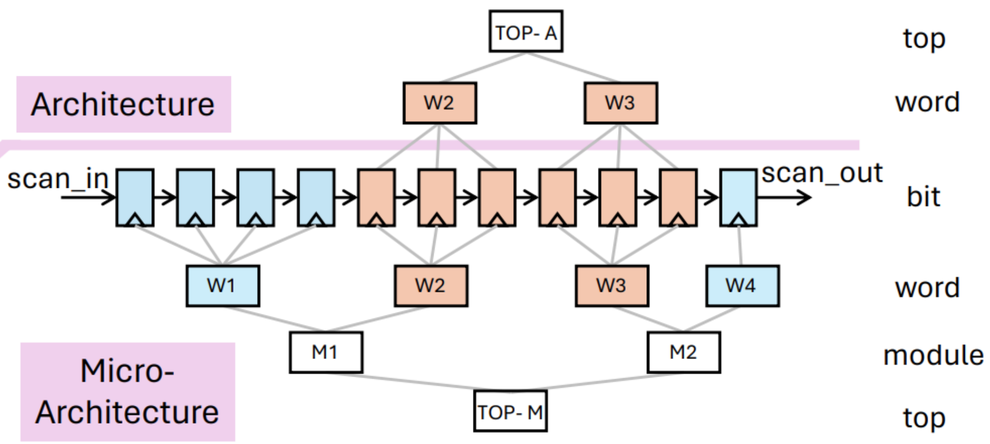
The impact of hardware faults on software is poorly understood. An improved fault model is needed to apply formal methods to program verification, synthesis, and repair. We must build a tighter link between hardware design and software verification, and a better understanding of hardware threats to software.

Background

Software execution as an Intended FSM

- Micro-architecture state of the CPU covers all registers
- ISA hides some registers, leading to a hierarchy of words in the state





Objective

- *Hardware:* Model injected faults as Sane/Weird Machines used by formal tools for software
- *Software*: Develop novel formal tools to verify and repair software code under fault attacks

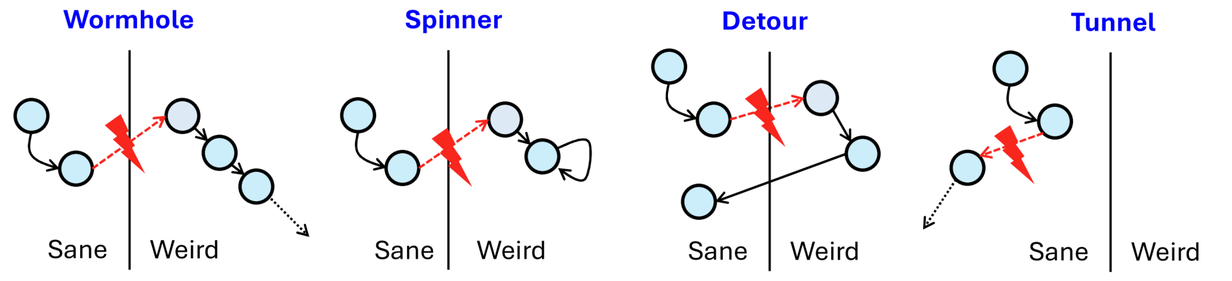
Approach

- *Hardware*: Study empirically the impact of hardware faults on ISA using hardware simulation
- *Software*: Use symbolic methods to quantitatively verify programs while considering fault attacks

Scientific Impact

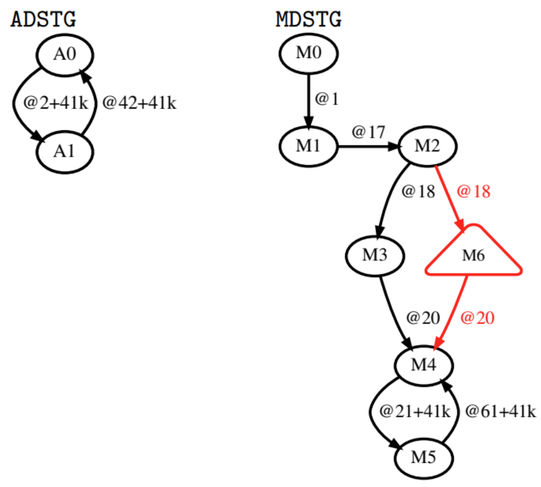
- Realization in ASIC (180 nm)
  6 identical MSP430 cores
- Publication
  [CHES 2024] Fault Detective: Explainable to a Fault, from the Design Layout to the Software
  [POPL 2025] An Incremental Algorithm for Algebraic Program Analysis

Major Finding: Weird machine does exist!



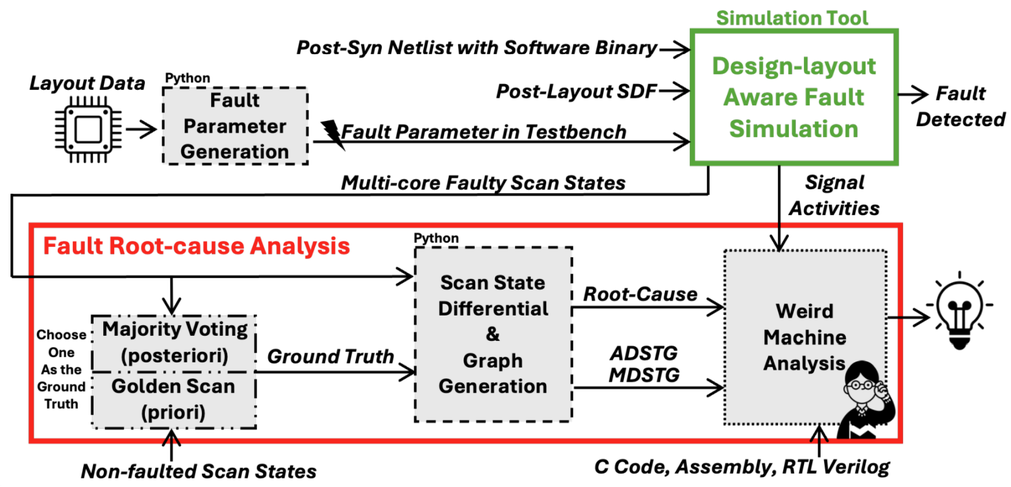
Root-cause of a *Detour* fault:

```
IMPLEMENTATION
f034:  mov     &0x0200,r12
f038:  cmp     #2,     r12
f03a:  jz      $+100
f03c:  mov.b   #2,     r13
f03e:  cmp     r12,    r13
f040:  jl      $+34
f042:  cmp     #0,     r12
f044:  jz      $+54
f046:  cmp     #1,     r12
f048:  jz      $+68
...
f07a:  mov     #0,     &0x0028
f07e:  mov     &0x0026,r12
f082:  cmp     #1,     r12
f084:  jnz     $-58
```




```
FAULT ROOT CAUSE
CORE4:
openmsp430_0
-frontend_0
  inst_alu     028
```

Design-layout ware simulation framework



Broader Impact on Society

- Enabling novel chip design and better countermeasures
- Improving the reliability and security of software

Broader Impact on Education

- Courses on secure chip design (WPI) and software verification (USC)
- Trained 2 PhD students and many undergraduate students

Broader Impact on Participation

- …
- Keynote talk on research career at SPLASH 2024 Doctoral Symposium