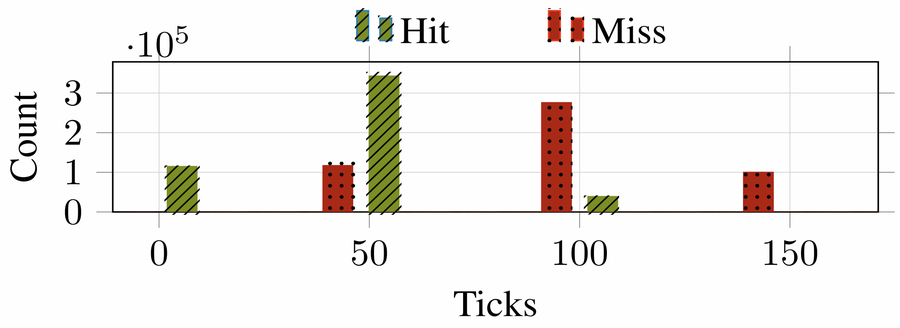
RISCy Cache Coherence: Timer-Free Architectural Cache Attacks via Instruction/Data Cache Incoherence

Fabian Thomas, *Michael Schwarz*

Modern CPUs and Operating Systems Limit Timer Resolution



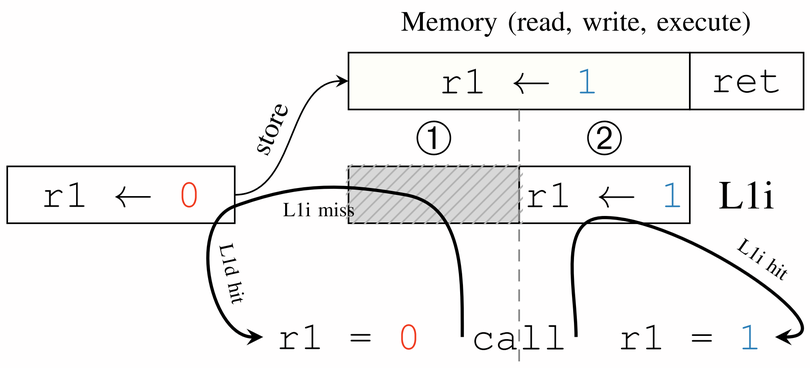
Flush+Reload on Qualcomm Snapdragon X1 (2025)

Idea: Exploit Instruction/Data Cache Incoherence as Side Channel

Building Block 1:
Leak I-cache state via
I/D-Cache Incoherence

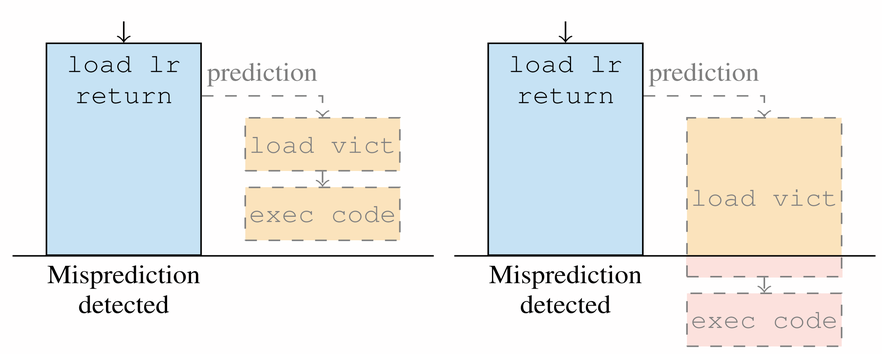
Building Block 2:
Transfer cache state of
D-cache line to I-cache line

Building Block 1: Architectural I-Cache State Leakage



Observation: code in I-cache ⇔ r1 = 1

Building Block 2: Cache-State Transfer Gadget



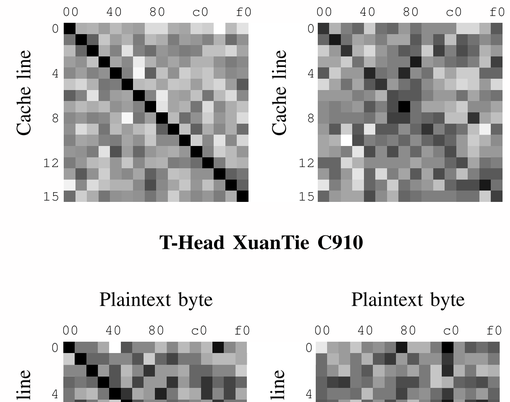
Observation: victim in D-cache ⇔ attacker code in I-cache

I²SC: Timer-Free D-Cache State Leakage on 12 Microarchitectures Across 3 RISC Architectures

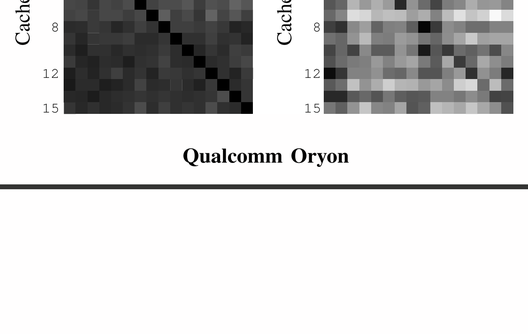
ARM											RISC-V				LoongArch
Arm							Q	H	Apple		T-Head			S	Loongson
◐ Cortex-A520	◑ Cortex-A72	◐ Cortex-A73	● Cortex-A76	● Cortex-A78	● Cortex-A720	● Cortex-A725	● Cortex-X4	● Neoverse-N1	● Oryon	● Kunpeng Pro	● Icestorm	● Firestorm	○ C906	◐ C908	● C910	◐ X60	● 3A5000-HV
			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓		✓

◐ = B1 works; ◑ = B2 works; ● / ✓ = I²SC works.
Q = Qualcomm; H = Huawei; S = SpacemiT.

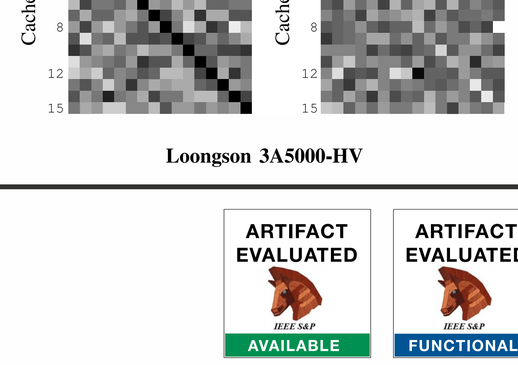
- 12 microarchitectures
- 3 RISC architectures:
  ARM, RISC-V, LoongArch
- Up to 30% lower error rate
  than Flush+Reload
- Timer-free side-channel attacks:
  - AES key recovery
  - Spectre
  - Touch-event timing leakage
    on Android (Pixel 9)



T-Head XuanTie C910



Qualcomm Oryon



Loongson 3A5000-HV

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

https://s.roots.ec/riscy

ARTIFACT EVALUATED
IEEE S&P
AVAILABLE

ARTIFACT EVALUATED
IEEE S&P
FUNCTIONAL