Revisiting Effects of Spectre-Meltdown Security Patches (Paper #16)

Yectli A. Huerta
University of Minnesota Supercomputing Institute

David J. Lilja
Department of Electrical and Computer Engineering
University of Minnesota
Minneapolis
Patches and Possible effects

- Security patches have potential performance effects
- Concerns with Spectre-Meltdown fixes
- Previous works showed performance effects were small
- We showed relative effects on the system in term of Top-Down metrics
Spectre/Meltdown Attacks

- Meltdown
- Spectre
Effect of Security Fixes

- Permanent patch
  - spectre Variant 1
- dynamic patches
  - Spectre Variant 2
  - Meltdown, variant 3
The Top Down Method

- Was uop allocated?
  - Yes
  - No
    - Did the uop retire?
      - Yes
        - Retiring
      - No
        - Bad Speculation
  - No
    - Was a BackEnd stall encountered?
      - Yes
        - FrontEnd Bound
      - No
        - BackEnd Bound
Purchasing Power Parity

- It’s been used to compare different currencies
- Most notable example is the Big Mac Index.
  - Big Mac comparison: in the US ($3.57) and Brazil (7.50 Reales).
  - 1.58 is the currency exchange rate.
    - $7.50 / $3.57 = 2.10
    - \((2.10 - 1.58) \times 100 / 1.58 = 32.91\%\)
Purchasing Power Parity

. In terms of PPP, currencies can be
  . Overvalued
  . Undervalued
Purchasing Power Parity

\[ PPP_{\text{Exchange\_Rate}} = \frac{CPU_{\text{clk}}}{CPU_{\text{clk_{baseline}}}} \]  

(3)

\[ PPP = 100 \times \left( \frac{Metric}{Metric_{\text{baseline}}} \right) - \frac{PPP_{\text{Exchange\_Rate}}}{PPP_{\text{Exchange\_Rate}}} \]  

(4)
Purchasing Power Parity

- When PPP is applied to performance metrics
  - Currency can be number of cycles
  - Product is a performance metric
  - PPP normalized percentage rates
    - Can be close to 0%
    - Be negative
      - more cpu cycles required when compared to the the baseline
    - Be positive
      - fewer CPU cycles required when compared to the baseline
Experimental Setup

- Used SPEC OMP2012
- Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz with 8 cores per socket, 2 threads per core
- Centos 7.6
- Compared
  - Intel 2021.1 compiler suite
- Patches were enabled/disabled by adding a 1 or 0 in
  - /sys/kernel/debug/x86/ibrs_enabled
  - /sys/kernel/debug/x86/retp_enabled
  - /sys/kernel/debug/x86/pti_enabled
Runtimes
350.MD Top-Down Results for Bad Speculation
350.MD Retiring Results
Take Aways

- PPP normalized metrics make it possible to identify relative differences between rates
- It makes it possible to distinguish between similar rates
- Rates that are different can be amplified or reduced
Conclusions

- We showed that bottleneck profiles can differ
- We showed that relative rates can vary significantly
- We highlighted trends and differences in metrics