Replikácia častí publikácie Platypus

Patrik Németh
(xnemet04)

Platypus

- **Množina exploitov využívajúca výkonnostný postranný kanál**
- **Neprivilegovaný prístup k čítačom**
- **Nové systémy ošetrené proti útokom**
- **Stále vykonateľné so zvýšenými právami**

RAPL (Running Average Power Limit)

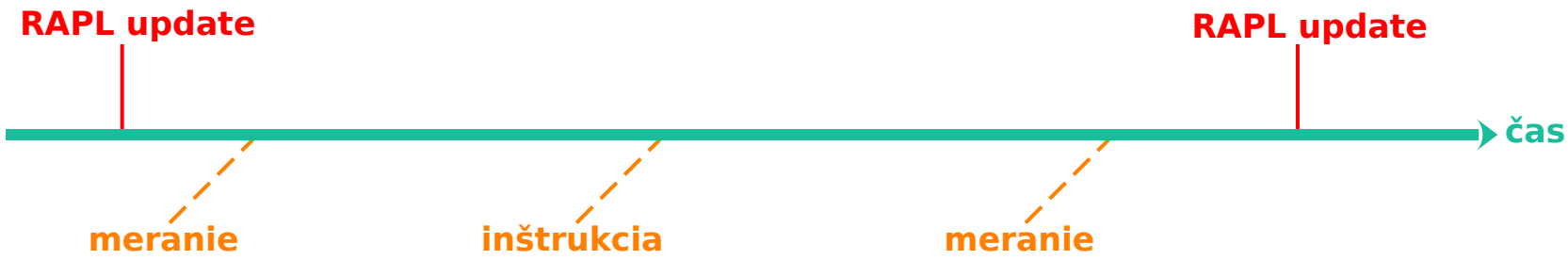
- **Systém čítačov sledujúcich spotreby CPU**
- **Rôzne domény:**
  - core: jadro procesora
  - package: obvykle procesorový soket
  - DRAM: pamäť
- **Perióda aktualizácie okolo 1ms**

Potrebné súčasti pre vykonanie experimentov

- **Prístup k časovaču na systéme s dobrým rozlíšením**
  - Time Stamp Counter (TSC)
- **Inline assembly v C/C++**
  - `asm volatile ("xor %0, %1" : "=r"(a) : "r"(b));`
- **Prístup k RAPL čítačom**
  - Powercap či priamy prístup k registrom

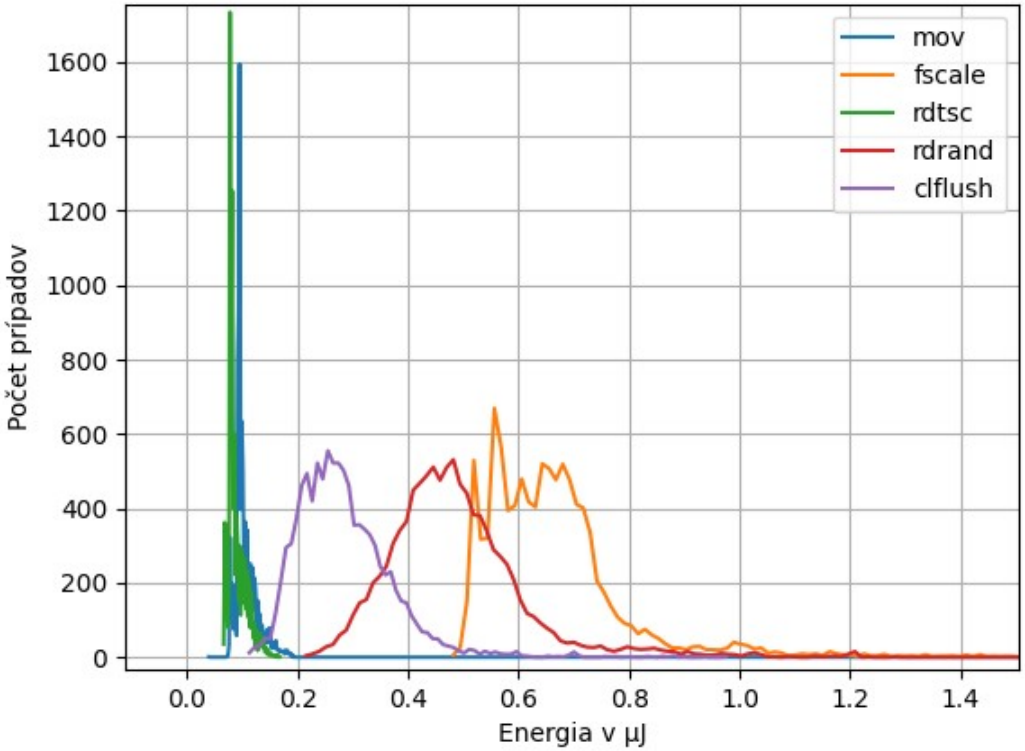
Meranie spotreby inštrukcií

- **Pomalá aktualizácia RAPL**
  - Vykonať jednu inštrukciu mnohokrát
- **Jedno meranie nestačí pre vytvorenie profilu inštrukcie**
  - Vykonať mnohonásobné vykonanie inštrukcie… mnohokrát

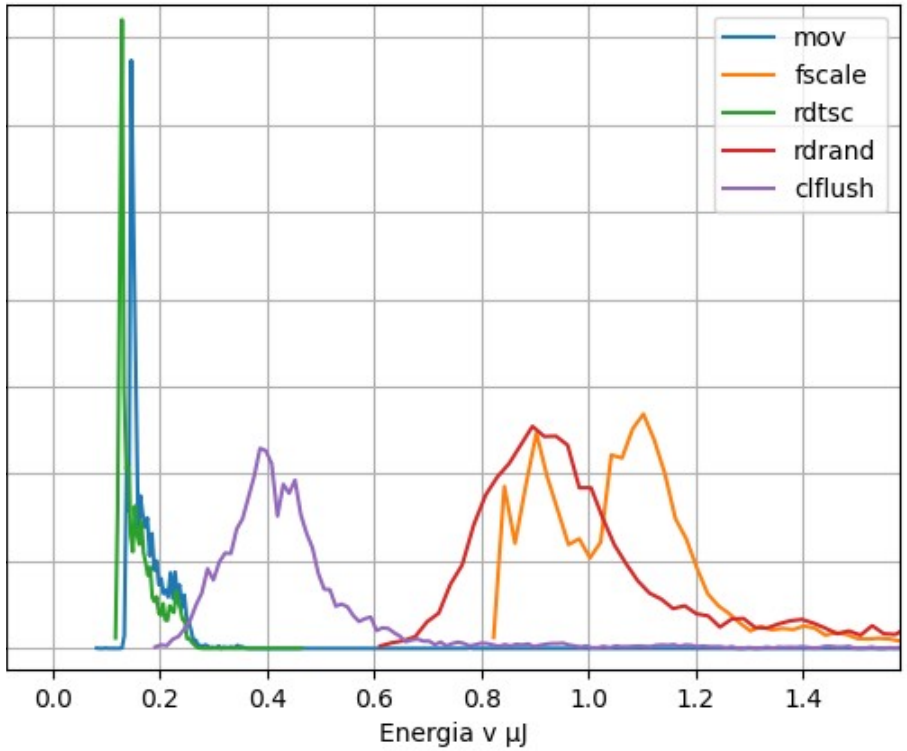


Rozlišovanie inštrukcií

core doména



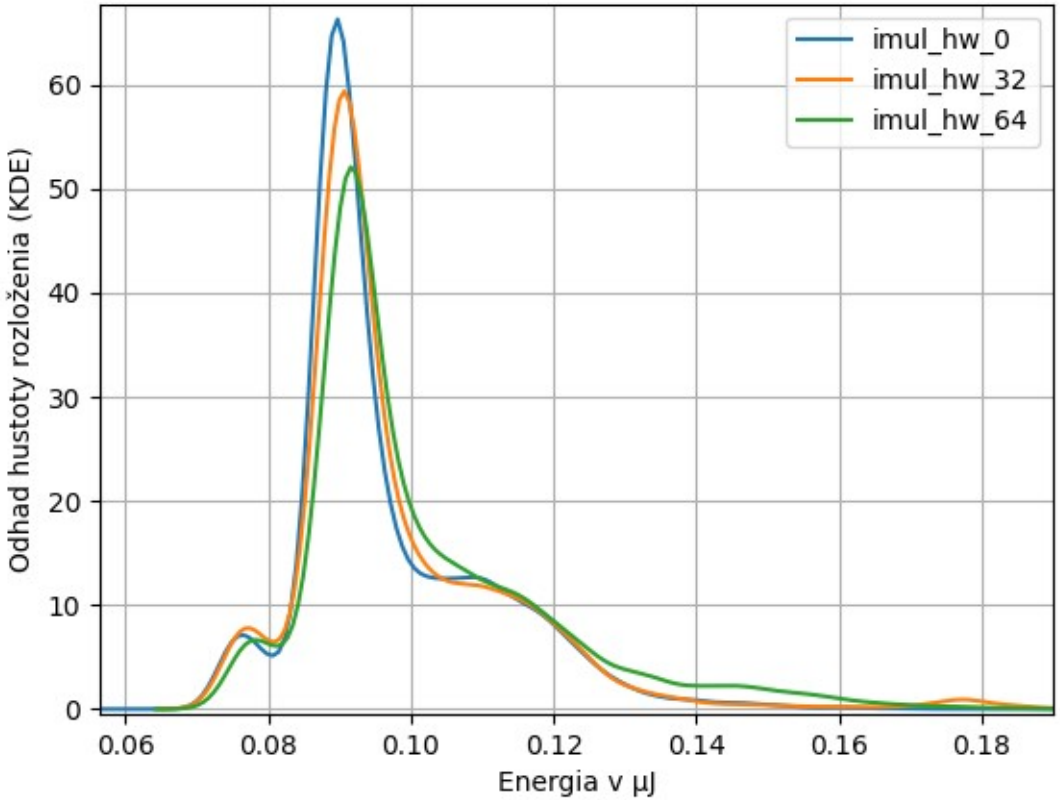
package doména



Rozlišovanie operandov

- **Na základe Hammingovej váhy**
  - Počet bitov nastavených na “1”
- **Inštrukcia `imul`**
  - Jeden operand konštantný
  - Druhý operand z líšiacimi sa váhami (0, 32, 64)

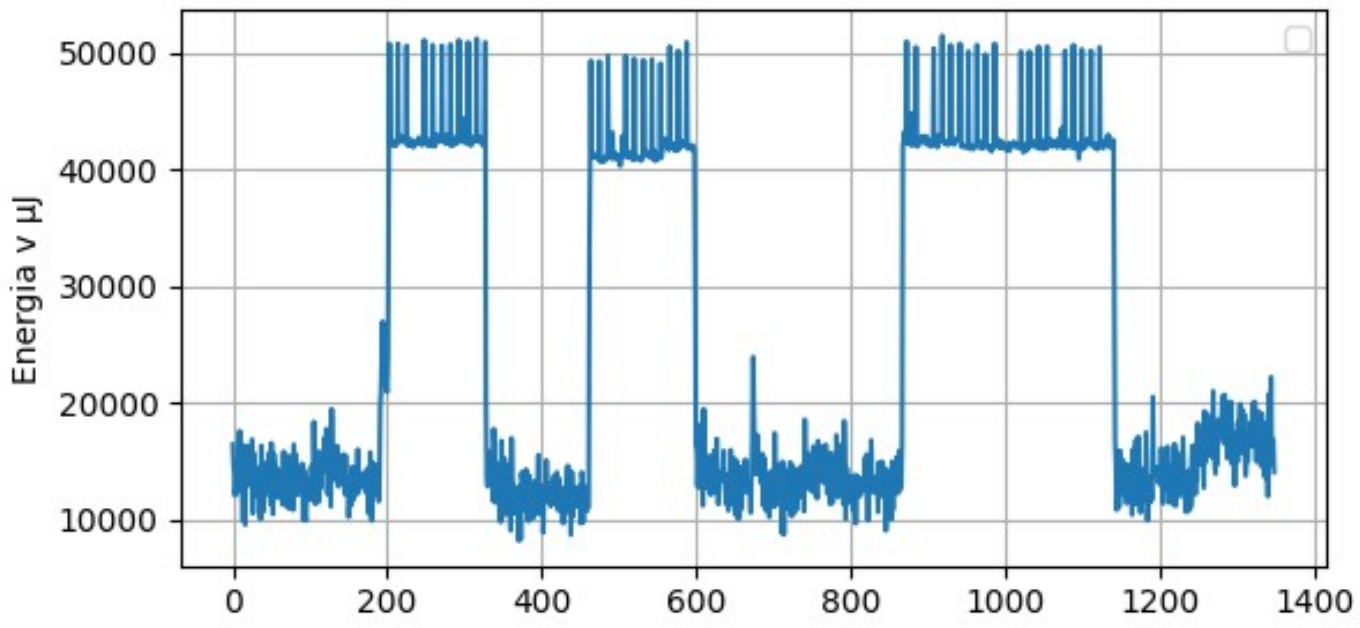
Rozlišovanie operandov



Skrytý komunikačný kanál

- **Spotrebou procesora je možné manipulovať**
- **Dve nezávislé vlákna - naslúchajúce a vysielajúce**
- **Naslúchajúce**
  - Periodicky zaznamenáva spotrebu CPU
- **Vysielajúce**
  - Vysiela binárnu správu kódovanú spotrebou CPU

Skrytý komunikačný kanál



Ďakujem