Implementácia modifikovaného algoritmu SHA-1 v jazyku C (CPU) a CUDA (GPU)

Peter Kaňuch
Fakulta informatiky a informačných technológií
Slovenská Technická Univerzita
Slovenská republika, Bratislava
Email: xkanuch@stuba.sk

***Abstrakt*—**

***Keywords*—IEEEtran, journal, LaTeX, paper, template.**

I. Úvod

II. CPU verzus GPU architektúra

Načo su určene CPU a načo GPU

A. Architektúra počítačových procesorov

CPU (Central Processing Unit) alebo aj procesor, je hlavný komponent počítača, ktorý načítava, spracováva a vykonáva inštrukcie nad rôznymi dátami. Procesor pozostáva z dvoch hlavných častí:

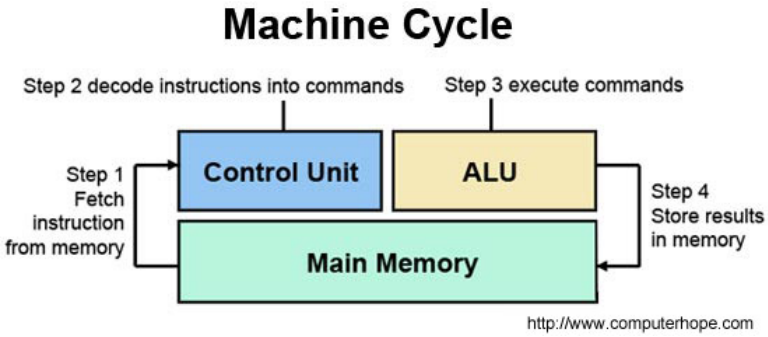
- kontrolná jednotka (CU)
- aritmeticko-logická jednotka (ALU)

Základný procesor pozostáva z piatich fáz [1]:

- IF (Instruction Fetch) - fáza, v ktorej sa načítava inštrukcia z pamäte do procesora na základe adresy v registry IP/PC (instruction pointer/program counter) a jeho následnej inkrementácii na ďalšiu adresu
- ID (Instruction Decode) - zabezpečuje dekódovanie inštrukcie
- EX (Execute) - fáza, v ktorej procesor vykonáva rôzne výpočty pomocou ALU
- MEM (Memory Access) - v tejto fáze, procesor pristupuje do pamäte pre načítanie alebo uloženie dát
- WB (Write Back) - procesor zapíše výsledky(hodnoty z predošlých fáz vypočítané v ALU) alebo hodnoty načítané z pamäte v predchádzajúcej fáze do registrov

Takáto základná architektúra bola postupne vylepšovaná rôznymi mechanizmami (prúdovým spracovaním, detekciou a riešením hazardov, či závislostí, predikciou vetvenia a iné) pre dosiahnutie čo najlepšieho výkonu, t.j. dosiahnutie čo najmenšieho CPI (CPI - počet cyklov na inštrukciu).

Jedným z vylepšení procesora je *prúdové spracovanie.* To spočíva v tom, že v každom hodinovom cykle procesora dokážeme začať spracovávať novú inštrukciu [1]. Tým dokážeme znížiť vykonávanie jednej inštrukcie z piatich cyklov na hodnotu blízkej jedna. Nie je to však jednoduché. Vznikajú takzvané *hazardy* a *závislosti v programe*.



Obr. 1. Základný cyklus procesora

Ďalším vylepšením procesora, kedy inžinieri chceli zvýšiť výkonnosť procesora, bolo vymyslením *Hyper-threading*-u. Hyper-threading vytvára z jedného fyzického, viacero logických procesorov [3]. Procesor podporujúci danú technológiu si dokáže zapamätať viacero stavov procesora pomocou pridanej kompletnej sady jednotlivých registrov (základných, kontrolných, ...). Princíp fungovania je jednoduchý: V každom čase sa spracováva len jedna úloha. Procesor však dokáže veľmi rýchlo prepínať medzi jednotlivými úlohami, čo vytvára pocit, že bežia súčasne.
Základnou nevýhodou hyper-threading-u je, že ostatné súčasti procesora (ALU, MMU, FPU, SIMD) zdieľa medzi úlohami (viď obr. 2 [5]) [4]. Preto tento spôsob zlepšenia nám nezvýši výkon pri výpočtovo náročných úlohách (napr. násobenie matíc).

B. Architektúra grafických procesorov

III. Opis riešenia

A. Algoritmus SHA-1 a jeho modifikácia

B. Testovacie prostredie a implementácia

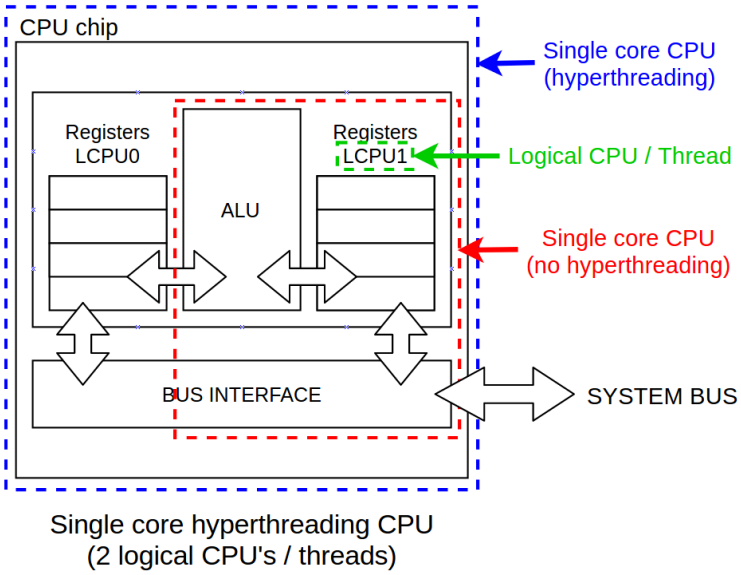
IV. Výsledky a grafické porovnanie

V. Záver

Dodatok A
AAA

Acknowledgment

The authors would like to thank...



Obr. 2. Procesor s hyper-threading

LITERATÚRA

[1] HENNESSY, John L.; PATTERSON, David A. Computer architecture: a quantitative approach. Elsevier, 2007.

[2] TATOURIAN, Alan. Nvidia gpu architecture and cuda programming environment. URL http://code. msdn. microsoft. com/windowsapps/NVIDIA-GPU-Architecture-45c11e6d, 2013.

[3] PRECOMPUTATION, Speculative. Hyper-Threading Technology.

[4] Intel Pentium 4 3.06 GHz with Hyper-Threading support, http://ixbtlabs. com/articles2/pentium43ghzht/, 12.11.2017.

[5] Differences between physical CPU vs logical CPU vs Core vs Thread vs Socket, http://www.daniloaz.com/en/ differences-between-physical-cpu-vs-logical-cpu-vs-core-vs-thread-vs-socket/, 12.11.2017.