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

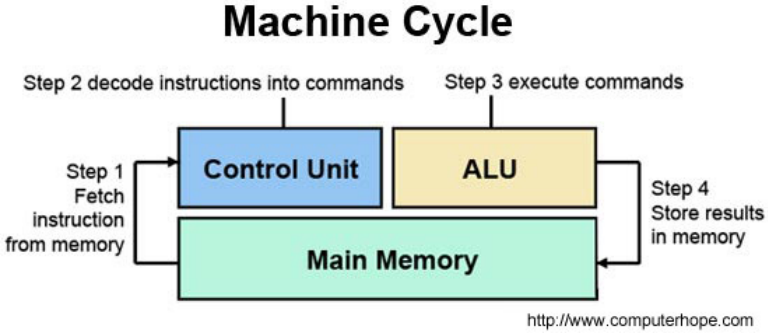
A. Architektúra počítačových procesorov

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]:

- 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
- DECODE - zabezpečuje dekódovanie inštrukcie
- 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



Obr. 1. Základný cyklus procesora

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

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...

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.