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

Peter Kaňuch
Fakulta informatiky a informačných technológií
Slovenská Technická Univerzita
Slovenská republika, 841 04 Bratislava IV
Email: xkanuch@stuba.sk

***Abstrakt*—Keďže grafické procesory sú prispôsobené pre paralelné spracovanie úloh na viacerých jadrách, implementácia takto prispôsobeného problému zníši čas potrebný na jeho vykonanie oproti klasickým počítačovým procesorom. V článku sa zaoberáme implementáciou hashovacieho algoritmu SHA-1 upraveného pre paralelné spracovanie uvedeného v článku [10]. Našim hlavným cieľom je však ukázať, prečo v súčasnosti neexistuje automatický paralelizmus výpočtovo náročných úloh a ich vykonávanie na grafických procesoroch.**

Keywords*—*SHA-1, Modified SHA-1, CPU architecture, GPU architecture, Automatic parallelism for GPU

I. Úvod

V posledných rokoch sa grafické procesory začali dostávať do popredia nie len na spracovanie obrazu, ale aj na vykonávanie, či spracovanie rôznych náročných výpočtových úloch. Architektúra grafických procesorov bola navrhnutá a optimalizovaná pre paralelné spracovanie inštrukcií a dát, zatiaľ čo CPU sú optimalizované pre rýchle sequenčné spracovanie toku programu. V tomto článku porovnáme základnú architektúru CPU a GPU. Vysvetlíme princíp fungovania algoritmu SHA-1 a jeho modifikovanej paralelizovanej verzii. Daný algoritmus implementujeme v programovacom jazyku C pre klasické a v jazyku CUDA pre grafické procesory. Výsledky ukazujú porovnanie nameraných časov vykonávania daného algoritmu na CPU a GPU. Taktiež daný algoritmus porovnávame s implementáciou štandartne používaného nástroja pre výpočet hashovacích funkcií SHA. V závere diskutujeme, prečo ešte v súčasnosti neexistuje automatický paralelizmus a automatické vykonávanie výpočtovo náročných úloch na grafických procesoroch.

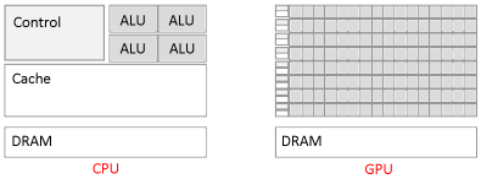
II. CPU verzus GPU architektúra

Aj keď sa zdá, že grafické procesory by mohli svojou výkonnosťou nahradiť klasické počítačové procesory, nie je tomu tak. CPU boli navrhnuté pre dosiahnutie čo najlepšieho výkonu pre sequenčné spracovanie dát, grafické procesory boli navrhnuté za účelom paralelného vykonávania inštrukcií. Pri porovnaní týchto procesorov CPU majú/sú [7]:

1) menej výpočtových jednotiek
2) optimalizované pre sériové operácie
3) nízku toleranciu latencie
4) podporu pre paralelné spracovanie (novšie verzie)

a GPU:

1) viac výpočtových jednotiek
2) vstavané pre paralelné operácie
3) vysokú toleranciu latencie
4) vysokú priepustnosť
5) lepšiu logiku riadenia



Obr. 1. CPU vz. GPU

A. Architektúra počítačových procesorov

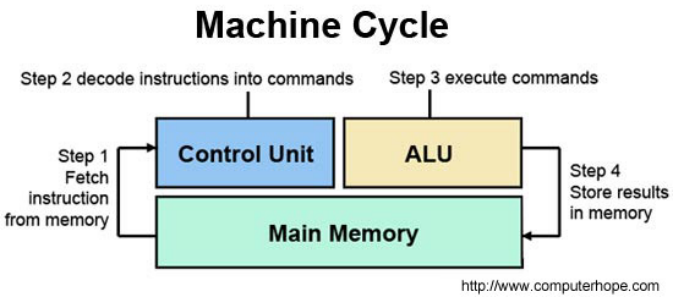
CPU (Central Processing Unit) alebo aj procesor, je hlavný komponent počítača, ktorý načítava, spracováva a vykonáva inštrukcie nad rôznymi dátami. Procesor pozostáva z dvoch hlavných častí:

- 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

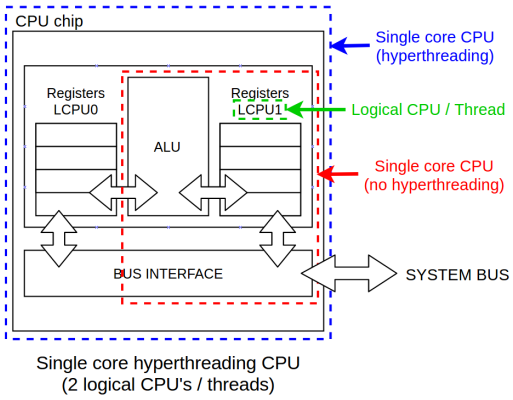
Takáto základná architektúra bola postupne vylepšovaná rôznymi mechanizmami (prúdovým spracovaním, detekciou a riešením hazardov, či závislostí, predikciou vetvenia a iné) pre dosiahnutie čo najlepšieho výkonu, t.j. dosiahnutie čo najmenšieho CPI (CPI - počet cyklov na inštrukciu).



Obr. 2. Základný cyklus procesora

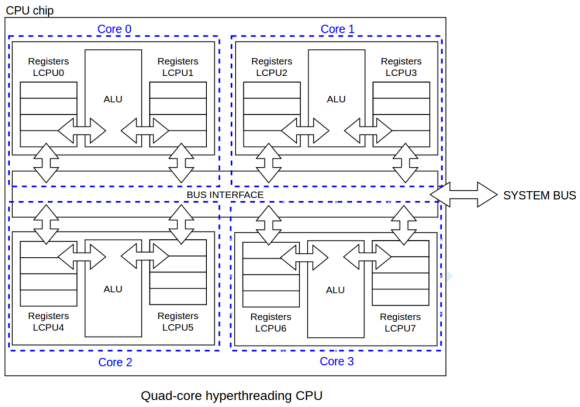
Jedným z vylepšení procesora je *prúdové spracovanie*. To spočíva v tom, že v každom hodinovom cykle procesora dokážeme začať spracovávať novú inštrukciu [1]. Tým dokážeme znížiť vykonávanie jednej inštrukcie z piatich cyklov na hodnotu blízkej jedna. Nie je to však jednoduché. Vznikajú takzvané *hazardy*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

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. 3 [6]) [4]. Preto tento spôsob zlepšenia nám nezvýši výkon pri výpočtovo náročných úlohách (napr. násobenie matíc).



Obr. 3. 1-jadrový procesor s hyper-threading

Iným vylepšením procesora je pridanie viacerých jadier procesora na jeden spoločný čip (viď obr. 4 [6]). Týmto spôsobom sa nám znásobi aj počet vykonávacich jednotiek čím dosiahneme aj znásobenie výpočtového výkonu. Súčasné bežné procesory v prenosných počítačoch obsahujú dve až štyri jadrá. Najvýkonnejšie procesory pozostávajú zo šiestich a viac jadier (12 až 18).



Obr. 4. 4-jadrový procesor s hyper-threading

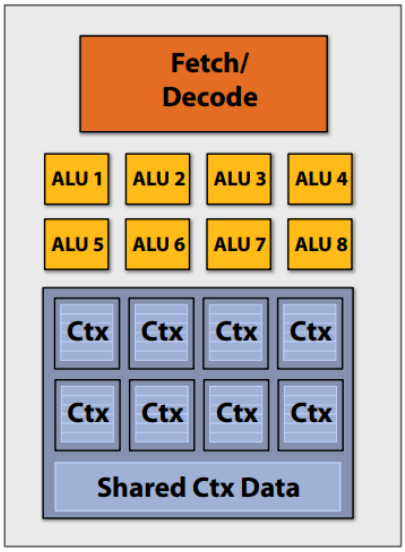
B. *Architektúra grafických procesorov*

Grafické procesory sú navrhnuté tak, aby čo najrýchlesjšie dokázali vykonať paralelizovateľný kód. Napríklad vykonať rovnaké inštrukcie nad rôznymi dátami. Do návrhu boli zahrnuté 3 myšlienky [5]:

1) Pre GPU odstrániť tie časti CPU, ktoré umožňujú rýchle sequenčné výkonávanie inštrukcií.

2) Znížiť náročnosť riadenia inštrukcií vo viacerých ALU.

3) Predchádzať hazardom pomocou začatia vykonávania iného bloku.



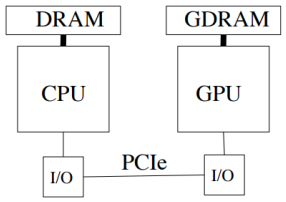
Obr. 5. Jedno jadro grafického procesora

Grafický procesor pozostáva z nasledujúcich častí [2]:

1) Globálna pamäť
2) Multi-procesor - ten sa skladá z:
   - Kontrolné jednotky
   - Registre
   - Výkonné jednotky
   - Cache pamäte

Programy, napísané pre grafické procesory, nevedia pristupovať k dátam uloženým v hlavnej pamäti [7]. Taktiež, GPU boli navrhnuté pre rýchle paralelné spracovanie dát a nepodporujú niektoré funkcie operačného systému. Z tohto dôvodu musia CPU a GPU procesory spolupracovať. Za vykonanie programu na grafike je zodpovedný CPU [2]. Ten má za úlohu:

- Prekopírovať dáta potrebné pre vykonanie programu z hlavnej pamäte do video pamäte.
- Vložiť program (GPU kernel) naprogramovaný programátorom na grafický procesor.
- Po dokončení a spracovaní dát nakopírovať späť výsledné dáta z video pamäte do hlavnej pamäte



Obr. 6. Spojenie CPU a GPU

III. Opis riešenia

Pre porovnanie časov vykonávania programu na CPU a GPU, sme sa rozhodli naprogramovať algoritmus SHA-1 v jazyku C pre CPU a v jazyku CUDA pre grafické procesory. Klasický algoritmus SHA však nie je paralelizovateľný, a preto sme implementovali jednu z jeho modifikácií pre paralelné spracovanie. Výber problému nie je veľmi vhodný vzhľadom na porovnanie architektúry procesorov, keďže daný problém nepozostáva zo zložitých aritmeticko-logických operácií.

A. Algoritmus SHA-1 a jeho modifikácia

Všeobecný algoritmus SHA pozostáva z nasledujúcich krokov:

1) Predspracovanie
   - Zarovnanie správy
   - Rozdelenie na bloky
   - Nastavenie počiatočného výsledku hash-u
2) Výpočet hash-u

Princíp fungovania SHA:

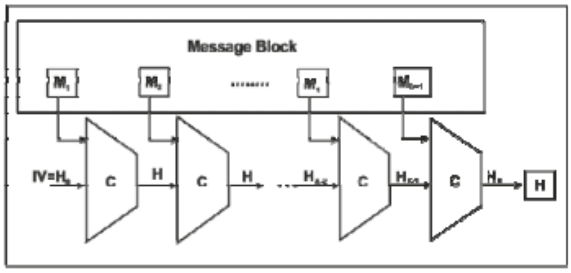
1) Zarovnanie správy pomocou nulových bajtov a doplnením veľkosti správy na koniec
2) Rozdelenie správy na bloky o veľkosti 64 bajtov
3) Nastavenie počiatočného výsledku hash-u
4) Vykonanie operácií a pripojenie medzivýsledku ku finálnemu hashu pre každý blok

Princíp fungovania modifikovanej SHA:

1) Rozdelenie správy na bloky o veľkosti 64 bajtov
2) Pre každý blok
   a) Nastavenie počiatočnej hodnoty
   b) Vykonanie operácií
   c) Pripojenie výsledku k počiatočnej hodnote
3) Spojenie výsledkov jednotlivých blokov
4) Ak veľkosť bloku nerovná sa 20 bajtov $\Longrightarrow$ pokračuj v bode 1.

Algorithm 1 SHA-1 [8]

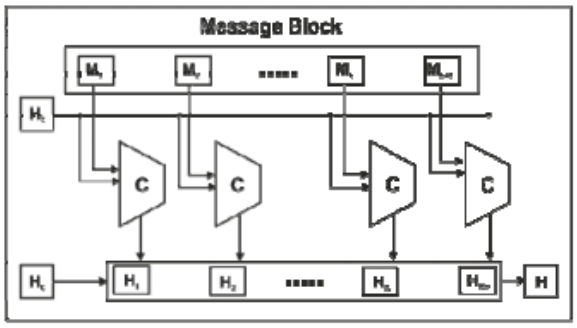
function SHA($Message\ M$)
  padding(M) ▷ Put zero bytes into message and its size at the end
  Set H_0 ▷ Initial value of hash
  for each $block \in \mathcal{M}$ **do** ▷ 512 bit block size
    for $i = 0$ to 15 **do**
      $W_i = M_i$
    end for
    for $i = 16$ to 79 **do**
      $W_i = ROTL^1(W_{i-3} \oplus W_{i-8} \oplus W_{i-14} \oplus W_{i-16})$
    end for
    Set $a, b \dots e$ with $H_{0..4}^{i-1}$
    for $i = 0$ to 79 **do** ▷ f = Ch for i == 0 ... 19; Parity for i == 20 ... 39 & 60 ... 79; Maj for i == 40...59
      $T = ROTL^5(a) + f(b, c, d) + e + K_i + W_i)$
      $e = d$
      $d = c$
      $c = ROTL^{30}(b)$
      $b = a$
      $a = T$
    end for
  end for
  $H_{0..4}^{i-1}$ = $a, b \dots e$ + $H_{0..4}^{i-1}$
end function



Obr. 7. Grafické znázornenie klasického algoritmu SHA

Algorithm 2 Modified SHA-1 (pseudo code) [10]

function MSHA($Message\ M$)
  $padding(M)$ ▷ Put zero bytes into message and its size at the end
  $Blocks(M)$ ▷ Breaking message into 64 bytes blocks
  for each $block \in \mathcal{M}$ **do** ▷ Each block is independent
    $H_i = SHA(block)$
  end for
  $H+ = H_i$ ▷ + mean concatenate
  if (size(H) != 20B) **then** $MSHA(M)$
  else return
  end if
end function



Obr. 8. Grafické znázornenie modifikovaného algoritmu SHA

B. Vlastnosti SHA-1 a jeho modifikovanej verzie

Pre všetky hashovacie funkcie je dôležité spĺňať nasledujúce vlastnosti [9]:

- Ireverzibilnosť hashu (Preimage resistance) - pre daný hash je ťažké nájsť správu, po ktorej zahashovaní dostaneme pôvodný hash
- Odolnosť voči kolíziám - je ťažké nájsť také dve rôzne správy, ktorých výsledky hashu sa rovnajú

Daný modifikovaný algoritmus SHA-1 by mal spĺňať všetky vlastnosti hashovacích funkcií, viď článok [10].

C. 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.

[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] How a GPU Works - Kayvon Fatahalian 15-462 (Fall 2011), https://www. cs.cmu.edu/afs/cs/academic/class/15462-f11/www/lec_slides/lec19.pdf, 12.11.2017.

[6] 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.

[7] The Continuing Importance of GPUs For More Than Just Pretty Pictures - Jeff Rowe, https://www10.mcadcafe.com/blogs/jeffrowe/2017/03/16/the-continuing-importance-of-gpus-for-more-than-just-pretty-pictures/, 12.11.2017

[8] GALLAGHER, Patrick; DIRECTOR, Acting. Secure hash standard (shs). FIPS PUB, 1995, 180-3.

[9] ROGAWAY, Phillip; SHRIMPTON, Thomas. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In: International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 2004. p. 371-388.

[10] KISHORE, Neha; KAPOOR, Bhanu. An efficient parallel algorithm for hash computation in security and forensics applications. In: Advance Computing Conference (IACC), 2014 IEEE International. IEEE, 2014. p. 873-877.