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

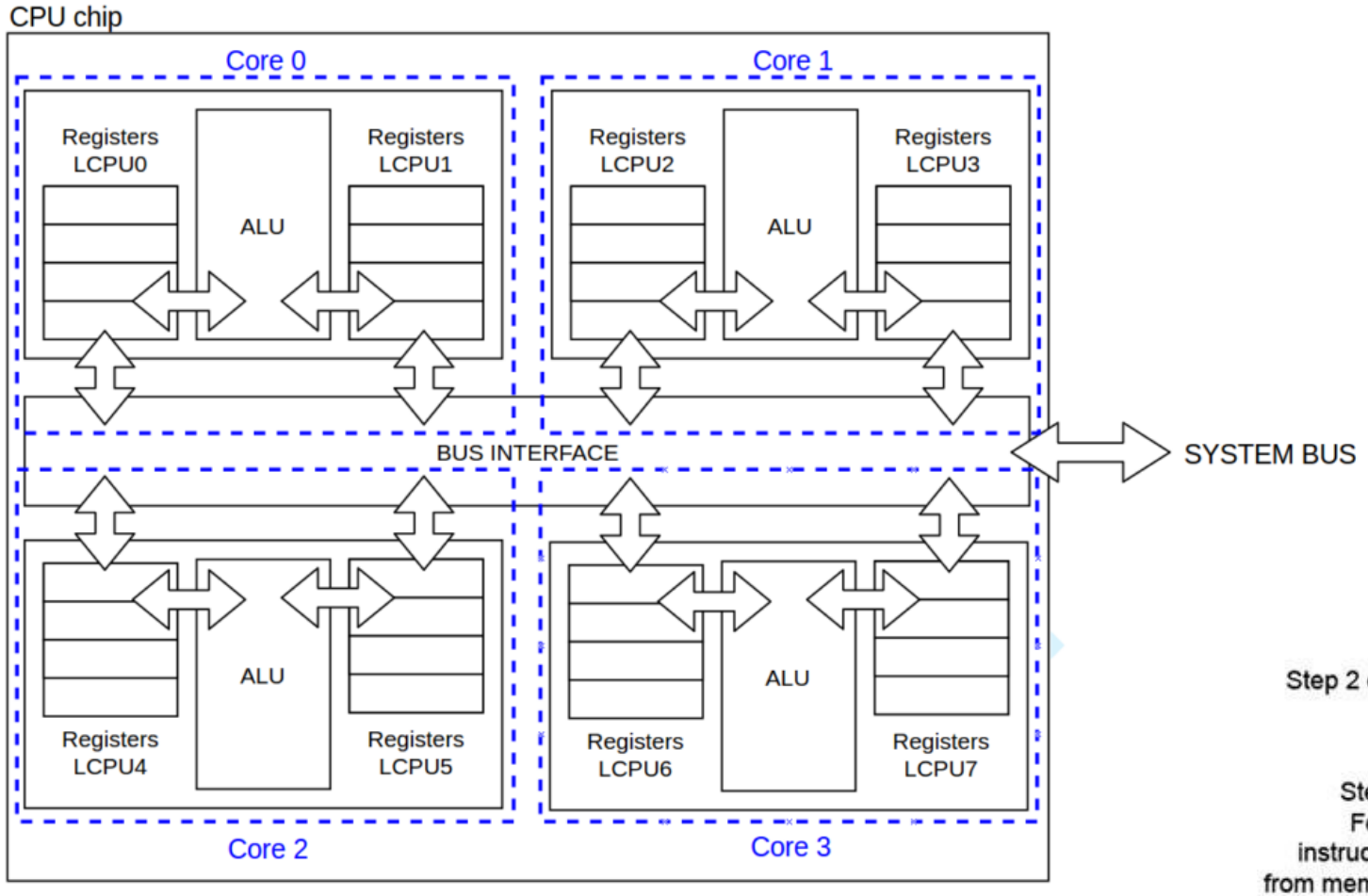
Architektúry počítačových systémov

Peter Kaňuch

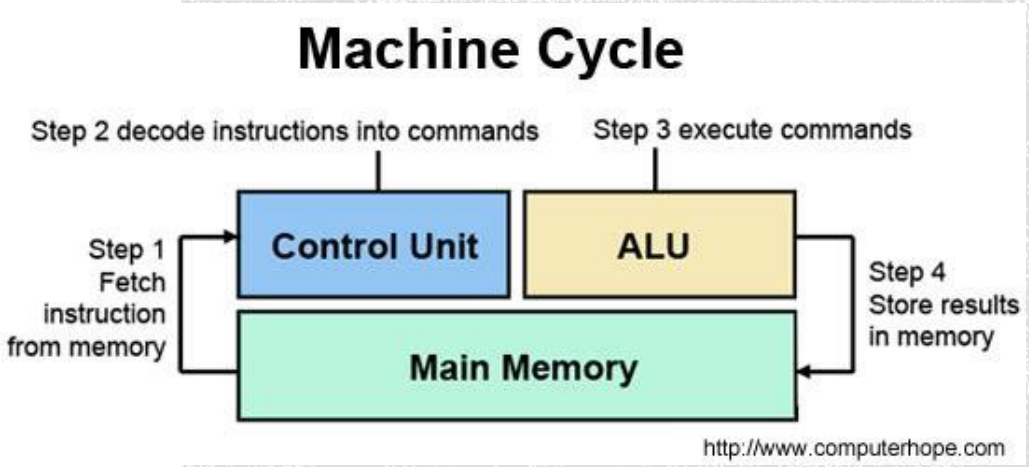
27/11/2017

Architektúra CPU

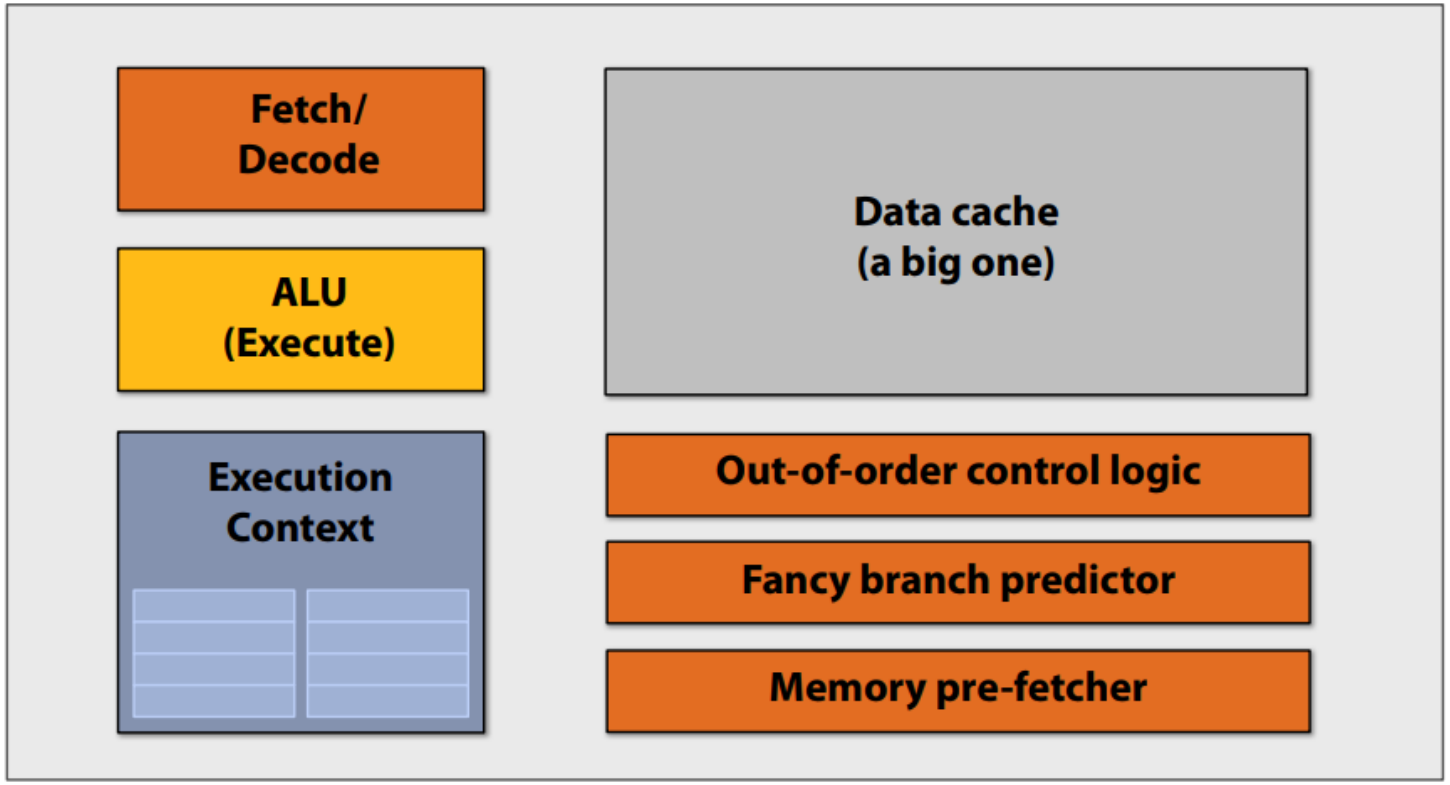
- Prúdové spracovanie
- Hyper-threading
- Multi-procesory

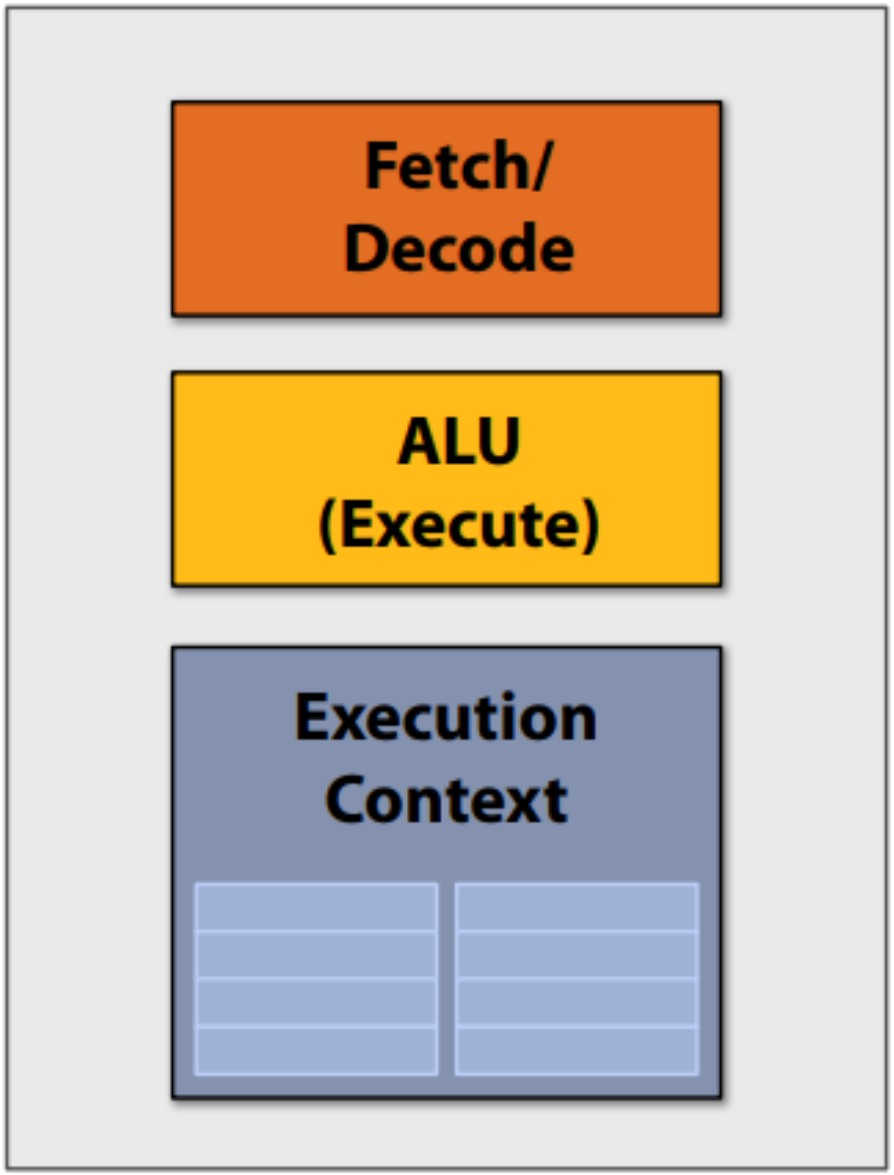


Quad-core hyperthreading CPU



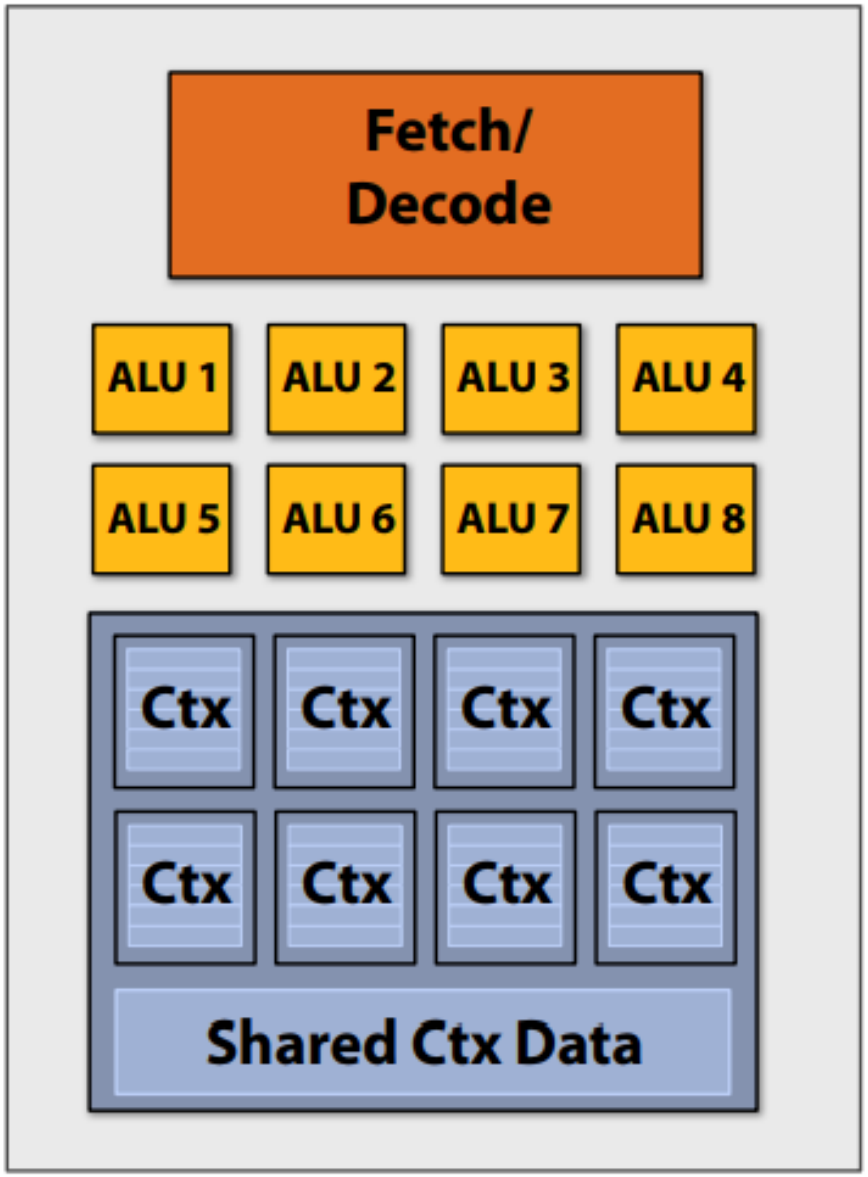
Architektúra GPU





Architektúra GPU

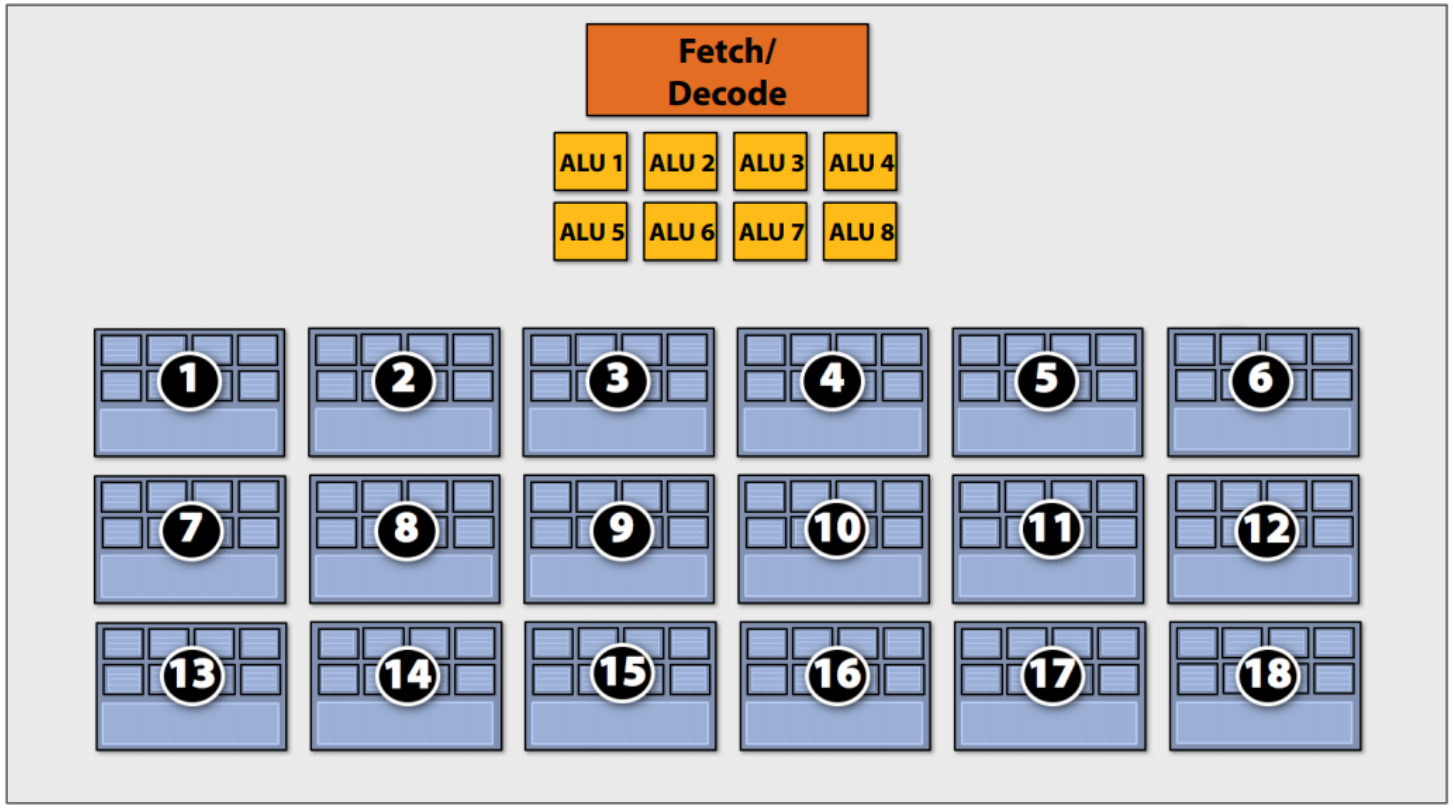
- odstránenie častí CPU umožňujúcich rýchle sequenčné výkonávanie inštrukcií



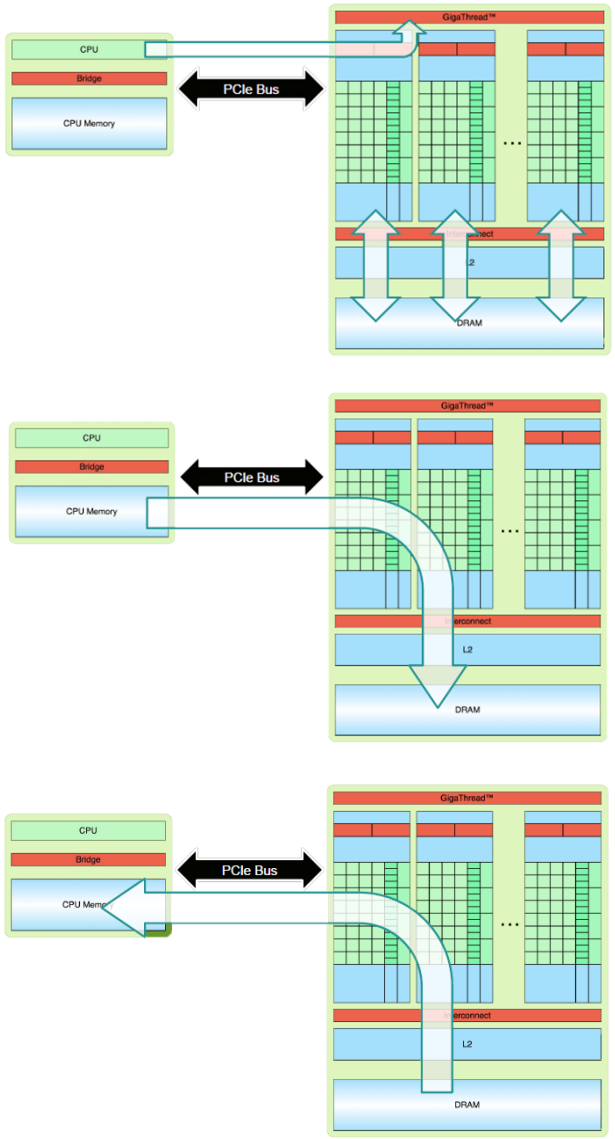
Architektúra GPU

- odstránenie častí CPU umožňujúcich rýchle sequenčné výkonávanie inštrukcií
- zníženie náročnosti riadenia inštrukcií vo viacerých ALU

Architektúra GPU

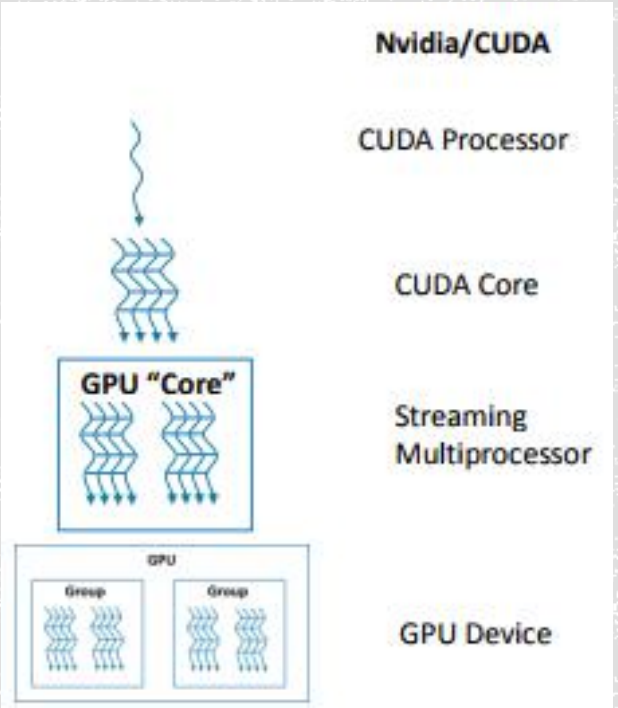


- odstránenie častí CPU umožňujúcich rýchle sequenčné výkonávanie inštrukcií
- zníženie náročnosti riadenia inštrukcií vo viacerých ALU
- predchádzanie hazardom pomocou začatia vykonávania iného bloku

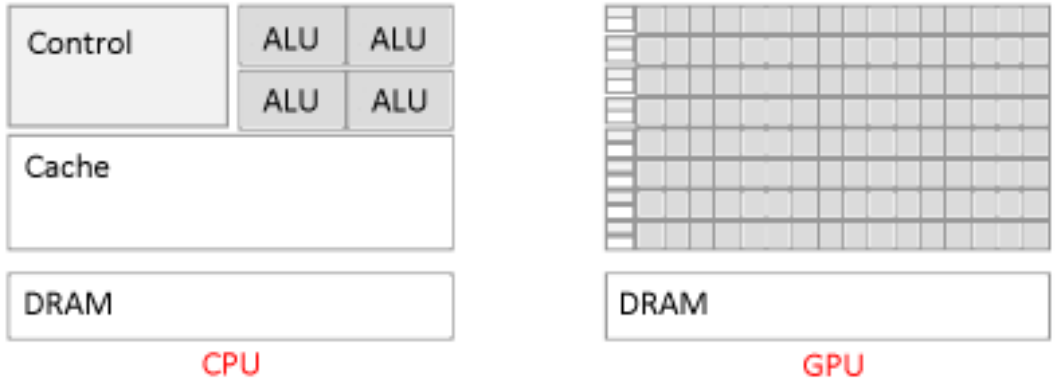


Vykonanie programu na GPU

- SIMT – rozdelenie rovnakej, nezávislej práce na rovnaké synchronizované vlákna



CPU vs. GPU

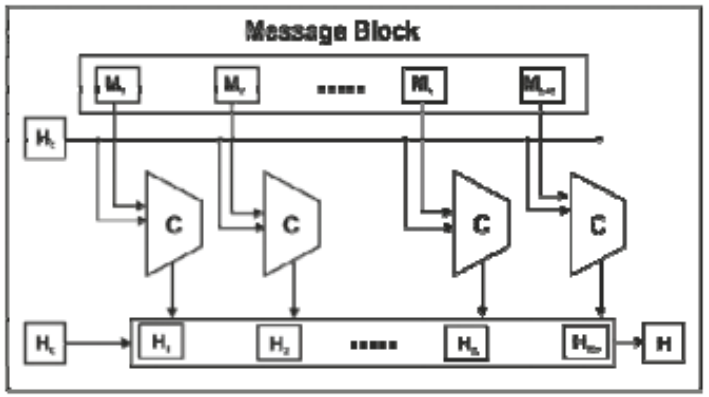


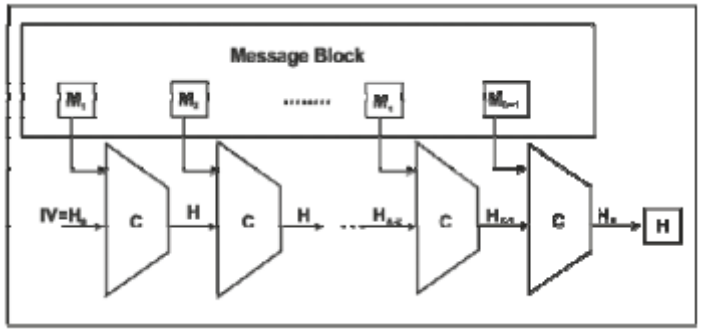
CPU:

- menej výpočtových jednotiek
- optimalizované pre sériové operácie
- nízku toleranciu latencie
- podporu pre paralelné spracovanie (novšie verzie)

GPU:

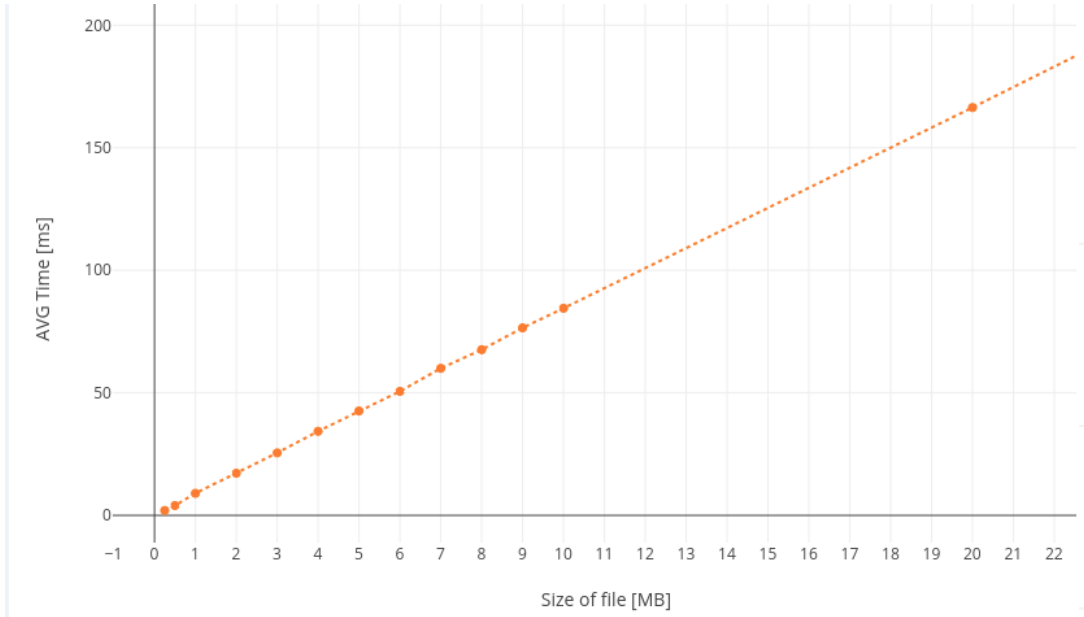
- viac výpočtových jednotiek
- vstavané pre paralelné operácie
- vysokú toleranciu latencie
- vysokú priepustnost’
- lepšiu logiku riadenia





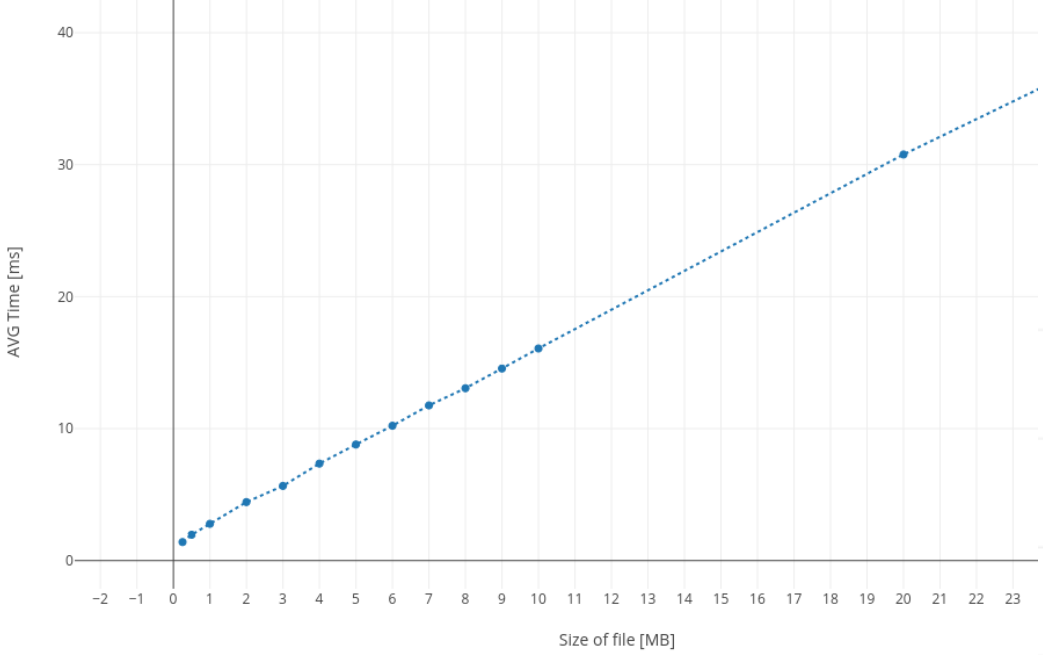
(M)SHA-1 a vlastnosti hashov

- 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


AVG Time [ms]
200
150
100
50
0
−1 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22
Size of file [MB]

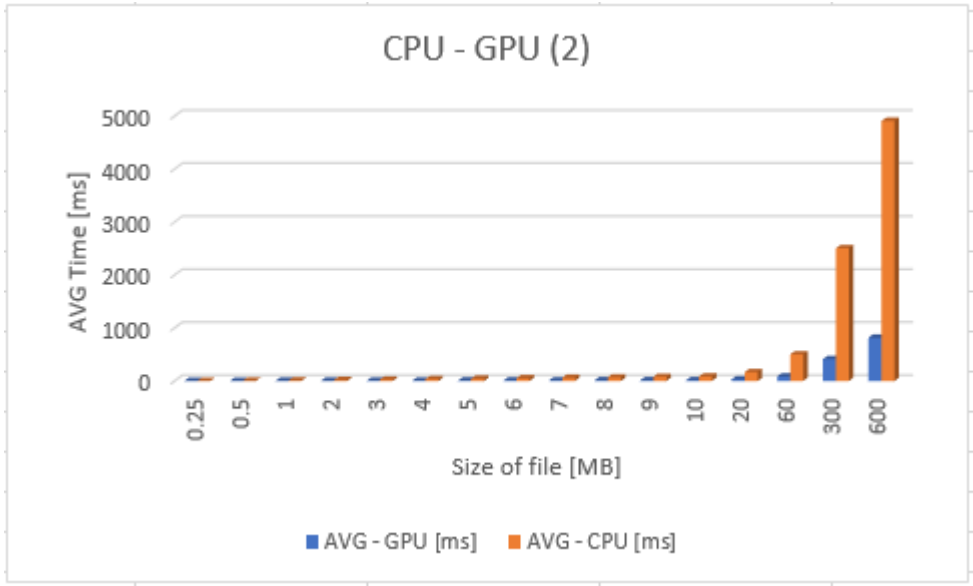
AVG - CPU

AVG Time [m
2000
1000
0
−20 0 20 40 60 80 100 120 140 160 180 200 220 240 260 280 300 320 340 360 380 400 420 440 460 480 500 520 540 560 580 600 620
Size of file [MB]


AVG Time [ms]
40
30
20
10
0
−2 −1 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
Size of file [MB]

AVG - GPU

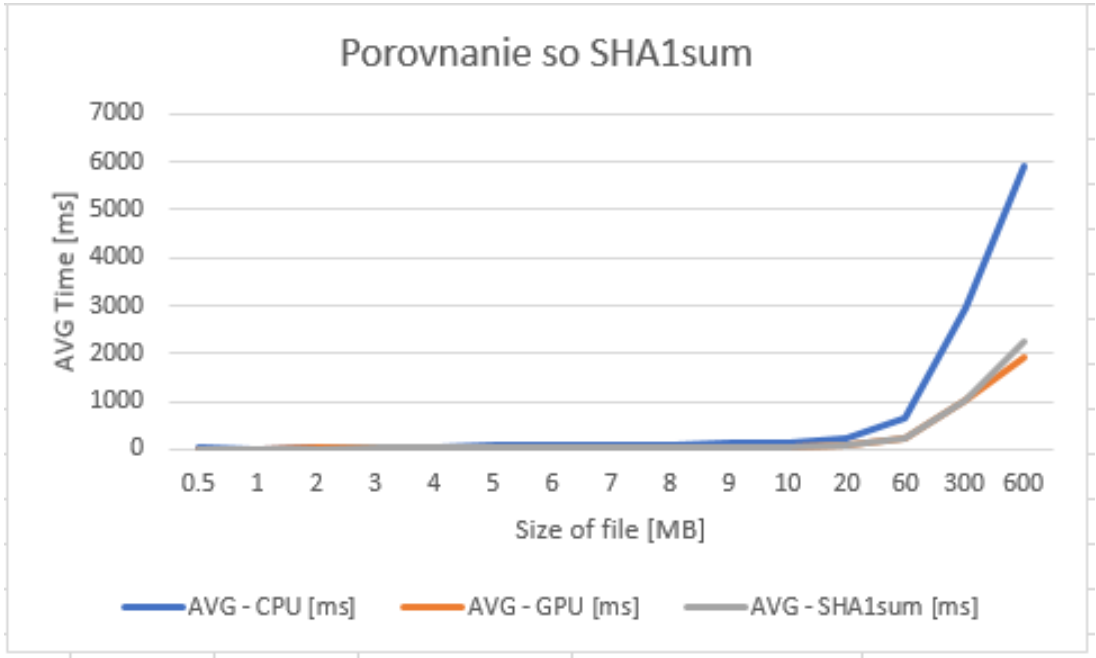
AVG Time [ms]
400
300
200
100
0
0 100 200 300 400 500 600
Size of file [MB]

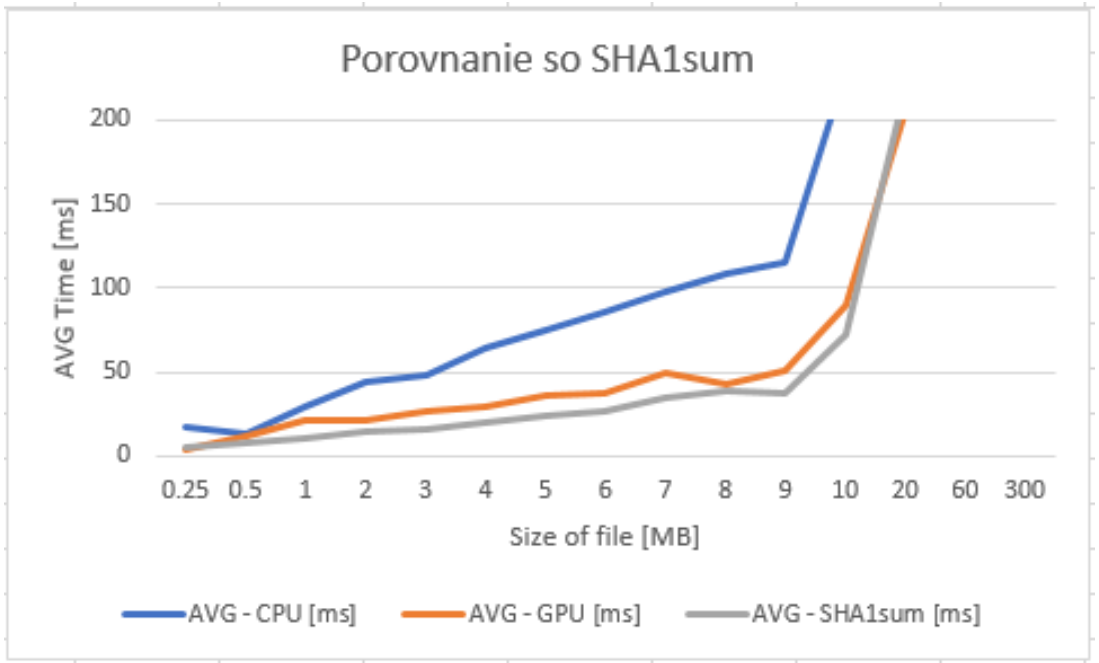

CPU - GPU (2)
AVG Time [ms]
5000
4000
3000
2000
1000
0
0.25
0.5
1
2
3
4
5
6
7
8
9
10
20
60
300
600
Size of file [MB]
AVG - GPU [ms]
AVG - CPU [ms]

CPU - GPU

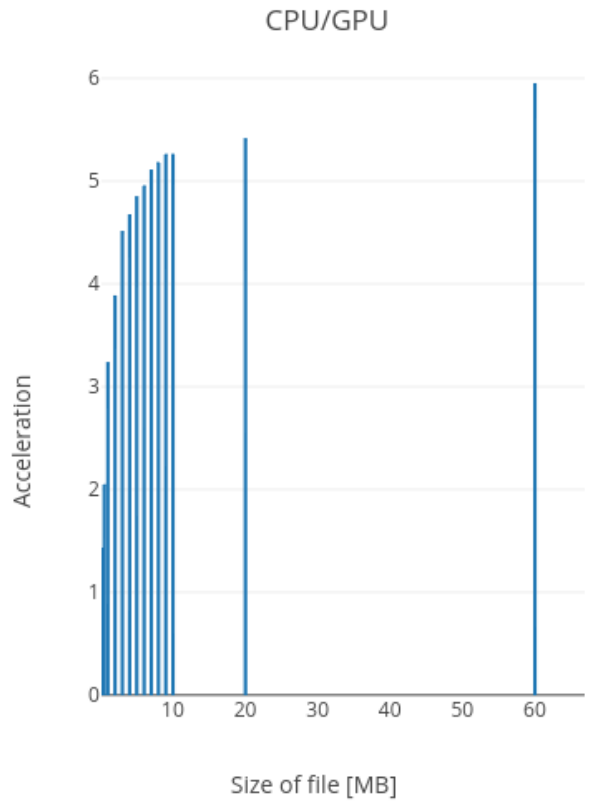
GPU
CPU
AVG Time [ms]
100
80
60
40
20
0
0 0.5 1 1.5 2 2.5 3 3.5 4 4.5 5 5.5 6 6.5 7 7.5 8 8.5 9 9.5 10 10.5 11 11.5 12 12.5 13 13.5 14 14.5 15 15.5 16 16.5 17 17.5 18 18.5 19 19.5 20 20.5
Size of file [MB]

Porovnanie so SHA1sum nástrojom





Zrýchlenie GPU oproti CPU



Tabuľka I. CPU vs. GPU

Size [MB]	AVG - GPU [ms]	AVG - CPU [ms]	CPU/GPU
0.25	1.4047648	2	1.423725879
0.5	1.958352	4	2.042533722
1	2.7868832	9	3.229414135
2	4.4332639	17.2	3.879760012
3	5.6588672	25.5	4.506202231
4	7.3489853	34.3	4.66731101
5	8.7965731	42.6	4.842794974
6	10.2195169	50.6	4.95131037
7	11.7593665	60	5.102315673
8	13.0595455	67.6	5.1762904
9	14.5545724	76.5	5.256080213
10	16.0727678	84.5	5.257339685
20	30.7733154	166.4	5.407282181
60	84.3981097	501.7	5.944445933
300	411.9776641	2504.7	6.079698533

Automatické využitie GPU

- Automatický paralelizmus na úrovni inštrukcií
- OpenMP

Výhoda nových GPU:

- volanie kernelu z kernelu

CPU a GPU:

- nájsť nezávislé časti programu
- prekopírovať dáta z pamäte RAM do video pamäte a späť
- rozdelit’ dáta pre jednotlivé bloky a thready GPU