

GPGPU i OpenCL

Krunoslav Đuras

28. siječnja 2013.

Sadržaj

Uvod

OpenCL

GPGPU programerski koncepti

Primjeri primjene GPGPU-a

Uvod

GPGPU (eng. General-purpose computing on graphics processing units) predstavlja primjenu grafičkih kartica (koje se najčešće koriste samo u računalnoj grafici) za provođenje izračuna u aplikacijama koje najčešće koriste samo CPU procesor.

GPGPU i ostale slične tehnologije koje se koriste radi boljih performansi kod izračuna počele su se koristiti zbog povećane potrebe za performansama u znanosti i inženjerstvu.

Te tehnologije se najčešće koriste za paralelno provođenje različitih izračuna nad velikim skupovima podataka.

Potreba za tim tehnologijama stvorila je jaku potrebu za arhitekturama za razvoj softvera koje omogućuju razvoj softvera koji je sposoban da iskoristi grafičke kartice i slične tehnologije za masivno paralelno izvođenje različitih algoritama.

OpenCL

OpenCL je otvoreni standard kojeg održava neprofitni konzorcij Khronos Group.

OpenCL je novi industrijski standard za podatkovno i zadačno paralelno provođenje izračunavanja na mnogim različitim vrstama procesora (CPU, GPU, DSP i sl.).

OpenCL definira skup osnovnih funkcionalnosti koje podržavaju svi uređaji.

OpenCL

Osim toga, OpenCL definira i neke dodatne funkcionalnosti koje se mogu koristiti samo na određenim uređajima. Iako OpenCL garantira portabilnost koda i mogućnost izvršavanja na različitim uređajima (CPU, GPU i sl.), ta portabilnost ima svojih granica a ona ovisi o veličini razlike hardverske arhitekture uređaja. Ipak, programer ima mogućnost da piše program za jednu određenu arhitekturu, a da taj program može ispravno raditi i na nekim drugim arhitekturama.

OpenCL uključuje jezik (baziran na C99 jeziku) za pisanje kernela (funkcija koje se izvode na OpenCL uređajima) i API-je koji se koriste za kontrolu izvršavanja.

OpenCL se može koristiti kako bi aplikacijama omogućio pristup grafičkoj kartici radi izvršavanja različitih vrsta izračuna koji ne moraju nužno imati veze sa grafikom.

GPGPU programerski koncepti - stream processing

Predstavlja izvođenje instrukcija nad velikim brojem nezavisnih grupa podataka istovremeno.

Stream je skup podataka koji zahtjevaju jednaku obradu. Oni omogućuju paralelizaciju.

Za primjenu GPGPU-a je bitan pojam aritmetičke intenzivnosti. Ona je definirana kao broj operacija izvedenih nad jednom jedinicom prenesene memorije (npr. jedan long ili double). Bitno je da GPGPU aplikacije imaju visok aritmetički intenzitet, jer bi inače spora memorijska latencija smanjila ubrzanje izračuna.

GPGPU je najbolje primjeniti za izračune nad velikim skupovima podataka koji podržavaju visoki stupanj paralelizacije i imaju minimalnu međuzavisnost.

GPGPU programerski koncepti - kerneli

Kerneli su funkcije koje se izvode nad svakim elementom stream-a.

Kerneli se pišu u programskom jeziku baziranom na ANSI C99 jeziku.

- ▶ Jezik je poznat programerima
- ▶ Ima neke dodatke i ograničenja
- ▶ Sadržava velik broj ugrađenih funkcija
- ▶ Podržava offline i online compiling

Primjeri primjene GPGPU-a - oclHashcat-plus

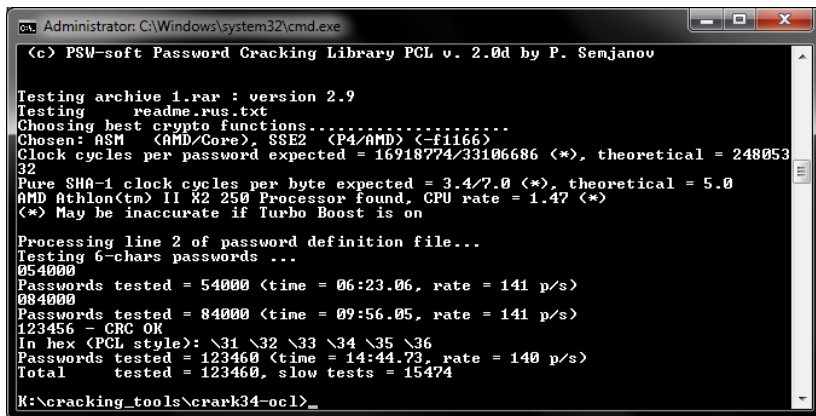
oclHashcat-plus je trenutno najbrži cracker za md5crypt, phpass, mscash2 i WPA / WPA2.

Multi-Platform (OpenCL CUDA)

Primjeri primjene GPGPU-a - cRARk

cRARk je besplatan alat za otkrivanje šifri RAR i 7-Zip arhiva.

Primjeri primjene GPGPU-a - cRARk



```
Administrator: C:\Windows\system32\cmd.exe

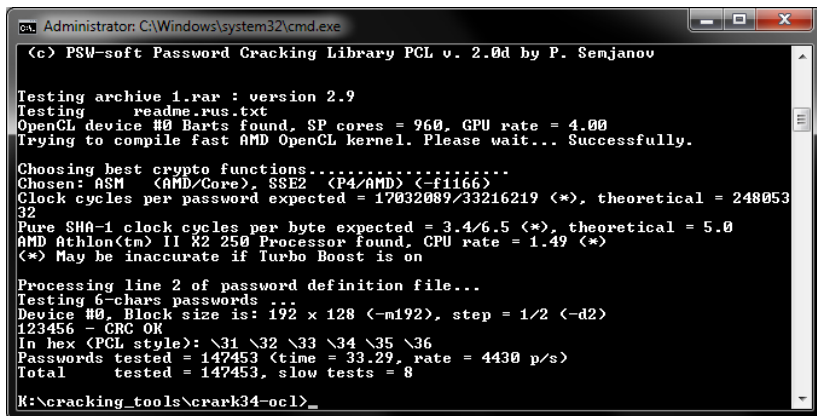
(c>) PSW-soft Password Cracking Library PCL v. 2.0d by P. Semjanov

Testing archive 1.rar : version 2.9
Testing      readme.rus.txt
Choosing best crypto functions.....
Chosen: ASM   (AMD/Core), SSE2  (P4/AMD) (-f1166)
Clock cycles per password expected = 16918774/33106686 (*), theoretical = 248053
32
Pure SHA-1 clock cycles per byte expected = 3.4/7.0 (*), theoretical = 5.0
AMD Athlon(tm) II X2 250 Processor found, CPU rate = 1.47 (*)
(*) May be inaccurate if Turbo Boost is on

Processing line 2 of password definition file...
Testing 6-chars passwords ...
054000
Passwords tested = 54000 (time = 06:23.06, rate = 141 p/s)
084000
Passwords tested = 84000 (time = 09:56.05, rate = 141 p/s)
123456 - CRC OK
In hex (PCL style): \31 \32 \33 \34 \35 \36
Passwords tested = 123460 (time = 14:44.73, rate = 140 p/s)
Total      tested = 123460, slow tests = 15474

K:\cracking_tools\crark34-ocl>_
```

Primjeri primjene GPGPU-a - cRARK



```
Administrator: C:\Windows\system32\cmd.exe

(c>) PSW-soft Password Cracking Library PCL v. 2.0d by P. Semjanov

Testing archive 1.rar : version 2.9
Testing      readme.rus.txt
OpenCL device #0 Barts found, SP cores = 960, GPU rate = 4.00
Trying to compile fast AMD OpenCL kernel. Please wait... Successfully.

Choosing best crypto functions.....
Chosen: ASM  (AMD/Core), SSE2  (P4/AMD) (-f1166)
Clock cycles per password expected = 17032089/33216219 (*), theoretical = 248053
32
Pure SHA-1 clock cycles per byte expected = 3.4/6.5 (*), theoretical = 5.0
AMD Athlon(tm) II X2 250 Processor found, CPU rate = 1.49 (*
(*) May be inaccurate if Turbo Boost is on

Processing line 2 of password definition file...
Testing 6-chars passwords ...
Device #0. Block size is: 192 x 128 (-m192), step = 1/2 (-d2)
123456 - CRC OK
In hex (PCL style): \31 \32 \33 \34 \35 \36
Passwords tested = 147453 (time = 33.29, rate = 4430 p/s)
Total      tested = 147453, slow tests = 8

K:\cracking_tools\crark34-ocl>_
```