File System Encryption

ACA - MIECT

Gabriel Silva (85129)
Gonçalo Vítor (85119)

Introdução

O objetivo deste projeto é descobrir se é vantajoso usar uma GPU para executar a cifragem dum sistema de ficheiros, em vez de fazer esse processo no CPU. Para isso é necessário otimizar a execução do programa em questão na GPU, usando grelhas de lançamentos de threads que permitam esta mesma otimização.

O programa foi executado na nossa máquina pessoal, que tem uma NVIDIA GTX 2070.

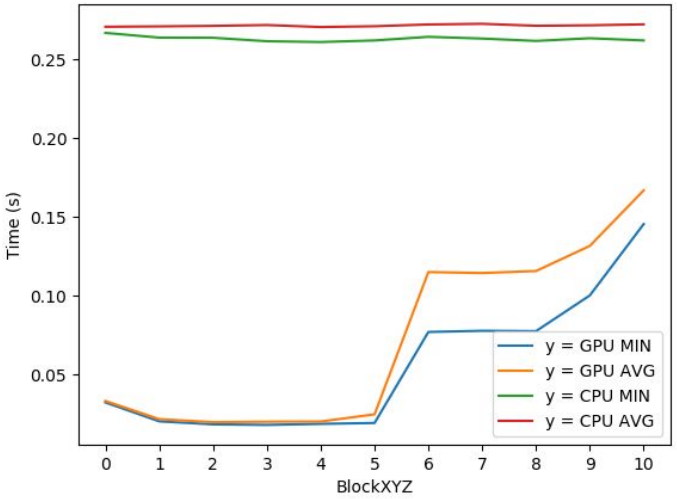
NVIDIA GTX 2070

Há várias características da GPU que são relevantes para otimizar a execução de código:

É composta por 36 SM's, cada uma podendo ter um máximo de 16 blocos de threads ou 1024 threads ativas simultaneamente. Deve ser nossa preocupação lançar grelhas de execução que garantem que exista o máximo de ocupação da gpu possível, isto é, o máximo número de threads ativas por SM, e também que respeitem os limites do problema e tempos de acesso à memória.

Tem um warp size de 32, o que significa que a GPU organiza os threads em grupos de 32 que executam a mesma instrução. Devemos, por isso, tentar que a GPU consiga organizar todos os threads em warps, usando um tamanho de bloco múltiplo de 32, não havendo threads de "sobra".

Resultados cryptCuda



Como podemos ver no gráfico, os melhores valores médios são atingidos entre as 2 e as 32 threads, tendo sido o menor atingido com a seguinte configuração:

blockX: '0',
blockY: '3',
gridX: '12',
gridY: '6',
gpuTime: '1.796e-02',
cpuTime: '2.752e-01'

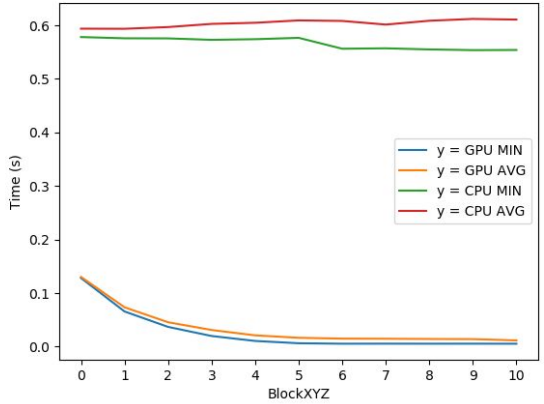
Stride

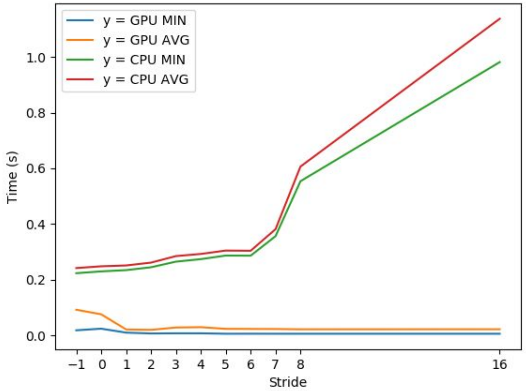
Há ainda um fator muito importante que falta otimizar : os acessos à memória.

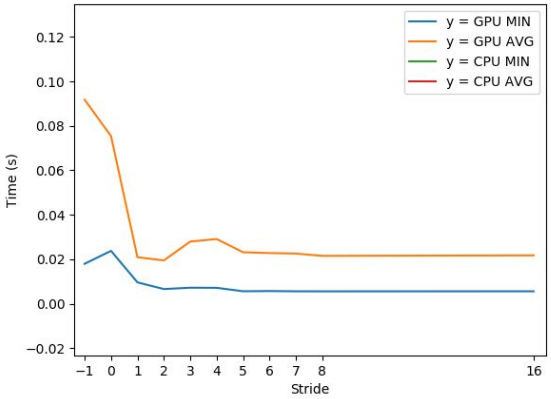
Isto pode ser conseguido introduzindo stride no array que guarda a informação relativa a um setor do sistema de ficheiros.

É necessário ter em atenção que valores muito altos de stride diminuem a largura de banda efetiva da memória.

Resultados cryptCudaStride







Variação do tempo de execução com diferentes quantidades de threads para Stride = 2^8, que deu o mínimo absoluto do projeto para a configuração:
Grid: X=1, Y=10;Block: X=3,Y=7;
GpuTime: 5,56e-3s; CpuTime: 5,946e-1s

Variação do tempo de execução com diferentes Stride, estando o -1 a representar os valores sem stride. Podemos ver que os valores da GPU saturam com stride 2^5, mas a partir daí só pioram para o cpu.

Conclusão

Em suma, vale a pena usar a GPU para fazer o esforço associado à cifragem dos setores do sistema de ficheiros. O *speed up* obtido, relativamente a uma execução no CPU, foi de aproximadamente 15 vezes, no exercício sem stride. Usando *stride*, o speed up foi de aproximadamente 48 vezes, para um valor de stride de 5, que foi quando a gpu saturou e começou a piorar no cpu.