Universidade de Aveiro

Mestrado Integrado em Engenharia de Computadores e Telemática

Arquitectura de Computadores Avançada

Assignment 2 – File system encryption

Academic year 2019/2020
Problem design: Tomás Oliveira e Silva

UNDERLYING CONCEPT

One way of performing the encryption of a file system consists of encrypting each file system block contents separately by using an encryption key that depends on the block number. The purpose of this assignment is to study the viability of offloading the computational part of the encrypting procedure to a GPU device.

In the naive reference implementations you have received, you may assume that the encryption and decryption operations work on disk sectors, each 512 bytes long, which have been previously transferred to main memory.

The *encryption operation* amounts to

1. define a 32-bit linear congruential pseudo-random number generator with parameters that depend on the sector number
2. generate 512/4 = 128 pseudo-random 32-bit integers using the pseudo-random number generator
3. XOR them with the sector data.

Since a XOR x XOR $x = a$, the *decryption operation* is implemented by performing the same procedure.

The fully functional reference implementations which are provided to you, `cryptCuda.cu` and `cryptCudaStride.cu`, are not optimized on purpose.

Your task is to optimize the thread launch grids and draw conclusions about the usefulness of offloading the computation to a GPU device.

The assignment entails that some investigation on the factors that limit GPU performance. The presentation must illustrate how these factors affect the performance in this specific case, so plots of execution times, and explanations of their variation, for meaningful thread launch grids should be provided.

GRADING

- thread launch grid optimization and conclusions about offloading the computation to a GPU device by using reference implementation `cryptCuda.cu` – 14 valores
- thread launch grid optimization by using reference implementation `cryptCudaStride.cu` – 17 valores.

DELIVARABLES

- an archive, named `EFS_T$G#.zip` (where $, equal to 1, … ,4, means the lab number and #, equal to 1, …, 8, means the group number), of the `*.cu` files of your solution
- a pdf file, up to 5 power point like pages, where the main results are presented, should be included in the archive.

DEADLINE

- December, 29, at midnight.