Universidade de Aveiro
Mestrado Integrado em Engenharia de Computadores e Telemática
Arquitetura de Computadores Avançada
Second assignment (November 2017) ARB, TOS

One way to encrypt a file system consists of encrypting each file system block separately, 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 encrypting and decrypting blocks to a CUDA or OpenCL device.

In the naïve reference implementation you have received, the encryption and decryption operations work with disk sectors (each with 512 bytes), instead of working with file system blocks. Assume that it is not necessary to split file system blocks into sectors, i.e., assume that you already have the sectors. The encryption operation amounts to

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

Since a xor x xor $x = a$, decryption is done using the same routine.

The fully functional reference implementation is, on purpose, not optimized. Your tasks are:

1. to get a grade up to 14, optimize the threads launch grid and draw conclusions about the usefulness of offloading the computation to the CUDA or OpenCL device, or
2. to get a grade up to 17, optimize the threads launch grid and CUDA or OpenCL kernel memory accesses and draw conclusions about the usefulness of offloading the computation to the CUDA or OpenCL device.

Deliverables:

- an archive, named `A2_tXgY.tgz` (`X` is the practical class number, and `Y` is the group number), with the optimized implementations (one or two implementations, according to the grading level you desire to achieve)
- a pdf file, with up to 4 power-point like pages, describing the main ideas of your solutions

Deadline:

- December 31, at 23h55m.