Final Project Phase 1

Members: Jonathan Jackson, Sriram Arjula, Ryan Luna

Our project direction is in the field of Image Processing and parallel execution of cryptography algorithms (e.g. AES). Our project is built off a previous project on parallel execution of image encryption. A sample of images is used to first encrypt and decrypt using concurrent execution of the algorithm. The execution time is recorded and is then compared against parallelized execution, using data-parallelization, using the same sample of images. The results from the previous project were not very conclusive possibly due to incorrect implementation of the parallel algorithm/instructions. Moreover, the method of encrypting images was suspected of having some effect on the parallelized execution. Specifically in the way the image is formatted and processed so that it can be run through the parallelized AES encryption scheme. A crucial task now is to determine the correct way to implement the Python package for the parallel execution OR move towards a different package (or language entirely eg. C++). As for the direction of the project, we are in the process of determining whether this should be continued using image processing, or simply just on parallelized execution of the AES encryption scheme (on simple samples of text data instead of images). This would remove the issue with implementing image processing and possibly yield more accurate results on the advantage of parallelized execution of encryption schemes vs sequential.

Paper Title: Parallel Implementation of Cryptographic Algorithm: AES Using OpenCL on GPUs

Paper link (IEEE): <https://ieeexplore.ieee.org/document/8398949>

NOTE #1: The paper might change with respect to the direction. We might look towards research works on parallelized encryption schemes not involving image processing.  
  
NOTE #2: This group was formed a bit late due to some last-minute complications on “who’s with who”. We realize this report leaves the direction a big vague regarding whether we are still tackling the image processing or not. This will be resolved within the week and will email you on any significant update. To clarify, the direction WILL focus on parallelized execution of encryption schemes. It is just not clear if we shall do this using image processing or just simpler data (e.g. text).