**Fall 2024: ECE 759 Final Project Proposal**

**Quick intro:**

* Name: Tsao-Ching, Kao
* Email: tkao4@wisc.edu
* Home department: Computer Science
* Status: MS student
* Name of your teammate (everyone needs to submit the same proposal):
* Hau-Cheng Yang
* Tan Huang

**Project Title**: CPU and GPU Parallelization of AES

**GitHub link to your project**: https://github.com/Rob12312368/repo759\_final\_project

**Problem statement**: We want to parallelize AES encryption and decryption using OpenMP and CUDA. Instead of just implementing both and treating them separately, we want to know when to choose which way to parallelize so we can finish the work in less time. That means we will try to find a threshold to switch from CPU parallelization to GPU parallelization.

**Motivation/Rationale**: AES is one of the most popular algorithm for encryption. It is widely used in the industry for different purposes. For example, when Netflix and Spotify are delivering their video or audio, they need encryption to protect their content. We aim to use CPU and GPU to parallelize the algorithm so this process can be executed more efficiently.

**Explain how you contemplate going about it**: As AES is very well-known, there are plenty of existing implementation. We will survey first to find the most efficient one and use OpenMP to parallelize. After done, we will switch to CUDA to parallelize it on GPU. At the end, we will do series of experiments to investigate what is the best threshold to switch from CPU parallelization to GPU parallelization to achieve better performance.

**ECE 759 aspects the proposed work draws on**:

* CPU Parallelism: OpenMP
* Data Locality
* False Sharing
* GPU Parallelism: CUDA

**Deliverables**: We hope to compare the performance of our CPU and GPU implementation, performance of our work and others’ work, and the threshold we find for switching the way of parallelization.

**How you will demonstrate what you accomplished**: As the code is going to be open-sourced, we will try to put a detailed readme on github so that anyone interested can git clone the project and use it according to their needs.

**Other remarks**: