Spring 2025: ECE 759 Final Project Report (Placeholder)

Quick intro:

* Name: Michael Pan
* Email: mpan4@wisc.edu
* Home Department: CS
* Status: MS Student

* Name: Saketh Katta
* Email: katta3@wisc.edu
* Home Department: CS
* Status: MS Student

* Name: Elice Priyadarshini
* Email: epriyadarshi@wisc.edu
* Home Department: ECE
* Status: MS Student

* Name: Ankit Mohapatra
* Email: amohapatra4@wisc.edu
* Home Department: CS
* Status: Undergraduate

* Name: Fahad Touseef
* Email: touseef@wisc.edu
* Home Department: CS
* Status: MS Student

* Name: K M Jamiul Haque
* Email: khaque@wisc.edu
* Home Department: ME
* Status: PhD Student

Project Title:

GPU-Accelerated MD5 Hash Attack

GitHub link to your project:<https://github.com/elicep01/gpu-md5-cracker>

Problem Statement:

The project aims to design and implement a GPU-based MD5 hash attack to efficiently brute-force 7-character alphanumeric passwords. The goal is to optimize the hash computation by leveraging CUDA’s parallelism, demonstrating how HPC can significantly accelerate the processing of compute-heavy tasks.

Motivation/Rationale:

* MD5 hash attacks are a well-known example of a task that benefits tremendously from parallel processing.
* The problem is well-scoped with a clear target (7-character passwords).
* The project provides an opportunity to delve into GPU programming and optimize a real-world algorithm using CUDA thereby showcasing both practical and theoretical HPC concepts.

Project Approach and Methodology:

* Parallel Computing Paradigm: Utilize GPU-parallel computing with CUDA for maximum performance.
* Libraries:
  + CUDA Toolkit: Primary framework for developing and running GPU kernels.

Page **1** of **2**

* + Possible use of CUB/Thrust or other external CUDA libraries: To handle parallel primitives and optimize memory operations.
* Algorithms/Approaches:
  + Implement a CUDA kernel to compute MD5 hashes in parallel for each candidate password. o Optimize the kernel by experimenting with thread blocks, shared memory usage, and library-specific functions to improve throughput.
  + Compare the performance with a serial CPU-based approach to highlight the speedup achieved via GPU acceleration.

ECE 759 Aspects the Proposed Work Draws On:

* GPU programming using CUDA.
* Parallel algorithm design.
* Memory hierarchy optimization.
* Performance analysis and benchmarking.

Deliverables:

* Basic CUDA implementation that computes MD5 hashes in parallel for a subset of the password space.
* Performance benchmarks comparing GPU and CPU implementations.
* Fully optimized and documented project code in the GitHub repo.
* A comprehensive performance analysis report, including discussion on strengths, weaknesses, and scalability of the GPU approach.

How You Will Demonstrate What You Accomplished:

* A working CUDA application that can perform an MD5 hash attack on 7-character alphanumeric passwords, running real-time benchmarks on different configurations.
* Present detailed comparisons (e.g., execution time, throughput) between the GPU implementation and a CPU baseline.
* Explain the implementation decisions, optimization strategies, and usage of CUDA libraries during the final presentation.
* A detailed report and well-commented code in the GitHub repository explaining the design, implementation, and evaluation of the project.

Page **2** of **2**