SHA-256 Benchmark Experiment

Yosef Edery

1 Introduction

In this experiment, we benchmarked the SHA-256 cryptographic hash function's performance on an Apple MacBook Pro with the following specifications:

- **Model Name**: MacBook Pro (16-inch, 2021)
- **Chip**: Apple M1 Pro
- **Total Cores**: 10 (8 performance cores, 2 efficiency cores)
- **Memory**: 16 GB

2 Methodology

We performed the benchmark on a system with a CPU capable of running 10 threads. The experiment was divided into two parts:

1. Benchmarking SHA-256 hashing on a single core.
2. Benchmarking SHA-256 hashing using 10 threads.

The hashing function was implemented using the CommonCrypto library on macOS, and the time taken to compute the hashes was measured using the `clock_gettime()` function for high precision.

3 Results

The following results were obtained from the experiment:

3.1 Single-Core Performance

- Number of hashes: 100,000,000
- Time taken: 34.21 seconds
- Hash rate: 2,923,139.67 hashes/second

3.2 Multi-Threaded Performance (10 threads)

- Number of hashes: 100,000,000
- Time taken: 4.39 seconds
- Hash rate: 22,788,563.61 hashes/second