DPHPC Project Proposal

Neville Walo, Basil Fürer

October 26, 2020

SHA-256 on GPU

Hash functions are one of the most important operations in cryptographic applications. They are also used in data structures like hash tables and for calculating checksums to compare files. The acceleration of this routine is therefore of great importance for many areas.

With the recent rise of the cryptocurrencies, it is as important as never before to hash as fast as possible. Many cryptocurrencies are based on the *proof of work* principle, in which one party (the prover) proves to others (the verifiers) that a certain amount of computational effort has been expended for some purpose. For example, in the Bitcoin protocol [1], users have to find a *nonce* such that the SHA-256 hash of the nonce and the current block is smaller than the current target of the network. Since only the first miner who finds a nonce that fulfills the target receives a reward, it is important to try out many SHA-256 hashes as fast as possible. Today mostly ASICs (application-specific integrated circuit) are used to mine Bitcoins, as ASICs work more efficient and compute more hashes per second than traditional hardware.

The goal of this project is to accelerate SHA-256 computations by using a GPU. While SHA-256 alone does not allow for much parallelization due to sequential dependencies, it is possible to compute multiple hashes at the same time using a GPU. Furthermore, there are other approaches to create parallelizable hash functions like PARSHA-256 [2] and SHA-3 [3].

Our project consists of the following milestones:

- Literature research ($\star$)
- Implement SHA-256 in CUDA [4] ($\star\star\star$)
- Implement PARSHA-256 [2] in CUDA ($\star\star\star\star$)
- (Optional) Implement SHA-3 [3] in CUDA ($\star\star\star\star\star$)
- Evaluate and benchmark our implementation against existing implementations [5] ($\star\star$)

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2009.

[2] Pinakpani Pal and Palash Sarkar. Parsha-256 – a new parallelizable hash function and a multithreaded implementation. In Thomas Johansson, editor, *Fast Software Encryption*, pages 347–361, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[3] Sha-3 standard: Permutation-based hash and extendable-output functions, August 2015.

[4] NVIDIA Corporation. NVIDIA CUDA C programming guide, 2020. Version 11.1.0.

[5] Torsten Hoefler and Roberto Belli. Scientific benchmarking of parallel computing systems: Twelve ways to tell the masses when reporting performance results. In *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, SC '15, New York, NY, USA, 2015. Association for Computing Machinery.