Milestone Report for Research on Oblivious Algorithms

15-400, Spring 2021

Mike Xu
https://mkpjnx.github.io/ObliviousSort/

February 15, 2021

1 Progress Update

Over break, our group has met with Professor Shi briefly. I have set up the repository and build system for the reference implementation, and implemented a first draft in C++. We will be meeting this week to review and improve the components involved. One notable change stems from a misunderstanding I had about the purpose of the reference implementation. I originally focused on trying to make it more performant rather than readable, but Professor Shi clarified that it ought to sacrifice optimizations for the sake of being more straightforward. As the intended use of the reference implementation is just that - a reference from which others can derive more optimized variants.

We have obtained some results from running the reference implementation and measuring the error rate. This error rate comes from the randomized nature of the algorithm and is bounded with respect to parameters in the algorithm. I have written a rudimentary test to measure how the error rate scales with respect to one of the parameters as a sanity check, and the exponential decay of the error rate matches the theoretical bound defined in Professor Shi's paper.

2 Looking Forward

Further investigation is needed to characterize the relationship between the parameters in the algorithm and the security requirements (e.g. error rate $\epsilon < 2^{-40}$) that a potential user may want. Our next step towards actually releasing this reference implementation is to calculate and set the parameters required for a security requirement.

After this, we will begin parallelizing the reference implementation using frameworks such as OpenMP. I anticipate this requiring some rewrites of the code, but generally speaking, the structure of the algorithms already corresponds to the binary fork-join model of parallelism.

3 Milestone Adjustments

For the time being, we have met the first milestone, though code review and discussion will change our goals for the future. Furthermore, our group is now just me and Marcia, so we will need to re-balance the tasks among the two of us. We plan on discussing what the project will look like moving forward in our meeting this week, but this will most likely entail changes to the scope of the project.

4 Resources Required

The requirements have not changed much since the last report, and those requirements are not urgent.