First Milestone Report for
Research on Oblivious Algorithms

15-300, Fall 2020

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

December 19, 2020

1 Progress Update

Since the proposal for the project, our group has met with Professor Shi three times. We continued to review the literature on Oblivious Algorithms and familiarized ourselves with the work we are building upon. Although I feel that our goal became clearer after each meeting, we have not made considerable progress towards the actual implementation. One particular surprise for me was the overhead of translating an algorithm on paper to one in code. Although the pseudocode is clear, many practical considerations arose in the implementation. For example, one particular sub-algorithm makes assumptions about the size of the input that does not translate particularly well to the implementation. To work around this incongruity, I spent more time than I thought I needed to adjust and verify the cost analysis. I hope that with more practice and experience, this translation will take less time.

As the year came to a close and work from other classes ramped up, our group was unable to meet outside of our brief zoom calls with the professor. Additionally some extenuating medical circumstances unfortunately made me unable to work for over a week following thanksgiving. One new goal I would like to set for our group is to learn to better delegate tasks hold each other accountable. The transition from literature review to generating new knowledge and insights is challenging. To avoid becoming directionless in spite of the relatively infrequent intervention of our advisor, we will need to take on more ownership of the project and hold ourselves accountable.

2 Milestone Adjustments

Although we have fallen behind the anticipated pace of the project, the break serves as a buffer to account for this disparity. We plan on maintaining our biweekly milestones for next semester, but will work to meet the goals of the first milestone over the break. We have already set up meetings to report on progress and have a plan over the coming weeks to deliver on the reference implementation.

3 Resources Required

In addition to the resources mentioned in the proposal, one additional requirement is that the testing platform needs to have Intel SGX enabled. This does not pose an issue currently, as I see that my personal machine meets this requirement. However, for other testing platforms, we may need to contact system administrators regarding the configurations.