Aarhus University

Cryptographic Computing project proposal

Alexander Munch-Hansen, 201505956
Casper Vestergaard Kristensen, 201509411
Thomas Carlsen, 201509613

Group one

October 25, 2019

Project Description

The project will revolve around assisting the Alexandra Institute in analysing and implementing oblivious querying of a distributed database. Specifically, we will be looking at the implementation and performance of private information retrieval protocols, which will be used as a primitive in the complete system. As such, we will be implementing multiple protocols which they currently consider in an undecided language of their choosing. We expect that the project will draw upon our knowledge of protocols acquired in the *Protocol Theory* course taught at Aarhus University, as well as require knowledge of cryptographic primitives from the *Cryptology* course (also taught at Aarhus University) and finally, as *PIR* protocols tend to use *Oblivious Transfer*, we will be using *Cryptographic Computing*. Oftentimes, a nice theoretical time complexity won't necessarily guarantee a nice time complexity when used practically, as such, it is of utmost interest to test the implementations, to decide upon which one to use.

Todo

- We must read the survey paper given to us by the Alexandra Institute [1–3]

- Consult Alexandra Institute regarding the specifics of the project.
- Decide upon which language to implement the protocols in.
- Benchmark each protocol in regards to both memory and time complexity.
- Conclude if scope of the project should be extended, based on when we complete previous step.

References

[1] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. Private information retrieval. *J. ACM*, 45(6):965–981, November 1998.

[2] Zeev Dvir and Sivakanth Gopi. 2-server PIR with sub-polynomial communication. *CoRR*, abs/1407.6692, 2014.

[3] William Gasarch. A survey on private information retrieval. *Bulletin of the EATCS*, 82:72–107, 2004.