Shortest Path Computation with No Information Leakage

reviewer: Jinfei Liu
Department of Mathematics & Computer Science, Emory University

In this paper, the authors solved a problem: client inputs his/her source and destination to the server, the client gets the shortest path from source to destination while the server only knows that a query is being executed and can infer nothing else.

1 Positive/Strong Points

1. A very good introduction section, those VLDB papers are really well written and structured.
2. I know how to do the experiment on SMC problem.

2 Negative/Weak Points

1. Too much related work like just for 12 pages, for example, the Obfuscation Methods part is really no help to understand this paper.

2. No privacy proof, no accuracy proof. If the client query several times, it is very easily to reconstruct the whole road network.

3. Based on the PIR and several rounds, the time overhead is really high.

4. The method for client is too professional, actually, the client who just wants to know the shortest path really do not want to do so complex protocols.

5. The time respond is too high, just as the experiments show, it need about 200 seconds for just one query.

3 Research Questions and Points for Discussion

Those questions just as Prof. said, all the background is assumed and here is shortest path, we also could compute neighbor. Hence, those questions are really not practical.