# **Vision Statement - MPC protocol implementation**

**by: Aviad Gilboa, Dolev Dublon, Daniel Zaken, and Yaakov Khodorkovski.**

**Project purpose:**

MPC protocol implantation for APSD (all pairs shortest distance) and SSSD (single source shortest distance) Graph Algorithm problems by the [article of Justin Brickell and Vitaly Shmatikov.](https://drive.google.com/file/d/1-2tmVxaN8rqQBX8J-jSSFEQVgQBnzDEZ/view?usp=sharing)

We have chosen an article that proves the effectiveness of the protocol that we will implement compared to the generic protocol by Yao. The protocol is mentioned in a large number of articles but is not implemented yet (listed only in pseudo-code), therefore researchers cannot use the protocol on concrete problems.

We've decided to implement the protocol and publish it as an open-source project.

**Goals:**

* Learning and understanding the protocol articles in depth.
* Writing an organized working document for the implementation of the protocol.
* Implementation of the protocol at the end of the year.
* Writing an orderly and clear document about the project to make it accessible for general use later.
* The implementation of the protocol in a language relevant to the problems on the subject.

**High-level features:**

* Implementation of MPC while maintaining the principle of safe computation i.e. without information disclosure. (essential feature)
* Clear and explained code. (desirable feature)
* Implementation of the project in the code language used for projects in the MPC field. (essential feature)
* Writing a neat and easy-to-understand Readme in the English language. (essential feature)

**requirements:**

* One professional meeting with the Ph.D.Anat Paskin Levin at least once every two weeks.
* An internal follow-up, learning, and update meeting about three times every two weeks.
* Implementing the protocol code in the most efficient way.