Our project is about Secure Multi Party Computation (MPC), it’s a subfield in information security, the goal is computing a function of a joint private inputs without revealing the inputs. As well-known from Boolean algebra, any function can be implemented with addition and multiplication gates. The addition gate does not require any communication. However, the multiplication gate requires some communication.

In order to make sure every party was honest throughout the protocol, at the end of the protocol there is a verification step which is calculated distributedly.

For that each party stores the output of each multiplication gate that was calculated. At this project we will implement the protocol and supply an analyzation of the run time and confirm/refute the theoretical assumption.