Assignment 02

Instructor: Mehrdad Nojoumian
Course: Secret Sharing Protocols

Deadline: Mar 02

For this assignment, you are supposed to work on Secure Multiparty Computation (MPC). You should work on constructions of simple “addition” and “multiplication” gates.

(1) Either, write a computer program to simulate secure MPC for the aforementioned gates.

Or

(2) Come up with a comprehensive example on papers for addition and multiplication gates.

You can work on prime numbers less than 50, i.e., |Z|<50.

You polynomials should have a degree between 2 and 8, i.e., threshold t=3 to 9.

You should have around 5 to 10 players, i.e., n=5 to 10.

You should demonstrate:

(a) The sharing phase, i.e., the players share their secrets.

(b) Computations in the back box, i.e., at least one addition operation and one multiplication operation with degree reduction.

(c) The recovery phase, i.e., revealing the function value.

Make sure to submit your assignment on Canvas.