CS 203.4860	Secure Multi-Party Computation	Fall 2021

Homework 6: Report

Lecturer: Dr. Adi Akavia *Student(s): ()*

Work space:

We used Python to implement a 1-out-of-2 OT protocol against passive adversary, we used OT to eliminate the dealer we implemented before.

Classes,Functions and implementation:

PKE ElGamal class:

we implemented class with the name PKE Elgamal, with init function which choose a random number p and check if it's prime number and if 2*p+1 is prime too using helper functions we've implemented, in addition it initialize q which is equal to 2*p+1. we also implemented Gen,OGen,Enc and dec as functions in this class as we've learned.

OT class:

OT class is a class we've implemented instead the dealer we've implemented in previous assignments , and it was implemented as we've learned in lectures, init function saves the PKE scheme, load function saves the messages into data variable to use it later,in getkeys function the function gets key as parameter and create a message using enc function we've implemented in PKE ElGamal class. Sendmsgs functions returns the message we've created in getkeys, chose defines sk and pk using Gen and OGen functions we've implemented before(pk and sk same as it was defined in lecture), sendchose returns the pks (Gen and OGen), getData returns output dec as defined in ElGamal cryptosystem in lecture.

TVK class:

In this class we used MACs to authenticate secret shares, this class is almost the same as previous assignments (Expat for the use of multiply MACs per value for security when using $p = 2$).
init function: in this function we get the keys of both Bob and Alice and value and prime p and we calculate Tag and save it in variable t.
add function:loading of the adding symbol, used as the additive secret sharing schema.
mul const function: Multiplying the share by a constant, the input parameter i is the indicator of which player running this commend (Alice or Bob).
add const function: Adding the share by a constant, the input parameter i is the indicator of which player running this commend (Alice or Bob).
str function:Helper function for printing the TVK object which consist of key,value and tag.
and function:Loading of the and symbol for two values and returns null/none if not valid.
kless function: returns TVK object with same tag and value and p.
TKVpair function: returns the pairs $t_{A,x}$, $t_{B,x}$ as taught in class.

BeDOZa Agent:

Instead of defining classes as Alice and Bob we defined BeDOZa Agent which has same functionality as Alice and Bob, We added init function to this class that initializing the circle and all the inputs, we used the OT class instead of the dealer(almost the same class as previous assignments).

circuits:

We've used the same circuits as previous assignments.

Test and complexity:

We tested and checked if all the classes are correct and the output is always right(PKE-ElGamal,1-out-of-2 OT,TVK ,BeDOZa on simple circuit,BeDOZa on Equation3) , we also calculated BeDOZa communication complexity in respect to the security parameter

Execution Time:

We also calculated the executing time by using package time and subtract the start time from the time when we end running the tests and we got different times of execution such as 7.6412622928619385 seconds, 8.687679767608643 seconds, 7.228432655334473 seconds.