Secure and Private Computation
Project Description

May 13, 2025

1 Topic of the Project

The aim of the project is to show how simple functions can be computed privately using MPC. The project requires you to

- Implement a simple Yao protocol for two parties (with AES).
- You can choose from the following functions which is to be computed between two parties using the protocol
  - Sum of a set of values
  - Maximum of two sets of values
  - Minimum of two sets of values
  - Common elements in two sets of values
- The floating point to integer (and vice versa) conversion for this implementation.

1.1 Some Details about Implementation

The implementation **must be done** in Python. Note that

- Your implementation must work for integer inputs of size *at least* 16-*bits*.
- Your implementation must be able to process floating point numbers.
  - your implementation must process decimal inputs with **at least one digit before and after the decimal point**. For example, 1.7, 0.4, 9.9 etc. The number of bits required to represent should be chosen in such way that it can process the floating points. Note that for the addition function the result can have two digits before the decimal point when the inputs are having exactly one digit after decimal points. For example, the addition of 9.9 and 0.2 will be 10.1. Your script should work for such input.

- Your implementation must be such that the inputs for Alice and Bob are given from two different terminals, and suitable outputs must be shown in both terminals. The inputs on two different terminals can be direct e.g. a number or a set of comma separated numbers entered using keyboard. Alternately, your implementation can take the inputs for Alice and Bob from two different files. Your implementation **should have the following outputs**

    1. The communication between Alice sends to Bob [this output is for your own clarity]
    2. OT between Alice and Bob [this output is for your own understanding]
    3. A function which verifies and returns 0/1 after successful or unsuccessful verification of the results (function outputs) obtained using Yao's protocol and in a normal way [this is mandatory]

Your implementation should (at least) work locally. This means that your implementation will not be checked (for correctness) on two different machines on a network but *only on a single computer*.

2 Use of Library

You can use the implementation from Github repository garbled-circuit as a library and guide/inspiration for your own implementation. The library is well documented and there are clear instructions on installation of dependencies, how to run the script with different options etc. It also clearly states the functionalities of each class and member functions. *Pay attention that the library is not using AES.*

The library uses `json` to describe circuit. You can use the same. If you choose to describe circuits differently then you will have to write the script to read the circuits.

3 Documentation and Submission

You are required to submit a document no longer than 2-3 pages (excluding figures), together with your script. It should contain the following

- The version of Python used
- The choice of parameters and function (for Yao's protocol)
- Description of the circuit of the function (and how you chose to describe circuits)
- The functionalities of your implementation with the name of the functions

- Clear instructions on how to run your script (including any dependencies other than those necessary for the Github script) and how to interpret the outputs

For submitting your project, compress the `pdf` file together with script files for your implementation. The (compressed) submission filename should contain your surname for easy identification.

4 Grade Points

Note that

- You are required to provide a demo of your **submitted** implementation. During the demo you will be asked questions related to your implementation.
- Submitting an implementation using any other language than Python will result in no grade points corresponding to your implementation.
- If your program does not allow giving inputs from two terminals (for Alice and Bob) as specified in section 1.1 then you will receive zero points.

The overall points that you receive for your project will be based on

- submitted implementation and documentation
- your demo and answers to the questions asked during the demo

5 Project Rules

1. If you use text verbatim from a source, or if you take a picture, table or the like, you must use quotation marks and make it clear via a citation (including page number or link) what the original source is.
2. If you use any code (fragment) from an existing source (other than the one provided here) that is available publicly then you must mention it in your document and put a reference to the source.
3. If there are copies of any kind (be these parts of source code or the written report), all students involved will receive zero points.
4. If there is any evidence that your source code or part of it was generated using any automatic code generation tool then you will receive zero points.