LELEC2770 – Practical Sessions

Practical Session 1: Two-Party Secure Computations

1. Complete the oblivious transfer protocol written in the file `OT.py`. This is protocol 7.2.4 of the book *Efficient Secure Two-Party Protocols* by Hazay and Lindell [1]. The encryption scheme is the additive El Gamal which is given in the module `utils.py`. Run the `test_OT()` method to check your work.

2. Alice and Bob want to play the *Paper – Rock – Scissors* game. They want to use two party secure computations via garbled circuits to do this. The circuit is defined as follows :

$$\begin{cases} E = & (((A \wedge C) \oplus (B \wedge D)) \oplus ((A \wedge B) \oplus (A \wedge D))) \oplus (B \oplus C) \\ F = & ((A \wedge C) \oplus (B \wedge D) \oplus ((B \wedge C) \oplus (C \wedge D))) \oplus (A \oplus D) \end{cases}$$

   where A, B are the secret inputs of Alice, C, D are the secret inputs of Bob and E, F are the outputs. Inputs meaning :

$$\begin{cases} (0,0) = & \text{means “Paper”} \\ (1,0) & \text{means “Rock”} \\ (0,1) & \text{means “Scissors”} \\ (1,1) & \text{means “Lose”, I give up} \end{cases}$$

   Outputs meaning:

$$\begin{cases} (E,F) = (1,0) = & \text{means “Alice wins”} \\ (E,F) = (0,1) = & \text{means “Bob wins”} \\ (E,F) = (1,1) & \text{means a draw} \end{cases}$$

   Alice is designated the garbler of the circuit and Bob, the evaluator. Following the protocol of Section 3 of the book [1], Alice sends to Bob the garbled circuit. Complete the evaluator class of `garbled_circuit.py` and make Bob evaluate the garbled circuit and reveal the output. Test your work via the `test_garbled_circuit()` method. Keep in mind that the evaluator cannot access the private variables of the garbler and the only interaction allowed for him is to call the method `oblivious_transfer(...)` of the garbler. The oblivious transfer methods depend on the `OT.py` module of Exercise 1.

3. Implement the “Free-Xør” optimization on the previous circuit and benchmark your result with the non-optimized case by running many instances of the garbled circuit.