CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Secure Multi-Party Computation

CS 523 – Live Exercises

Wouter Lueks | February 25, 2025 | v1.0.2

Assignment
Old Exam Question 1/3

Alice is a private collector of toy cars and she wants to check if Bob (another collector) owns cars that are not present in Alice's collection. Neither of them wants to disclosure which cars they have before the negotiations. Your task is to implement a circuit that let's Alice answer her question? (Alice is considered to be a client and Bob to be a server).

Assumption: The sets of existing toy cars is small, and you can enumerate it.

Question (was not on exam): *Formulate the problem that we are trying to solve.*

Assignment
Old Exam Question 2/3

We denote Alice's car set with $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ where **x** is a bit vector where the bit $x_i = 1$ if Alice owns car model "*i*". We denote Bob's collection $y = (y_1, \ldots, y_n)$ similarly.

Then lets design a SMC protocol:

1. The server (Bob) creates a garbled circuit *C* that operates on **x** and **y** and sends it to the client (Alice)
2. The client interacts with the server to evaluate the circuit *C* on the client bit vector **x** and the server bit vector **y**. The client learns the output z = *C*(**x**, **y**).
3. The client computes whether there are common elements in sets **x** and **y** based on z

Question: *Specify the circuit C. Assume that Bob and Alice can implement OR< AND and NOT gates.*

Assignment
Old Exam Question 3/3

Suppose the client is honest-but-curious in your protocol (i.e., the protocol above instantiated with your circuit from the previous question).

Question: *Can the client learn anything more about the server's set than the target expression?*