CSCI1515 Capstone - GMW Multi-Party Computation

Nathan Andrews
nathan_andrews@brown.edu
Brown University

Abstract

In CSCI1515, I implemented secure two-party computation using Yao's Garbled Circuits for a class assignment. For my capstone, I implemented a different method to achieve secure multi-party computation (MPC) for an arbitrary number of parties: the Goldreich-Micali-Wigderson (GMW) protocol. In essence, there are n parties that want to compute the output of some function f. Each party P_i has some input x_i. The parties want to compute $f(x_1, x_2, \ldots, x_n)$ while keeping all of the inputs secret. I implemented this GMW protocol to support MPC across an arbitrary number of parties using functions made up of NOT, XOR, and AND boolean circuits. Additionally, my implementation provides security against a semi-honest adversary. Performance benchmarks indicate that GMW is slower than Yao's Garbled Circuits, with a 300% increase in execution time of the same circuit with the same number of parties by GMW over Yao's. However, the tradeoff between the slower execution time is the ease with which GMW can compute functions with an arbitrary number of parties.