Yao's Garbled Circuit Optimizations with Half Gates

Divyam Dang, Harisen Luby

Brown University

Two party computation (2PC) is a standard topic in cryptography where two parties want to evaluate some function over two inputs without either party learning the other's information. This feat is accomplished by constructing a Yao's garbled circuit and using it to evaluate the data anonymously. Construction involves translating a given logic circuit used for evaluation into an indecipherable representation to hide the computation and input values from other parties. This, along with oblivious transfer of input labels, allows for secure two party computation. We implemented a basic Yao's garbled circuit protocol as regular coursework in CSCI1515, but revisited our implementation for our capstone project to optimize the hash complexity and data transfer between the garbler and evaluator over the whole protocol.

To accomplish this, we implemented a few optimization techniques such as point-and-permute, which reduces the number of calls to the hash function made by the evaluator; free XOR and NOT gates, which evaluate XOR and NOT gates with no hashing needed; and half gates, which consolidate the total number of ciphertexts representing AND gates from four to two while maintaining security guarantees of basic Yao's garbled circuits.