Two-Party Computation for Decision Making

Two-Party Computation allows Alice and Bob to jointly compute a function of their choice, without revealing their respective inputs. As an instance, these cryprographic primitive can be used in order to add a privacy layer to decision forest evaluation. Decision forests are classical models to efficiently make decision on complex inputs with multiple features. While the global structure of the trees or forests is public, sensitive information have to be protected during the evaluation of some client inputs with respect to some server model. Indeed, the comparison thresholds on the server side may have economical value while the client inputs might be critical personal data. In addition, soundness is also important for the receiver. In our case, we will consider the server to be interested in the outcome of the model evaluation so that the client should not be able to bias it. In this paper, we proposed a new offline/online protocol between a client and a server with a constant number of rounds in the online phase, with both privacy and soundness against malicious clients. The talk will introduce this protocol, preceded by the main two-party computation primitives used.