Monash University
FIT 5124: Advanced Topics in Security
Week 8 Tutorial Sheet

Ron Steinfeld, 22 April 2015

In this week's tutorial we will look at private computation protocols and applications / implementations.

Problems

1 **1-of-N OT protocol.** Consider the basic Diffie-Hellman based 1-of-2 OT protocol from the lecture (secure aga against semi-honest attacks). Design a natural generalization of this protocol to a 1-of-N OT protocol, for any integer $N \geq 2$? Discuss whether or not your protocol is secure against malicious attacks.

2 **Yao's Millionaires problem.** Yao's millionaires problem involves two millionaires Alice and Bob, who wish to determine which one of them is richer, without revealing to each other any other information about their fortunes. The abstract problem of numerical comparison of course also has relevance in providing privacy for other applications, such as an online auction, where a bidder submits a bid and the auctioneer has a minimum acceptable selling price ('reserve price'). Design a protocol for solving the millionaires problem, using a 1-of-N OT protocol and explain why it provides privacy for the both parties against semi-honest attacks, assuming the OT protocol is secure against semi-honest attacks. How does the communication and computational efficiency of your protocol scale with the maximal size M of the amounts being compared in the protocol?

3 **Yao's Garbled Circuit for the Millionaires problem.** Suppose we applied Yao's general garbled circuit protocol to Yao's Millionaire's problem. How does the communication and computational efficiency of this protocol scale with the size M of amounts compared?

4 **Optimized Implementation Compilers for Yao's Garbled Circuit Protocol.** Explore one or more of the implementation compilers of Yao's garbled circuit protocol, as referred to in the lecture. This will be useful for Assignment 2 (soon to be posted online!).