RUNI: Blockchains and Cryptocurrencies

Exercise 1

Submitted by: **Yarden Fogel (yarden.fogel@post.runi.ac.il)**
Partner: Liron Cohen (liron.cohen@post.runi.ac.il)

1 Question 1: Dolev-Strong Validity Proof

Claim 1. *The Dolev-Strong protocol satisfies validity*

This is to say that if the sender is honest, then all honest nodes (or generals or parties) will output the sender's input bit.

Proof. To support this claim and complete our proof, the validity proof depend on the following assumptions:

□

Assumption 1. ***Honest Sender:***

The sender is honest, as given, and as required to evaluate validity

Assumption 2. ***Synchronous Protocol:***

The protocol is synchronous, and all messages broadcasted at time t, as the protocol is executed in some unit of time which we refer to as round r, are received by all participating nodes or receiving parties by the start of time $t + 1$ or, round $r + 1$.

Assumption 3. ***Ideal Signatures Assumption:***

Signatures cannot be forged or fabricated by a malicious party and therefore a verified signature is in fact authentic and valid.

Additionally, at the start of the protocol ($r = 0$), once a message in the form $< (b, i, s) >$ is signed by the sender - where b is the sender's input bit, i is the sender's id, and s is the sender's authentic signature (requiring the sender's secret key sk as an input) - no changes can be made to that authentic signature and the signed message tuple, and it can never be replaced or removed from the valid list of messages.

Protocol Proof: At time $t = 0$ or round $r = 0$, the honest sender will send his valid input bit b' to all other nodes or parties, and due to the synchronous protocol, they are all required to receive that message (in the form $< (b, i, s) >$) by the start of time $t + 1$ or round $r + 1$.

By this time already, every honest node is already convinced of the value of the "real" b', as it has met the requirements of - an honest sender - a valid unforgeable signature by the sender - and according to Dolev-Strong, the number of distinct signatures received at the start of the round ($r = 1$) is in fact equal to r and includes the sender's signature.

At this time, all honest nodes receiving the valid bit b' will be convinced and there will be no way for any corrupt or malicious actor to convince any honest node after that, of any value for the valid input bit other than that same b' that they received and authenticated.

We had designs and an outline for a full inductive proof, but were simply not afforded the time to do the work properly as we'd like, instead spending many dozens of hours on spaces, indentations, unknown issues, and formatting styles. We hope this suffices.

QED

Compiled with LaTeX on December 7, 2022.