ECE598 Ideal Functionalities, Spring 2022
Lec 7: Impossibility Proof of Commitments in Plain Model

Lecturer: Andrew Miller
Scriber: Tzu-Bin Yan (tbyan2)

Date: Feb 8, 2022

1 Lecture overview

In this lecture, we looked at the negative result on it being impossible to have a universally composable commitment protocol without relying on ideal functionalities, such as the $\mathcal{F}_{RO}$ or $\mathcal{F}_{CRS}$ (common reference string) we saw in past lectures, for simulator committed message extraction. This is achieved by showing that for any such protocol, we can always find an environment/distinguisher that can differentiate between the ideal and real world for the protocol. In addition, an exercise was given to help the students familiarize themselves with proving impossibility results.

2 Commitment impossibility result

The commitment impossibility result was given by Canetti and Fischlin in [1]. The theorem stated is provided as follows:

Theorem 1. *There exist no bilateral, terminating protocol π that securely realizes functionality $\mathcal{F}_{COM}$ in the plain model. This holds even if the ideal-model adversary S is allowed to depend on the environment Z.*

To prove the impossibility result, the first step is to assume that such a protocol exists, and then show that either

- we can come up with an environment that can always distinguish between the ideal and real world for the protocol, or
- there is a contradiction based on the assumption.

For this impossibility result, we will prove by showing that such a distinguishing environment exists. Before looking into the full proof, we will first consider a simpler scenario - the sender-corrupt case, which will be the building block to the full proof.

2.1 Building block - the sender-corrupt case

Consider the ideal world of the sender-corrupt case for the protocol π. The environment Z_S selects a random bit b, and then runs the sender-part of the protocol (π_s) within Z_S to commit b following π. As we are in the ideal world, the sender simulator Sim_S receives messages from Z_S, and generates any honest receiver protocol messages back to Z_S to provide the view as if Z_S is in the real world. As π is a UC commitment protocol, we have Sim_S will at some point commit a bit b' to $\mathcal{F}_{COM}$ where $b = b'$.

2.2 Full proof

We now utilize the building block to construct the distinguishing environment. Consider the receiver-corrupt case for protocol π. The environment Z_R randomly samples a bit b and requests the honest sender to commit b. However, note that Z_R *NEVER* requests the honest sender to decommit b. Z_R also simulates (*run in a sandbox*) the whole building block scenario inside Z_R, where the sole difference is that instead of Z_S picking b and running π_s directly within, Z_R now just forwards the messages returned by the dummy adversary (which is either generated by the honest sender following π_s, or by Sim_R to provide the view as if Z_R is in the real world) to Z_S (and in turn to Sim_S in the sandbox), and use the Sim_S generated messages (mimicking honest receiver messages) as the messages supplied to the dummy adversary, which are then either supplied to Sim_R in the ideal world or directly to the honest sender in the real world. Z_R then gives its guess based on the committed bit b' by Sim_S inside the sandbox, where Z_R guesses it is in the real world if $b' = b$.

Observe that in this case, Z_R is a valid distinguishing environment that distinguishes between the ideal and real world for the receiver-corrupt case.

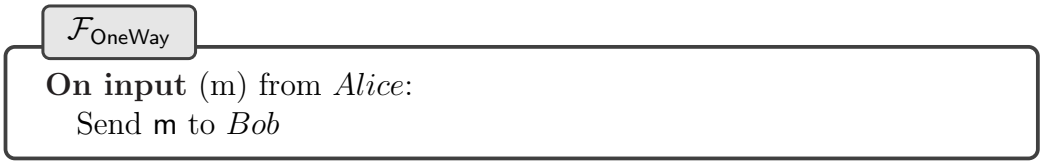

Figure 1: One way channel ideal functionality.

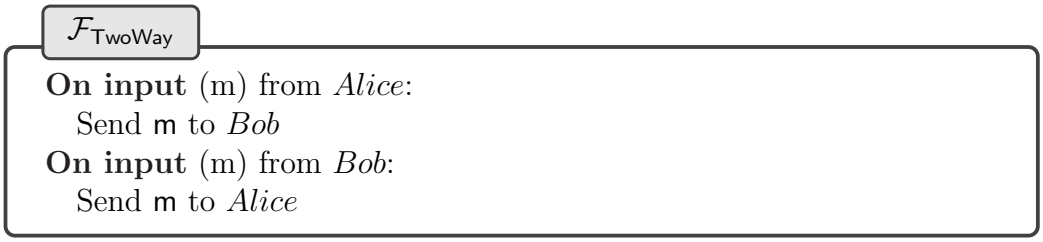

Figure 2: Two way channel ideal functionality.

This is because, in the real world, Sim_S will be acting on real protocol π messages and will successfully extract the committed bit b. However, in the ideal world, as no information regarding b is ever disclosed to Sim_R (and in turn to Sim_S, as b was never decommitted), we have b' outputted by Sim_S in the ideal world must be statistically independent of b. We thus have a distinguishing environment that can always distinguish between the ideal and real world for arbitrary such assumed protocol π. □

3 Exercise

The in-class exercise for this lecture is to show the following:

Show that $\mathcal{F}_{TwoWay}$ is stronger than $\mathcal{F}_{OneWay}$.

To do this, effectively one will need to show that for any protocol π that realizes $\mathcal{F}_{TwoWay}$ with $\mathcal{F}_{OneWay}$, we can always find an environment that distinguishes between the ideal world and the real world for π.

References

[1] R. Canetti and M. Fischlin. Universally composable commitments. In *Proceedings of the 21st Annual International Cryptology Conference on*

Advances in Cryptology, CRYPTO '01, page 19–40, Berlin, Heidelberg, 2001. Springer-Verlag.