ETH Zurich, Department of Computer Science
SS 2020

Prof. Ueli Maurer
Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 12

12.1 Shared Accounts and Escrow Services

a) Extend the account scheme seen in the lecture such that it allows for accounts which are owned by n parties, and where transactions can be approved by k out of n of the parties owning the account.

b) An escrow service allows mutually distrusting parties to exchange goods for payments. Build an escrow service using the extended account scheme from a), for the setting where A wants to buy a good from B. For that, assume that there is a trusted judge J that can participate in case there is a dispute. Moreover, we require that if both A and B are honest, the judge should not participate.

12.2 Decoupling Parties and Users

In the lecture we have seen a protocol that allows to decouple parties and users. In this protocol, a user needs to request a block from all parties and then do a majority decision.

a) Eve proposes the following scheme to improve efficiency: Each king broadcasts a *signed* block. Now, if a user requests a block from a party, it also gets the signature. The user accepts the block if the signature of the king is valid. Why is this a bad idea?

b) Come up with a fix for Eve's protocol such that if a user asks a single party, the user has a method to identify whether the block was wrong. How many parties does a user need to query (in worst-case) to ensure that he gets the correct block?