Security 1 - Mandatory Hand-in 2

Sam Al-Sapti (sals@itu.dk)

October 12, 2022

- Pedersen commitments, Alice and Bob first send `c`, then each of them send `r,m` (confidentiality and integrity). Coin tossing protocol.
- Digitally sign each message (authenticity).
- Key exchange to establish symmetric encryption scheme (TLS).
- Self-sign certificates.
- ALTS: https://grpc.io/docs/languages/go/alts/

Protocol steps:

1. Alice and Bob does an authenticated key exchange to obtain a shared symmetric encryption key.
2. Alice and Bob does coin tossing with Pedersen commitments.
3. Each message is encrypted using the shared symmetric key, and signed.