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.