ETH Zurich, Department of Computer Science
SS 2017

Dr. Martin Hirt
Chen-Da Liu Zhang

Cryptographic Protocols
Exercise 11

11.1 Information-Theoretic Commitment Transfer Protocol

a) Consider the information-theoretically secure (distributed) commitment scheme from the lecture. Describe the state achieved by the COMMIT protocol, i.e., describe the output of each player and the consistency condition among these outputs.

b) Design a commitment transfer protocol CTP for a COMMIT-state. Show that your protocol is secure.

11.2 Information-Theoretic Commitment Multiplication Protocol

a) Show that the commitment multiplication protocol for the generic information-theoretic secure MPC from the lecture is secure for $t < n/3$, i.e., that it satisfies the properties:

1. CORRECTNESS: At the end of CMP, either the dealer D is committed to d such that $d = ab$, or it is publicly seen that D is corrupted.
2. PRIVACY: Up to t players (not including D) obtain no information on the values a and b.

b) Show that the protocol CMP is insecure if $t \geq n/3$.

HINT: Show that if $n = 3t$, then an adversary corrupting t players (including D) can achieve that at the end of the protocol player D is committed to some $d' \neq ab$.

11.3 Commitment Multiplication Protocol for ElGamal

Recall the ElGamal commitment scheme. The blob function maps elements of $\mathbb{Z}_q \times \mathbb{Z}_q$ to elements of $G \times G$, where q is a prime number and G is a cyclic group of order q. More concretely, it takes the value $a \in \mathbb{Z}_q$ and randomness $\alpha \in \mathbb{Z}_q$ and outputs a pair $A := (g^\alpha, \gamma^a h^\alpha)$, where g, h and γ are generators of G.

Provide a commitment multiplication protocol CMP for this commitment scheme.