

# Cryptographic Protocols

## Exercise 10

### 10.1 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 commitment created via COMMIT. Show that your protocol is secure. How many corrupted players can be tolerated?

### 10.2 Information-Theoretic Commitment Multiplication Protocol

- a) Show that the commitment multiplication protocol (CMP) 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  $c$  such that  $c = ab$ , 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  $c' \neq ab$ .

### 10.3 Information-Theoretic Commit Protocol

The Commit-Protocol from the lecture requires up to  $t$  rounds of accusations (Step 3). In this exercise, we prove that two rounds of accusations are sufficient.

Prove that after two rounds of accusations, either

- the dealer is disqualified ( $> t$  accusations in rounds 1–2), OR
- all accusations in Round 2 are by corrupted parties.

Use the following notation: Let  $H$  denote the set of honest parties and  $A_i$  denote the set of parties accusing the dealer in Round  $i$  (for  $i \in \{1, 2\}$ ).

*Hint:* If  $|A_1| \leq t$ , then  $H \setminus A_1$  define a unique degree- $t$  polynomial  $f'(x, y)$ .