ETH Zurich, Department of Computer Science
SS 2021

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

Cryptographic Protocols
Solution to Exercise 11

11.1 Information-Theoretic Commitment Transfer Protocol

a) At the end of protocol Commit, there exists a polynomial g of degree at most t. If the dealer is honest, then he outputs g, and $g(0)$ is the committed value s. Every honest party P_i outputs the commit-share $s_i = g(\alpha_i)$.

b) The commitment transfer protocol CTP allows to transfer a commitment from a player P to a player P' The protocol works as follows:

1. P sends the polynomial g to P'.
2. Each P_i sends s_i to P'.
3. P' checks that the degree of g is at most t, and that all but at most t of the received s_i's lie on g. If so, he accepts $g(0)$ as value for s, otherwise he assumes that he did not receive any value for s.

The above protocol is secure for $t < n/3$:

Privacy: Straight-forward as only P' receives values in the protocol and he only obtains the values which he is supposed to receive.

Correctness: This can be argued along the lines of the correctness of the protocol Open from the lecture notes: Assume that P sends P' some wrong polynomial $g' \neq g$. Then, at most t of the commit shares can lie on polynomial g'. Hence the commit shares of at least $n - t$ players do *not* lie on g'. As at most t of those players might be corrupted, there are at least $n - 2t > t$ players who will send commit shares that do not lie on g' to P', and therefore P' will not accept $g(0)$ as value for s.

11.2 Information-Theoretic Commitment Multiplication Protocol

In the following we will use f_a and f_b to denote the polynomials used in the commitment sharing protocol (CSP) to share the values a and b, respectively. Furthermore, let $f_c := f_a \cdot f_b$.

a) We show that correctness and privacy are satisfied:

Privacy: In steps 1-2, privacy is guaranteed by the privacy of the CSP, i.e., no information on a, b, and c is revealed in these steps. In step 3, the players only see values they already know, namely $c_i = a_i \cdot b_i$, hence again no information is revealed. Finally, the commitments to some a_i, b_i, and c_i are opened only if D or the player P_i is corrupted, which means that the adversary already knows them.

Correctness: Any dealer who is not disqualified must successfully complete the CSP for values a and b. Thus, every player P_i ends up with shares a_i on f_a and b_i on f_b. Suppose, D commits to a value $c' \neq c$ and shares it using a polynomial

$f_{c'} \neq f_c = f_a \cdot f_b$ in protocol CSP.[1] Since both f_c and $f_{c'}$ have degree at most $2t$, they can have at most $2t$ points in common. Thus, there exists at least one honest player P_i for which $c'_i \neq a_i b_i$, where c'_i is his share of c'.[2] This player will accuse the dealer and prove that he is corrupted by opening a_i, b_i, and c_i.

b) Let $n = 3t$, and assume that the players $P_1, \ldots, P_t$ are corrupted, where P_1 plays the role of D. In order to achieve that at the end of the protocol the players accept a false $c' \neq ab$, the corrupted players have the following strategy:

1. In step 0, D chooses c' (instead of c) and is commited to it.
2. Step 1 is executed normally, i.e., D invokes the CSP for a and b.
3. In step 2, D invokes the CSP for c', with the (unique) degree-$2t$ polynomial $f_{c'}(x)$, such that $f_{c'}(0) = c'$ and

$$f_{c'}(\alpha_i) = f_a(\alpha_i) \cdot f_b(\alpha_i)$$

   for $i = t+1, \ldots, n$.
4. The corrupted players do not complain in step 3.

As $f_{c'}(x)$ is chosen such that it satisfies the consistency check for all honest players, no player will complain and the commitment to c' will be accepted.

11.3 Information-Theoretic Commit Protocol

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

Consider the set X of honest parties that do not accuse the dealer in the first round of accusations, i.e., $X = H \setminus A_1$. Observe that these parties must have pairwise consistent polynomials $h_i(x)$ and $k_i(y)$. In order to see this, assume that two honest parties P_i and P_j have received inconsistent polynomials in Step 1, e.g., $h_i(\alpha_j) \neq k_j(\alpha_i)$. Then P_i and/or P_j complain (in Step 2), and P_i and/or P_j accuse in Step 3.

Furthermore, we have $|H| \geq 2t+1$, and $|A_1| \leq t$ (or the dealer is disqualified), and so $|X| \geq t+1$. Hence, the polynomials $h_i(x)$ and $k_i(y)$ of the parties in X define a unique degree-t polynomial $f'(x, y)$.

Now consider an accusation in Round 1 of some $P_i \in A_1$, then the dealer must broadcast the polynomials $h_i(x)$ and $k_i(y)$. We focus on $h_i(x)$, but the same holds also for $k_i(y)$. The polynomial $h_i(x)$ is either in $f'(x, y)$, i.e., $h_i(x) = f'(x, \alpha_i)$, or it has at most t points in common with $f'(x, \alpha_i)$. In the first case, no honest party will accuse in Round 2, and in the second case, at least $|X| - t$ honest parties will accuse in Round 2. However, if there are $|X| - t$ accusations in the second round and $|A_1| \geq |H| - |X| \geq 2t + 1 - |X|$ accusations in the first round, then the dealer is disqualified.

[1] Note that the dealer cannot share c' using f_c as can easily be seen by inspecting the CSP.

[2] The condition $t < n/3$ implies that there are at least $2t + 1$ honest players.