ETH Zurich, Department of Computer Science
SS 2018

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

Cryptographic Protocols
Exercise 9

9.1 Not Sending Values

Consider the case where the at most $t < n/2$ corrupted players can withhold information (but do not send wrong values).

For a finite field $\mathbb{F}$, let $[a] = (a_1, \ldots, a_n)$ be a sharing of a value $a \in \mathbb{F}$ among the players $P_1, \ldots, P_n$. The share a_i of P_i is a point on some polynomial $f \in \mathbb{F}[X]$ of degree at most t, i.e., $a_i = f(\alpha_i)$, where $\alpha_1, \ldots, \alpha_n$ are distinct values in $\mathbb{F} \setminus \{0\}$.

Devise a protocol that allows the players to reconstruct a share of a corrupted player. Keep in mind that in your protocol up to $t < n/2$ players can be corrupted and may not send values they are supposed to send.

9.2 ElGamal Commitments

The ElGamal commitment 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 precisely, the ElGamal commitment to a value $a \in \mathbb{Z}_q$ with randomness $\alpha \in \mathbb{Z}_q$ is a pair $A := (g^\alpha, \gamma^a h^\alpha)$, where g and γ are (fixed) generators of G and h is a randomly chosen element of G.[1]

a) Show that ElGamal commitments are homomorphic with respect to addition.

b) Prove that ElGamal commitments are perfectly binding.

c) Prove that the ElGamal commitment scheme is computationally hiding under the assumption that the *decisional Diffie-Hellman (DDH)* problem is hard, i.e., under the assumption that it is computationally hard to distinguish (for a fixed generator g) triples (g^u, g^v, g^{uv}) from triples (g^u, g^v, g^w) for randomly chosen exponents u, v, w.

9.3 Multi-Party Computation from Homomorphic Commitments

Consider a (non-interactive) commitment scheme characterized by a function $C : \mathcal{X} \times \mathcal{R} \to \mathcal{B}$, where $\mathcal{X}$ is the space of committable values, $\mathcal{R}$ is the randomness space, and $\mathcal{B}$ is the blob space. Assume that C is homomorphic, i.e., that $\mathcal{X}$, $\mathcal{R}$, and $\mathcal{B}$ are groups and that C is a group homomorphism.

The goal of this task is to adapt this commitment scheme such that it can be used in an MPC.

a) Construct a protocol Commit that allows a player P to commit towards all players to some value $x \in \mathcal{X}$.

b) Provide a protocol Open that allows a player P to open a certain commitment to some player P'. Moreover, provide a protocol Open$'$ that allows P to open a commitment to all players.

c) Construct a commitment transfer protocol CTP that allows to transfer a commitment from a player P to some other player P'.

d) Finally, provide a commitment multiplication protocol CMP.

[1] Assume that h is chosen during a setup phase such that neither the sender nor the receiver knows its discrete logarithm w.r.t. g.