Homework 1

Cryptography
CS 598 : Spring 2016

Released: Thu Jan 21
Due: Tue Feb 2

Exercise on Secret Sharing [Total 25 pts]

1. Alice and Bob are given two integers x and y, respectively, both in the set $\{0, .., n\}$. Devise a protocol (over private, point-to-point channels) among Alice, Bob and Carol, so that at the end of the protocol, Carol outputs $x + y$, but learns *nothing more* about x and y. That is,

$$\forall x_1, y_1, x_2, y_2 \in \{0, \cdots, n\} \text{ s.t. } x_1 + y_1 = x_2 + y_2, \quad \text{View}_{\text{Carol}}(x_1, y_1) = \text{View}_{\text{Carol}}(x_2, y_2),$$

   where $\text{View}_{\text{Carol}}(x, y)$ denotes the distribution of the view of Carol[1] in your protocol when Alice and Bob's inputs are x and y respectively. Also, we require that Alice and Bob learn *nothing* about each other's inputs:

$$\forall x, y_1, y_2 \in \{0, \cdots, n\}, \quad \text{View}_{\text{Alice}}(x, y_1) = \text{View}_{\text{Alice}}(x, y_2),$$
$$\forall x_1, x_2, y \in \{0, \cdots, n\}, \quad \text{View}_{\text{Bob}}(x_1, y) = \text{View}_{\text{Bob}}(x_2, y).$$

   You may assume that all three parties will follow your protocol honestly. Briefly argue that your protocol indeed satisfies all three secrecy conditions, and gives the correct output to Carol. [20 pts]

   (Hint: Use additive secret-sharing over a suitable finite group.)

2. The problem gets trivialized when any one of the 3 secrecy conditions are removed. Suggest 3 *deterministic* protocols for the above problem, when each of the three secrecy conditions is removed and only the other two are required. [5 pts]

[1] The view of a party consists of its input and the random coins used by it (if any), as well as all the messages received by it during the protocol.