

# Homework 1

Cryptography  
CS 598 : Fall 2014

Released: Tue Sep 2  
Due: Thu Sep 11

## Exercise on Secret Sharing

[Total 25 pts]

1. Alice and Bob are given two integers  $x$  and  $y$ , respectively, both in the set  $\{0, \dots, n\}$ . 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,

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

where  $\text{View}_{\text{Carol}}(x, y)$  denotes the distribution of the view of Carol 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:

$$\forall x, y_1, y_2 \in \{0, \dots, n\}, \text{View}_{\text{Alice}}(x, y_1) = \text{View}_{\text{Alice}}(x, y_2),$$

$$\forall x_1, x_2, y \in \{0, \dots, n\}, \text{View}_{\text{Bob}}(x_1, y) = \text{View}_{\text{Bob}}(x_2, y).$$

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

[20 pts]

2. Suggest 3 simple protocols for the above problem, when each of the three secrecy conditions is removed and only the other two are required. [5 pts]