KFUPM
College of Computer Science and Engineering
Computer Engineering Department
COE 449: Privacy Enhancing Technologies

Fall 2019 (191)

Assignment 3: Due date Thursday 21/11/2019

Tasks

Question1: Oblivious Transfer (OT) (50 pts)

(a) (20 points) Implement 1-out-of-2 with Socket programming using a programming language of your choice. The program should be run on two machines (or two terminals) to emulate a sender, i.e., Alice, and a receiver, i.e., Bob. Alice will generate two messages, e.g., two numbers, and will send exactly one number to Bob. On other hand, Bob needs to choose which number he wants to receive. When received, Bob should know nothing about the other number with Alice, and Alice should not know which number Bob chose.

(b) (20 points) Give a simple, deterministic protocol for 1-out-of-n OT. Assume that both Alice and Bob are honest-but-curious. In your protocol, Alice and Bob can access the 1-out-of-2 functionality n times. (Hint: Think of how to extend 1-out-of-2 to 1-out-of-3 and then generalize it to 1-out-of-n)

(c) (10 points) Implement the 1-out-of-n OT protocol in the previous task.

Question2: Homomorphic Encryption (20 points) Consider Elgamal encryption (`http://homepages.math.uic.edu/~leon/mcs425-s08/handouts/el-gamal.pdf`)

(a) (10 points) Is Elgamal encryption additive homomorphic?

(b) (10 points) Is Elgamal encryption mulitplicative homomorphic?

Question3: Dining Cryptographer (30 points) In the lecture, we discussed the Dining Cryptographers protocol. In this problem, we will explore how to use that protocol as a building block to construct a general protocol for anonymous communication. Consider a group of n agents. [1]

(a) Describe a protocol using which one of the n agents can send an m-bit message. Explain informally why the protocol is correct (i.e., all agents receive exactly the message that was sent) and anonymous (i.e., none of the other agents have any clue who the real sender is).

(b) Sketch a prove that the anonymity is preserved by the protocol for the case where n = 4 and m = 1. (You need to show that from the point of view of any non-sender, the probability of any of the other agents being the sender is 1/3).

[1] You may want briefly read this paper `https://sites.cs.ucsb.edu/~ravenben/classes/595n-s07/papers/dcnet-jcrypt88.pdf`