ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

HS 2022

Prof. R. Wattenhofer
Ard Kastrati

Computational Thinking
Exercise 6 (Cryptography)

1 Zero Knowledge Proofs in Geometry

Peggy and Vic live in a world where they can only use a compass and a ruler (without markings[1]). That is, they can only use operations that we know from high school, such as drawing a line through 2 points, drawing a circle, intersecting lines and circles and so on.

a) As a warm up, show how can you find the middle point between two points, copy circles, copy angles, add and subtract angles, and finally construct the half of a given angle.

In the following, we consider the problem of trisecting an angle, meaning construction of an angle equal to one third of a given arbitrary angle. This problem was proposed by ancient Greeks, and only after 2000 years it was proven that it is impossible. Of course, if we are allowed to use other operations like measuring angles, algebra, the problem is solvable. However, we assume Peggy and Vic live in a world where only the use of the ruler (without markings) and compass is possible.

b) Peggy wants to prove to Vic that he has the trisection α (drawn in a paper) of a publicly known angle $\beta = 3\alpha$. Construct an interactive protocol that allows him to prove this claim without revealing any information about the angle α to Vic. Show that your protocol achieves completeness, soundness. In addition, argue about the zero knowledge property: can Vic convince a third party that Peggy knows the trisection?

2 MPC with Secret Sharing

a) Let s_1 be shared to n parties through polynomial $f_1(x) = s_1 + a_1 x + ... + a_{t-1}x^{t-1}$ and s_2 similarly through a different polynomial $f_2(x) = s_2 + a'_1 x + ... + a'_{t-1}x^{t-1}$. Each participant P_i holds the shares $(x_i,\ f_1(x_i))$ and $(x_i, f_2(x_i))$. Show that by summing locally the shares — that is, if each party P_i computes locally $(x_i, f_1(x_i) + f_2(x_i))$ — one gets a sharing of $s = s_1 + s_2$.

In the lecture, we have seen the 3Sum MPC protocol. Dave is a new member of the group and wants to be part of the protocol as well.

b) Describe a protocol where Alice, Bob, Carol and Dave compute their sum of the salary (i.e. 4Sum MPC protocol).

Alice and Carol don't like Bob and Dave, so they form a coalition where they tell their income values to each other and want to find out what the salary of Bob and Dave is.

c) How can Alice and Carol *together* find out the income of Bob and Dave?

d) Can you design a protocol where Alice and Carol cannot find the salary of Bob and Dave even if they tell their income salaries to each other?
Hint. Use secret sharing.

[1] They cannot measure distances in meters