ETH Zurich, Department of Computer Science
SS 2019

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

Cryptographic Protocols
Exercise 3

3.1 Geometric Zero-Knowledge

In this exercise we consider geometric constructions using a ruler (without markings) and a compass (Lineal and Zirkel). The operations we consider are those that we know from high school, namely to draw a line through two points, to draw a circle with center at one point that goes through another point, to obtain the intersection between two lines/two circles/a line and a circle, and to copy circles.[1][2]

a) An *angle* is a geometric object consisting of two rays (half-lines) with a common end point. Show how one can add and subtract two angles, i.e., given angles α and β, construct $\alpha + \beta$ and $\alpha - \beta$ using the above operations.

A well-known result from abstract algebra states that the trisection of an arbitrary angle cannot be drawn in the above sense.

b) Peggy claims that she knows[3] the trisection α of a publicly known angle $\beta = 3\alpha$. Construct an interactive protocol that allows her to prove this claim. You may assume that Peggy can generate a random point on a circle and that Vic can flip a fair coin.

c) Prove that your protocol is complete and argue (informally) why it is a proof of knowledge.

d) Prove that your protocol is zero-knowledge.

3.2 Honest-Verifier Zero-Knowledge and c-Simulatability

In this exercise, we investigate the relation between HVZK protocols and c-simulatable protocols. It is easy to see that any c-simulatable protocol is also HVZK, while the converse is generally not true.

However, one can prove that any 3-round HVZK protocol with challenge chosen uniformly from a challenge space $\mathcal{C}$, can be transformed into a c-simulatable protocol. More concretely, given an HVZK protocol (P, V) for relation R (P proves knowledge of a witness w for an instance x such that $(x, w) \in R$), find a c-simulatable protocol (P', V') for R.

3.3 An Interactive Proof

Let G be a cyclic group of prime order (i.e., $|G|$ is prime) and let $g, h \in G$ be publicly known.

a) Construct a *zero-knowledge* interactive proof protocol that, given some $z \in G$, allows Peggy to convince Vic that she knows some pair (x, y) such that $z = g^x h^y$. Prove that your protocol is complete and argue (informally) why it is a proof of knowledge.

b) Prove that your protocol is zero-knowledge.

[1] This last operation can actually be performed with the other three.
[2] If you desire, you may play with the applet on `www.geogebra.org`.
[3] i.e., holds a copy of the geometric object α.