Prof. Christian Cachin
Jovana Mićić

Exercise 6

6.1 Soundness error (2pt)

The *soundness error* is the probability that a verifier V does not detect a false proof by a cheating prover P.

Determine the soundness errors of these zero-knowledge proofs we have discussed so far and discuss the influence of this parameter on the protocol:

- ZKP for Graph Isomorphism;
- ZKPK of knowledge of a discrete logarithm (Schnorr proof);
- ZKPK of knowledge of an RSA-inverse (Ex. 5.2).

6.2 Proof-of-knowledge protocol of a representation (REP) (3pt)

We have introduced a ZKPK for knowlege of a representation of a value y with respect to multiple bases $g_1, \ldots, g_n$, abbreviated

$$\mathsf{PK}\Big\{(\alpha_1, \ldots, \alpha_n) : y = {g_1}^{\alpha_1} \cdot \cdots \cdot {g_n}^{\alpha_n}\Big\}.$$

Prove soundness and zero-knowledge for the case $n = 2$.

Hint: The soundness property for this ZKPK means that given two accepting transcripts with the same commitment but different challenges, you can extract $\alpha_1, \ldots, \alpha_n$ such that the above relation holds (but not necessarily that you can compute any discrete logarithm).

6.3 Encrypting a vote (5pt)

Consider the additively homomorphic ElGamal cryptosystem.

a) For a given public key y, describe a protocol and a corresponding ZKPK that allows a party P to encrypt a value $i \in \mathbb{Z}_q$ and prove to V that it knows the encrypted value.

b) Now P participates in an e-voting protocol and encrypts its vote under y. A vote must be $v = 0$ or $v = 1$. Develop a protocol for P to encrypt v and to prove the correctness of the encrypted vote to V.