NIE-AIB — Homework 4 – 15.11.2023

Instructions.

Complete the exercises and write your solutions on papers. Comment your solutions sufficiently. **A result alone without the solution is insufficient**. Submit your solutions to the MS Teams assignment "NIE-AIB, Homework 4" no later than November 28.

1 Exercise 1.

Graph-isomorphism protocol.
Suppose G_0 and G_1 are public graphs, and Alice knows an isomorphism $\pi : G_0 \to G_1$.

- Alice simultaneously choose a random isomorphic copy H of G_0 and an isomorphism $\tau : G_0 \to H$. Alice sends H to Bob.
- Bob choose random $b \in \{0, 1\}$ and sends b to Alice.
- If $b = 0$, let $\sigma = \tau$. If $b = 1$, let $\sigma = \tau \circ \pi^{-1}$. Alice sends σ to Bob.
- Bob checks if $\sigma(G_b) = H$.

Prove the correctness, soundness and zero-knowledge property of the graph-isomorphism protocol.
Note:

- Two undirected graphs G and H are said to be isomorphic if there exists a bijection π from vertices of G to vertices of H that preserves edges.
- That is, $\{x, y\}$ is an edge of G iff $\{\pi(x), \pi(y)\}$ is an edge of H.
- The graph isomorphism problem is, given graphs G and H, to determine whether or not G and H are isomorphic.

2 Exercise 2.

Consider a Schnorr identification protocol between Alice and Bob with primes $p = 595939$ and $q = 2027$, $\alpha = 216$ and $t = 8$ and Alice's private key is $a = 131$. Describe the communication between Alice and By Bob if she chooses $r = 667$ and he challenges $e = 13$.

3 Exercise 3.

In Shamir's $(3, 4)$ scheme for $p = 5$, Alice, Bob and Charles were given the following (x_i, y_i) values: $(1, 0), (2, 1), (3, 4)$. Compute the corresponding Lagrangian interpolation polynomial and determine the secret.
HINT: The Lagrangian interpolation polynomial will be $P(x) = a_2x^2 + a_1x + b$.