PWr, Inf. algo. CRYPTOGRAPHY, 2022 assignments list # 12, Zero Knowledge Proofs

The following problem is to be solved before the test planned for June 2. The question is not difficult computationally, but requires rethinking the notions and ideas from the lecture on zero-knowledge proofs.

1. One can use ElGamal encryption for authentication: Peggy holds x such that $g^x = \beta$ and authenticates herself by proving that she knows x.

   Protocol execution:

   (a) Victor chooses y, k at random and calculates an ElGamal ciphertext $(A, B) := (\beta^k \cdot y, g^k)$

   (b) Victor sends (A, B) to Peggy,

   (c) Peggy decrypts the ciphertext, obtains the plaintext y and sends it to Victor,

   (d) Victor accepts if he gets y.

   Completeness of this protocol is obvious.

   Questions:

   (a) Is the soundness property fulfilled? What is the probability to cheat (probability that the result is Accept, while Peggy does not know x)?

   (b) Can you construct an extractor for this protocol? (the question is about "special soundness")

   (c) Does it satisfy Zero-Knowledge property for an honest verifier?

   (d) What about the situation for a dishonest verifier?

   (e) in each case: if Zero-Knowledge property is satisfied, is it perfect or computational?

/-/ Mirosław Kutyłowski