Home Assignment 3

Niklas Jnsson, 9208273772

Complete the eight A-assignments below and solve them individually.

A-3 Why is it natural to think of the communication channel as a bulletin board?

A-4 Why is the homomorphic property of ElGamal encryption not really suitable in an electronic voting system based on homomorphic encryption?

A-8 Briefly explain the properties Completeness, Soundness and Zero-Knowledge regarding zero-knowledge proofs.

A-9 Explain how the zero-knowledge property of a zero-knowledge proof is related to a simulator.

A-10 In the lecture notes, it is remarked that an interactive zero-knowledge proof can be made noninteractive through a trick, by letting "the challenge provided by Victor be a function of some predetermined parameter". What cryptographic building block would be suitable as such a function?

A-19 Consider the blind signature based protocol. No result will be published before all voters has had the chance to verify that their vote is indeed correct. How is this important property achieved?

A-21 Compare the fairness provided by the Mix-based and blind signature-based protocols given in the lecture notes.

A-23 In the homomorphic encryption based scheme, why is it important that voters prove that their vote is correct, e.g., either $v_i = -1$ or $v_i = 1$?