Home Assignment 3

Rasmus Olofzon, 9104192472

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

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

A-13 Describe two different usages of secret sharing, one where the secret is reconstructed "explicitly", and one where it is not.

A-14 In the commitment scheme using a hash function (given on the lecture slides), is the *binding* and *conceiling* properties information theoretic or computational?

A-15 Why is the mix network voting example in the lecture notes divided into registration and voting phase? What would happen if the phases were combined and the vote was sent immediately?

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-22 In the slides, two main strategies for making an electronic voting scheme are presented. One is that "the vote is posted on the bulletin board in encrypted form, and the person (casting the vote) is not anonymous". Describe a scheme like this, and in particular explain how the vote can be counted without sacrificing privacy/anonymity.

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 $v_i = 1$?

A-25 Explain why (how) the homomorphic voting scheme in the lecture notes does not have receipt-freeness.