Home Assignment 3
EITN41

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

The idea is that if a verifier could simulate the communication of the proof, i. e. fake a transcript of it, and this simulated/faked transcript cannot be distinguished from an actual communication exchange then the verifier cannot be said to have learnt anything from the proof. Then the zero-knowledge property is present. The thing is that in an actual communication between verifier and prover the probability of a prover providing the right choices/information without actually knowing the secret is very, very low (e. g. for 50 iterations of classic examples with graph isomorphism or Ali Baba's cave: $2^{-50} = 8.88.. * 10^{-16}$). So, if the prover provides correct information in an online setting the verifier must conclude that the prover knows the secret, but the verifier still have not learned anything about the secret.

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

TODO

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

TODO

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?*

TENTATIVE: Timing attack?

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?*

TODO

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.*

TENTATIVE: Blind signature scheme?

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 $v_i = 1$?*
TODO

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