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.*

The "explicit" variant is the one first described in the lecture notes.

The "non-explicit" variant is the variant of the second one, used in 4.3 'Using Homomorphic Encryption'. It is not the actual message m that is decrypted but instead w^m mod q.

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?*

Computational. A hash function is used, and it is inversible. It is only unfeasibly difficult to do so. Most can also be found collisions to.

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?*

If there is an error (Voter is not registered correctly, a Mix is corrupt etc) then this will not be discovered until the voting already has been carried out. This has the potential of disturbing a re-election triggered by the erroneous management, which breaks the fairness property.

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 voter can check their vote on the Bulletin Board after the Voting phase, then their x is up there. They can see if it is the same value as when they calculated it. If it is, they send their secret k so that the Counter can extract the voter's vote, v. Before the voter send their k, their vote is unextractable and therefore untalliable.

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.*

Threshold encryption scheme. The vote can be counted because of the homomorphic encryption properties: in the encrypted space, the ciphertext can be multiplied and this brings the same result as multiplication of the plaintext. We use this in the way that the votes are put in an exponent, this means that the votes will be added to each other. The final result is produced (in the -1, 1 case) by adding all votes together, positive if there are more positive values than negative values and vice versa. Since the votes are encrypted, privacy/anonymity is preserved.

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 $v_i = 1$?*

If they do not use -1 or 1, their vote will be weighted more than others. The sign of the exponent of $w^{\sum_{t-1}^{m} v_i}$ is what is taken as the final result. Two very simple examples to illustrate the difference: $\{ w_1 = -1, w_2 = 1, w_3 = -1 \}$, a correct procedure. Here the result will be negative, as it should be when it is two against one. $\{ w_1 = -1, w_2 = 3, w_3 = -1 \}$, an incorrect procedure. Here the result will be positive, which it should not be when it is two against one.

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

The Voter is listed, uniquely on the Bulletin Board. This means that they (and everyone else) knows that they voted. This does not reveal what they voted for, but at least *that* they voted. So not full receipt-freeness.