Home Assignment 3

A-1 Explain the connection between threshold encryption and robustness in the context of electronic voting.

Since in threshold encryption many different authorities work together, it is impossible for one or more parties to cheat or be corrupt in order to manipulate the votes. Therefore if some parts of the system would cheat/fail the system as a whole would still work. Threshold encryption therefore satisfies the robustness property.

A-6 Consider the zero-knowledge proof in Figure 1 of the lecture notes. Show the special soundness property, i.e., given two transcripts of the protocol (a' , b' , c, r) and (a' , b' , c' , r'), show that it is possible to recover s.

From Figure 1 in the lecture notes we know that: r = w + sc. The two transcripts have different c (challenges) and r (responses).

By combining the two transcripts we get that s is:

$$s = \frac{r-r'}{c-c'}$$

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

In the following example, Peggy is the prover and Victor is the verifier.

Completeness: If Peggy knows the secret, Victor have to trust her since she knows how to reproduce an isomorphic cycle that creates H.

Soundness: Let's say that Peggy doesn't know the proof. Then the chance of Victor accepting her guess is very small. In fact, it is 2^-n where n is the number of rounds.

Zero-knowledge: In the end, Victor will not know anything about the secret except the fact that Peggy has got it.

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

Shamir secret sharing can be used if the secret shall be reconstructed. Then several parties cooperate in order to reconstruct a secret that a trusted dealer already knows. The trusted dealer first creates a polynomial f(z) where f(0) is the secret. Each participant is then given a variant of

the function and with the help of Lagrange interpolation they can together calculate f(0). It is good to use Shamir secret sharing if we have a trusted authority who wants to share a secret that can only be constructed with the help of many parties. It can be used when we don't want to rely on one single party to behave correctly, since everyone is needed in order to gather the secret.

Another way is to let participants together create public/private key pairs and then agree on a public key that is used to encrypt messages. To decrypt the message, *t* number of participants needs to cooperate using the private key. Now they don't need the "help" of a trusted authority. It is good if we don't for example trust the authority.

A-16 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 clear text, but the person casting the vote is anonymous". Describe a scheme like this, and in particular explain why this scheme still ensures "one-voter-one-vote".

The lecture notes brings for example up Mixes as a way to ensure anonymity when creating an electronic voting scheme. With Mixes a list of public keys is created were each public key represents the pseudonym of a voter. The keys are then encapsulated and encrypted with the public keys from the mix network. This is called the registration phase. When voting, a user creates a digital signature of the message using a private key. They then send the digital signature through the mix until reaching the last mix which will post the chosen public key (pseudonym), the vote along with the digital signature of the vote. The votes are publicly displayed but the voters are still anonymous. Each voter can check that "their" pseudonym has voted and that the result corresponds with the desired one. It therefore ensures "one-voter-one-vote" since each user only has one digital signature and pseudonym.

A-20 In the voting protocol using blind signatures, if a voter cannot find their commitment in the published list, they reveal r, so that e can be derived and identified in the list published by the administrator. It is claimed that this does not reveal their vote. What property of the commitment scheme is crucial here?

The concealing property is crucial. It says that the value of the vote can not be determined before it is actually revealed.

A-24 In the slides regarding homomorphic encryption based voting, it is stated that if the sum of mi is moderate, we can compute the discrete log. Why does the sum need to be moderate?

This is because it's difficult to compute a discrete log if the sum is too big. Discrete logarithms grows exponentially when the sum gets bigger. There is no known way to compute them efficiently. The sum therefore needs to be moderate in order for the voting scheme to be somewhat efficient.

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

Receipt-freeness means that the voter can't verify what he or she has voted. In Homomorphic voting scheme it is possible to know that a voter has voted, that the vote is eligible. It is however not possible, due to the nature of the homomorphic property of ElGamal, for a voter to prove how they voted.