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

Because it is assumed that anyone can listen to the traffic entering and leaving the Mixes. This lets anyone know who is participating, i.e. who is a "user" on this bulletin board, and what the actual output is(posts on a bulletin board), but does not know that a post is linked to a certain user(unlinkability). So the input and output of each mix is compared to being written on a publicly readable bulletin board. Because the Mixes secretly permute the list of messages we get unlinkability.

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

The homomorphic property of ElGamal encryption is given by $E(m_1, r_1)E(m_2, r_2) = E(m_1 m_2, r_1 + r_2)$. This shows that the product of two encryptions(cipher texts) will result in the encrypted product of the two plain texts. This is not very useful since votes are summed up to get the final result. Multiplying votes would result in very incorrect results.

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

The idea of a zero-knowledge proof is to allow a prover to prove that he/she knows a secret without revealing any information about the secret itself. Completeness is the property that if the prover knows the secret, the verifier will always accept the provers proof. This means that the verifier should be able to repeat the protocol of proving with different challenges a number of times and the prover should be able to prove successfully for all cases.

Soundness is if the prover does not know the secret, the verifier will accept the proof with very small probability. This means that if the protocol of proving is repeated many times with different challenges, the chance of the prover to actually prove correctly, even though he/she is not in control of the secret, is very low.

Zero-knowledge is the property that the prover should be able to prove that he/she knows the secret without revealing anything about the secret, no matter how many times the prove protocol is run.

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

If the verifier is able to produce a faked transcript(simulate the steps of the proof) of the communication in the proof, and this transcript can not be distinguished from an actual transcript, then the verifier can not have learned anything during the proof.

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

The hash function. If the prover compute the message of the verifier as the hash of the message sent by the prover. If the hash is modelled as random oracle the message computed this way should look random as in an interactive execution, hence the properties of the original proof system should be preserved.

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?

Each voter commits to their vote by computing their commitment $x_i = \xi(v_i, k_i)$ for their vote v_i and a random value k_i. The voter then computes a blinded value of the commitment $e_i = \chi(x_i, r_i)$ and then signs this value using the private key $s_i = \sigma_{v_i}(e_i)$. An administrator A then verifies the signature, identifies the voter and checks that the voter is allowed to vote, and has not applied for voting before. If everything is ok then administrator A signs the blinded commitment $d_i = \sigma_A(e_i)$. Administrator A then publishes a list of $\langle ID_i, e_i, s_i\rangle$ on a bulletin board.

Now because the list(bulletin board) is publicly available, each voter can see a list of accepted voters together with their blinded commitment e_i. It is not possible for a voter to change its mind as of the commitment being posted on the bulletin board. If a voter is not included in this list he/she can complain and have it corrected.

The next step is the voting and collecting phase. Each voter sends in the signed commitment(d_i) to the counter C using an anonymous channel. The signature is extracted knowing r_i. Counter C verifies the signature and publishes l_i, x_i, y_i on the bulletin board, where l_i is just an integer identifying the vote ballot.

Now every user can compare this posted list to the list mentioned in the beginning, and if they do not match, releasing the value of r_i, it is possible for everyone to verify which voter's ballot was not received. If there are no complaints then the counting phase can begin.

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

The fairness property is the property that no partial results should be disclosed before the end of the voting procedure, as this could affect people if they see that a certain party is winning/losing etc.

In the blind signature based protocol this property is achieved because the actual counting of the votes is not done if a single voter complains that their vote is missing on any of the lists.

But in the Mix-based protocol the fairness property does not hold because the mixes will publish all votes before any verification that everything is OK is done. Because if a single Mix is corrupt, e.g., it changes the encryption, then there will be an error in the posted result in the end. A voter may of course complain since they can verify their own vote, but then all votes have already been posted in the clear and this breaks the fairness property.

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 $v_i = 1$?

$E(v_i, r_i) = (a_i, b_i) = (g^{r_i}, w^{v_i} y^{r_i})$
When collecting the votes all $E(v_i, r_i)$ are collected and product is taken by $\prod_{i=1}^{m} E(v_i, r_i)$ where m is the amount of voters.

This can be simplified to:
$(\prod_{i=1}^{m} a_i, \prod_{i=1}^{m} b_i) = (g^{\sum_{i=1}^{m} r_i}, w^{\sum_{i=1}^{m} v_i}, y^{\sum_{i=1}^{m} r_i}) = E(w^{\sum_{i=1}^{m} v_i}, \sum_{i=1}^{m} r_i)$.

If voters can not prove that their vote is correct, they can insert other values for v_i, such as 1000, and this would be added up in the sum of the votes and therefore skewing the result. This would not be very democratic and it is therefor a demand that each vote can be proven to be $-1, 1$ first.