Problem Set 9 Solutions

Problem 9-1. Atomicity of withdrawal protocol

The only problem is at step 2. At all the other points if the line goes down the protocol can be started from scratch.

At the end of step 2, the Bank must require the User to use the same commitment to the blindings that was used in step 1. Otherwise a malicious user could try to cheat on the bank in the following way. He puts one coin that has a larger denomination among the blinded coins. He hopes that the Bank will ask the other 99 coins. If the Bank asks the User to reveal the blinding of the bad coin, he pretends that he never received the message and asks to start from scratch.

After an expected number of 100 trials the user will be able to cheat on the bank. Notice that this would not be much of a concern if we were able to construct a blinding protocol with exponential probability of cheating. That is a protocol in which the User blinds 100 coins but the probability of cheating the Bank is 2^{-100}. Indeed in that case the User would need 2^{100} expected trials in order to cheat the bank.

Problem 9-2. Blinding with ElGamal

Ok this was a tough one. The solution almost everybody, including the teaching staff, came up with was the following.

1. The User tells the bank she wants a \$1 coin.
2. The Bank replies with 100 values $a_i = g^{k_i}$ for random k_i.
3. The User chooses a random $\alpha_i \bmod p-1$ and computes $a_i' = a_i g^{\alpha_i}$. Let $c_i' = H(m_i, a_i')$, she sends back $c_i = \frac{c_i'}{g^{\alpha_i}}$ where m_i are all \$1 coins.
4. The Bank asks the user to open 99 of those.
5. The User reveals 99 of the m_i's and α_i's.
6. The Bank checks that everything is in order and if so it replies with $b_i = k_i c_i + x a_i \bmod (p-1)$ for the unopened index i
7. The User computes $b_i' = g^{\alpha_i} b_i + \alpha_i c_i'$. Notice that (a_i', b_i') is a good signature for m_i.

This seems to be anonymous. However we realized during the grading that there was a problem. The ratios $\frac{a_i'}{a_i}$ and $\frac{c_i'}{c_i}$ are equal (to g^{α_i}). This makes the coin traceable to the User when it comes back to the Bank (at least with high probability).

Here is a possible solution. However for this to work we need to assume that g is an element of prime order q, where q is a large prime dividing $p-1$. The resulting scheme becomes very close to the Digital Signature Standard (DSS).

1. The User tells the bank she wants a \$1 coin.
2. The Bank replies with 100 values $a_i = g^{k_i}$ for random k_i.
3. The User chooses a random $\alpha_i, \beta_i \bmod q$ and computes
   - $a'_i = a_i^{\alpha_i} g^{\beta_i} = g^{\alpha_i k_i + \beta_i}$
   - $c'_i = H(m_i, a'_i)$
   - $c_i = c'_i \alpha_i a_i (a'_i)^{-1}$

   where m_i are all \$1 coins. The User sends c_i to the Bank .
4. The Bank asks the user to open 99 of those.
5. The User reveals 99 of the m_i's, α_i's and β_i's
6. The Bank checks that everything is in order and if so it replies with $b_i = k_i c_i + x a_i \bmod q$ for the unopened index i
7. The User computes $b'_i = b_i a_i^{-1} a'_i + \beta_i c'_i \bmod q$

Notice that (a'_i, b'_i) is a correct ElGamal signature for m_i (at least considering our definition of ElGamal). The assumption that g is an element of prime order q is needed in order to be able to compute inverses modulo q.