ALGORITHMICS, CRYPTOGRAPHY & COMPUTER SECURITY, graduate programs 2023
CRYPTOGRAPHY, SPRING 2023, assignments list # 9, 17.5.2023

1. Alice presents two ElGamal ciphertexts: C_1 and C_2. She wants to convince Bob that they hide the same plaintext.
   Question: Find a way to do it without revealing the plaintext. Assume that neither Alice nor Bob knows the secret decryption key. They know the public key used for encryption. Alice knows the random numbers used to create C_1 and C_2.

   Hint: first find out how to prove that a ciphertext corresponds to the plaintext 1.

2. Assume that C_1 and C_2 are two ElGamal ciphertexts defined over the same group.
   Questions:

   - Is it possible to check that C_1 and C_2 correspond to the same public key? If so, then show the algorithm. If not, then show a reduction to one of the standard cryptographic assumptions to explain why it is infeasible.
   - How does the situation change, if the attacker knows a candidate plaintext?

3. Assume that C is an ElGamal ciphertext. Is it possible to derive any information on which public key has been used to create it? Consider this question for the case where you have a priori knowledge that either $\mathtt{pk}_1$ or $\mathtt{pk}_2$ has been used.

4. Can you publish a single ElGamal ciphertext, so that each user can derive their own pseudorandom value and so that a user learns only its own value and cannot guess the value obtained by anybody else?

5. For privacy of e-voting one can use the concept of partial decryption with ElGamal scheme. Assume that there are two servers involved: S_1 and S_2. The public key $\mathtt{pk}$ used to create encrypted ballots is composed as $\mathtt{pk} = \mathtt{pk}_1 \cdot \mathtt{pk}_2 \bmod p$, while S_1 and S_2 keep their private keys $\mathtt{sk}_1$, $\mathtt{sk}_2$. Decryption of a ciphertext $(a, b) = (\mathtt{pk}^k \cdot m, g^k)$ of m, consists of two steps: first S_1 computes $a' := a/b^{\mathtt{sk}_1}$. Then S_2 computes $a'/b^{\mathtt{sk}_2}$.
   Questions:

   - how to use partial decryption for mixing the ballots? Is it enough to partially decrypt according to the above procedure and sort the results before outputting?
   - Any idea how to check that S_1 and S_2 are not cheating during decryption?

6. Assume that e-voting has been designed with 6 intermediate mix servers performing re-encryption. Randomized Partial Checking has been used to ensure that the mix servers are not cheating. Check what is the impact for anonymity of votes. Assume that there are two candidates and 100 voters, candidate A gets 90% of votes. How far the voters' anonymity are endangered by RPC?

7. IBE scheme presented during the lecture required to map user's identity ID to group elements via a hash function.

   Assume that the citizens ID's are right away the elements of the pairing group (well, it is not true now). In this case, could we skip the hash function?

/-/ Mirosław Kutyłowski