Privacy and Computer Science
Examination
ECI 2015

Frédéric Prost

Deadline : The answers should be sent before the 15th of August 2015

Answers : The answers should be sent by mail as a pdf file to frederic.prost@ens-lyon.fr, you have to include your full name in the text and the subject of the mail should be [ECI 2015 Privacy & CS Test]

---

1 Virtual coin tossing

The aim of this exercice is to design a protocol between Alice and Bob that simulates a random coin toss. In order to achieve that, Alice and Bob can communicate between each other and use a secure hash function h (we suppose that h has all the "good" properties with relation to collisions, pre-image etc.).

Q.1 : Describe a protocol to simulate a coin toss in such a way that neither Alice nor Bob (if they are honnest) can challenge the result.

Q.2 : Discuss the security aspects of your protocol : is there any way Alice or Bob can cheat (under what hypotheses ?) ? What are the precise requirements with relation to h ? etc.

2 Secret sharing between two parties

The aim is to share a secret, as in the Shamir scheme of secret sharing seen in course. But here we are in a particular case : Trent's secret (an integer of size n bits) is shared between only two participants : Alice and Bob. Neither Alice nor Bob can recover the secret by themselves, but sharing their information they should be able to recover the secret.

Q.3 Give a protocol allowing Trent to share its secret.

For this protocol you only have access to simple operations on bits : and, or, xor, negation.. In particular you cannot perform modular arithmetic computations (as the ones used in Shamir's scheme).

3 Electronic Vote

The aim of this exercice is to study a protocol allowing to vote through a network.

Q.4 What general properties/guaranties should have an ideal electronic vote protocol ? List and explained all the desired features of such an ideal protocol.

We propose the following voting scheme:

1. Every voter signs its vote with its private encryption key.
2. Every voter encrypts its signed vote with the public key of a central authority.
3. Every voter sends its vote to the central authority.
4. The central authority decrypt the messages, cheks the signature and record the vote.

Q.5 What are the properties verified by this protocol?

Q.6 What are the problems raised by this protocol with respect to an ideal vote scheme?

We propose a better protocol by making a distinction betwenn two central authoritiesl: one is going to authenticate the voters (AV) and the other ones will count the votes (CT). The protocol goes as follows:

1. Every voter sends a request to AV in order to get a validation number.
2. AV sends a big random number to requests and maintains the list of validation numbers issued and the list of voters to whom she distributed validation numbers.
3. AV sends the list of validation numbers to CT.
4. Every voter randomly chooses an indentification number. He creates a message in which there is this number as well as the validation number sent to him by AV. The voter includes its vote and sends the whole message to CT (the message being encrypted with CT public key).
5. When CT receives a vote, he decrypts it and checks that the validation number has not already been used. If it is the case he removes it from the list of validation numbers and adds the identification number in the column registering the vote written in the message.
6. Once the election is finished, CT publishes the list of all identification numbers with the vote corresponding to this number.

Q.7 What is the interest of the identification number ?

Q.8 How this protocol can be attacked ? Are there any ways to deal with such attacks ? Can you make the protocol safer ?