Lecture - 10

Thursday, 18 August 2016 (15:20- 16:10)

Zero Knowledge Proofs (Part 1)

In the next two lectures we will briefly discuss on what are Zero Knowledge Proofs (ZKFs) and how to achieve these.

1 When can I label my authentication protocol to be a good one?

Intuitively, an authentication protocol will be termed "good" if is satisfies the following two properties:

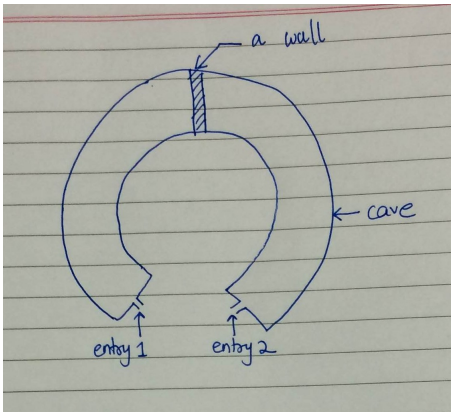
- COMPLETE: An authentic person must be able to authenticate with ease
- SOUND: An unauthentic person should struggle a whole lot for authenticating herself

We will discuss an example to illustrate such an authentication protocol.

1.1 Julie's Secret Cave

There is an amazing article titled "How to explain zero-knowledge protocols to your children" available online, please read this in your leisure time! We will discuss a small variant of its story.

Fig. 1: Julie's cave



Consider the cave shown in Figure 1, where Julie lives. This cave has a wall of rocks in between and Julie claims to have a magic trick using which she can travel across the wall. Since no one believes her words, people ask her to prove it. Julie wishes to prove it while keeping her magic trick to herself. She comes up with the following plan:

She will sleep in the cave today night. Next day morning, the villagers must come outside the cave and shout "left" or "right", indicating the door through which she must come out. If she actually possesses a magic trick up her sleeve, she will have no difficulty demonstrating her claim. However, if she is unauthentic (i.e. she possesses no magic trick) there is only a half probability that she might come out from the right door. Further Julie suggests that the people can repeat this experiment for an entire year i.e. 365 days. Hence, we can conclude the following:

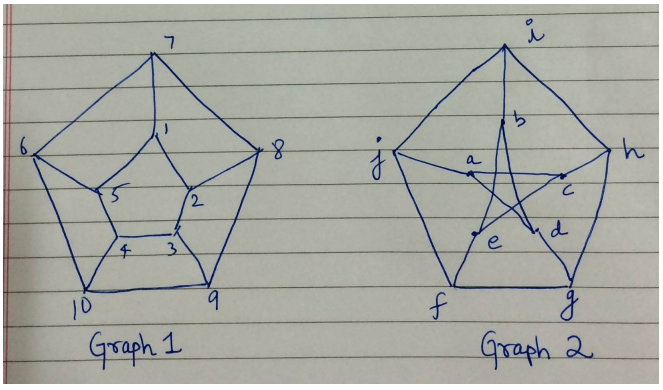
- P(she is authentic and she passes the test) = 1
- P(she is unauthentic and she passes the test) = $1/2^{365}$

Hence, at the end of a successful run of the experiment we can be very sure that Julie does have a magic trick up her sleeve, and she was able to convince us without demonstrating us the secret directly! This is an example of a ZKP.

1.2 Netaji's Wealth Inheritance Issue

Let say Mr. Haldi, who is a very corrupt Neta, has earned plenty of black money in his entire life. He further decides that after his death he wish to distribute his money among his loved and dear ones. He doesn't wish to disclose the name of his loved and dear ones to the court (due to whatsoever reason). Hence, he wish to pass some sort of a secret to his loved and dear ones, such that after Haldiji's death, they are able to authenticate to the court about their share in the money left behind by Haldiji. Also, no one other than the loved and dear ones of Haldiji must be able to demonstrate that they deserve a share in Netaji's wealth. The corrupt yet intelligent Neta comes up with a nice plan, which we describe below.

Fig. 2: Are the two graphs isomorphic?



Consider the two graphs given in Figure 2, are they isomorphic? On some thought and trial and error you must have concluded that they are not isomorphic. If I give you two 100 node graphs and ask you whether they are isomorphic or not, how easy is it? One obvious way is to scan through all 100! possible bijections that may be defining the isomorphism. The truth is, this is a hard problem and till data there does not exist a polynomial time algorithm to check if two input graphs are isomorphic or not. Hence, for the discussion up ahead we will assume that proving/dis-proving whether two given graphs are isomorphic is a hard problem. There are two clever techniques that Netaji comes up with, one of which will be discussed next and the other one in the next lecture.

Technique I Netaji picks a 100 node graph G_1 and shuffles the vertex labels to obtain an isomorphic graph G_2, let the corresponding shuffling be represented by the permutation σ. Netaji passes G_1 and G_2 to the court and the bijection σ to his loved and dear ones. How does a loved and dear one authenticate? The authentication protocol goes as follows:

1. Let say Ram wishes to authenticate himself to the court
2. Repeat the following experiment 100 times:
   (a) Ram constructs an isomorphic graph G' to G_1, let say the corresponding permutation is represented by σ'.
   (b) Ram passes the graph G' to the court.
   (c) The court asks him to do one of the following with probability half each:
      i. Depict a bijection between G_1 and G'
      ii. Depict a bijection between G_2 and G'
   (d) If Ram fails to show the bijection, he is labeled "unauthentic"
3. If Ram passes the test, he is labeled "authentic"

If Ram is authentic, he will for sure pass this test. Let us now calculate the probability with which an unauthentic person will be able to pass this test. The unauthentic person has a permutation representing the isomorphism between G' and G_1 or G' and G_2, and not both, hence with probability half he/she will be caught in an iteration. The probability with which an unauthentic person will be labeled authentic is therefore equal to $1/2^{100}$. Hence, this technique works, given the assumption that isomorphism is a hard problem.