Lecture - 11

Thursday, 18 August 2016 (17:10- 18:00)

Zero Knowledge Proofs (Part 2)

In this lecture we will study another way to resolve Netaji's wealth inheritance issue.

Before we describe the technique, let us revise what the HAMPATH problem is. In a graph, a walk is a sequence of vertices, such that there is an edge between two successive vertices. A Hamiltonian path is a walk such that each vertex in the graph appears precisely once in the walk. Given a graph G, to check if there is a hampath in it is an NP-Complete problem, hence it is very hard! We will use this to our advantage in the next technique.

1 Netaji's Wealth Inheritance Issue (Part 2)

Technique II Netaji constructs a 100 node graph G_1 such that it has a hampath H in it; such a graph is easy to construct: construct a path of length 99 and then add random edges between pair of vertices. Netaji passes G to the court and the hampath H 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 which is public, let say the hampath in G' corresponding to the hampath H in G is H'.
   (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 and G'
      ii. Depict a hampath in G'
   (d) If Ram fails in the above test, 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 will either have constructed G' by shuffling G or he/she may have constructed some arbitrary graph with a hampath, 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 $1/2^{100}$.

Please note that this technique is no better than the previous one i.e. this techniques'security also boils down to the hardness of the isomorphism problem. Consider the following scenario to understand why this is true:

Let say an authentic person is playing the authentication protocol with the court and an unauthentic person is watching the game. Further assume that the adversary (i.e. the unauthentic person) has a very efficient algorithm for checking if two input graphs are isomorphic or not. Let say the

authentic person passes a graph G' to the court. Further, the court asks the person to display the hampath in G'. The authentic person now displays H', hence authenticating herself. The adversary finds the isomorphism σ between G and G', and further using H' he is able to find the hampath H is G, which breaks our authentication protocol! Hence, this protocol is as secure as the hardness of the isomorphism problem.