Zero Knowledge Proofs

Problem Set : 2/26

Source : Wikipedia

Zero Knowledge Proofs

A zero-knowledge proof must satisfy three properties:

1. **Completeness**: if the statement is true, the honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.
2. **Soundness**: if the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.
3. **Zero-knowledge**: if the statement is true, no verifier learns anything other than the fact that the statement is true. In other words, just knowing the statement (not the secret) is sufficient to imagine a scenario showing that the prover knows the secret. This is formalized by showing that every verifier has some *simulator* that, given only the statement to be proved (and no access to the prover), can produce a transcript that "looks like" an interaction between the honest prover and the cheating verifier.

Source : Wikipedia

Red and Green Balls

“Imagine your friend is colour-blind and you have two balls: one red and one green, but otherwise identical. To your friend they seem completely identical and he is skeptical that they are actually distinguishable. You want to *prove to him they are in fact differently-coloured*, but nothing else, thus you do not reveal which one is the red and which is the green.”

Source : Wikipedia

Cryptography

“Peggy wants to prove to Victor that she knows the discrete log of a given value in a given group.[5]

For example, given a value y, a large prime p and a generator g, she wants to prove that she knows a value x such that g^x (mod p) = y, without revealing x.”

Source : https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/

K Colorings

Say Peggy has a graph G and some k coloring of it. How can Peggy prove she has a k coloring to Victor without revealing her k coloring?

Weird Question: What if Peggy didn't have a k-coloring but DID have a time machine that could rewind time by 10 minutes? How might she use that to trick Victor into thinking she does have a valid k-coloring?

Source : Euler Circle

Very Similar Sudoku Problem

Say Peggy wants to show that she has solved a 9 x 9 sudoku puzzle. How can she prove to Victor she indeed has done so without explicitly revealing any of her own numbers?

Source : Wikipedia

Hamiltonian Cycle

“In this scenario, Peggy knows a Hamiltonian cycle for a large graph *G*. Victor knows *G* but not the cycle (e.g., Peggy has generated *G* and revealed it to him.) Finding a Hamiltonian cycle given a large graph is believed to be computationally infeasible, since its corresponding decision version is known to be NP-complete. Peggy will prove that she knows the cycle without simply revealing it.”

Source : Euler Circle

Graph Isomorphism

(9) Let $G = (V_1, E_1)$ and $H = (V_2, E_2)$ be two graphs, so that E_i is a set of pairs of vertices in V_i, for $i = 1, 2$. We say that G and H are isomorphic if there is a bijective function $\sigma : V_1 \to V_2$ such that $\{v, w\} \in E_1$ if and only if $\{\sigma(v), \sigma(w)\} \in E_2$. (That is, G and H are "the same" up to relabeling the vertices.) Find a zero-knowledge proof for determining that G and H are *not* isomorphic. (You may assume that Peggy knows an actual isomorphism of the graph, and furthermore than she can solve the graph isomorphism problem for *every* pair of graphs.) This is interesting, because there does not seem to be a general way of producing a short proof that two graphs are not isomorphic, i.e. graph non-isomorphism is not believed to be an NP problem. By contrast, one can produce a short proof that two graphs *are* isomorphic by simply writing down an isomorphism.

(10) Find a zero-knowledge proof for showing that two graphs *are* isomorphic.

Sources

Slides 2,3, 4, and 7 were literally copy pasted from Wikipedia.

Slide 5 came from

https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/

Slide 6 and 8 were taken from Euler Circle, and Dr. Simon Rubinstien Salzedo.