Zero Knowledge Proofs

MATH 408

Trevor Nichols

What is a Zero Knowledge Proof (ZKP)?

A Zero Knowledge proof is a way of proving whether a statement is true or false without divulging any other information

For example, what if you are trying to convince your friend that you've proved the Riemann hypothesis but do not want to give your proof to him?

What is an Interactive Proof?

Formally, a proof modelled as a sequence of messages between two entities

- Typically a set of rules are agreed to beforehand
- Consists of a Prover (P) and Verifier (V) at a minimum
- V is proving that a statement is true to P
- P may choose critical values or make decisions during the proof process

Adam Hutching's Labyrinth (The Ali Baba Cave)

Say Adam Hutching owns a Labyrinth with two entrances, A and B

Adam claims that you can enter through entry A and exit through entry B

The interactive proof would go as such:

- Trevor sits outside the labyrinth, only with view of the entries
- Adam enters entry A and exits through entry B
- Trevor is now convinced that his statement is true

The 3-Colored Graph Problem

Is a simple true or false problem given any graph G.

It asks whether graph G may be colored with 3 colors such that no two nodes connected with an edge have the same color.

You may be wondering why we are talking about the 3-Colored Graph Problem

- It is an NP-Complete, meaning any other NP or P problem may be reduced to the 3-Colored Graph Problem
- We can easily prove a graph is 3-Colorable or not with a zero-knowledge proof!

The Zero Knowledge 3-Coloring Graph Proof

P is attempting to prove that a graph G is 3-Colorable, we call this colored graph C

1. P sends V a new C'
    1. P generates a random 1-to-1 mapping M from $\{1, 2, 3\}$ to $\{1, 2, 3\}$
    2. P computes C_M, such that each node on C is mapped through M
    3. P generates a random secret key S_N for each node N
    4. P encrypts every node in C_M with its relevant key S_N
    5. This is C'

The Zero Knowledge 3-Coloring Graph Proof Continued

2. V selects any edge E of C' and asks for the S_N to the nodes N_1 and N_2 associated with E
3. P sends the keys
4. V decrypts N_1 and N_2 and verifies that they are different and in $\{1, 2, 3\}$
5. Restart from step one with a new C' until V is satisfied

An Example Sudoku

Let our domain be $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ for the numbers in a sudoku

Our contraints:

- Each entry must be different from every other entry in its superblock, its row, and column
- Each given number must be different from all other non-matching given numbers

This is very similar to the Zero Knowledge 3-Coloring Graph Proof!

Proving I know the Sudoku

- P will send V the graph representing the sudoku board's constraints G and agree that it does in fact represent the same problem
- P will derive B' from the numbered graph B satisfying G
- P sends V B'
- V randomly chooses an edge
- P send the decryption keys
- V verifies that they are different and within the domain

Why this is useful

- P just proved to V that he has completed the sudoku without telling V what the solution to the sudoku problem is
- More generally any NP problem may be reduced to the 3-Coloring problem and thus your proof “explained” to another person without divulging any secrets.

Applications

- Blockchain
- Smart contract verification
- Identity management

Sources

New Paradigms for Digital Signatures and Message Authentication Based on Non-Interactive Zero Knowledge Proofs

https://cseweb.ucsd.edu/~mihir/papers/nizk-ds.pdf

Proofs that Yield Nothing but Their Validity - ODED GOLDREICH

https://cseweb.ucsd.edu/~mihir/papers/nizk-ds.pdf