Zero knowledge protocols and oblivious transfer

What is zero knowledge protocol?

It is a cryptographic concept developed in the early 1980's.

Ex: Suppose Alice found a solution to a problem like she has ~~she~~ ~~proved~~ proved a theorem.
suppose she wants to PROVE that she has found a solution but at the same time conveying ~~no~~ NO KNOWLEDGE about her proof or solution.
This is called "Zero knowledge protocol".

Let us take another example:

Picara is the "prover" is the person with the solution.

Vivales is the "verifier" is the one who in the end must become satisfied that Picara has the solution, while still not having the idea of what the solution is.

The example is of map colouring.

Map colouring

every planar map can be coloured with 4 colours. Suppose Picara is given a complicated map, which after much effort she is able to find a way to colour the map using 3 colours only (Red, Blue, Green). Now she wants to convince Viralci that she has found a solution.

~~Steps:~~

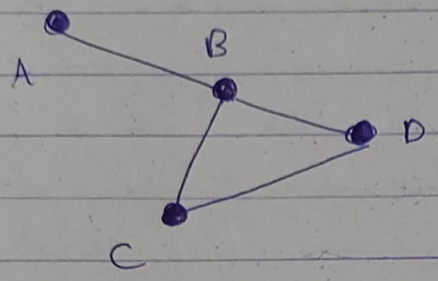
Step 1: Translate the problem into the language of graphs.

What is a graph?

A graph is a set V, whose elements are called vertices and a subset E of the set of all (unordered) pairs of elements of V. The elements of E are called edges.

An edge $e = \{u, v\}$ where $u, v \in V$ is a line joining vertices u & v.

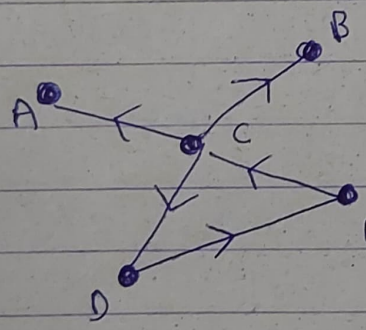
Example:



= undirected graph

$V = \{A, B, C, D\}$

$E = \{(A, B), (B, D), (C, D), (B, C)\}$



= Directed graph

Definition: A graph is colourable by the colours (r, b, g) if there exists a function $f: V \to \{r, b, g\}$ such that no vertices joined by an edge have the same colour, that is:

$$\{u, v\} \in E \Rightarrow f(u) \neq f(v)$$

* To translate the map colouring problem to graph colouring problem, take V to be the set of countries and connect 2 countries with an edge if they have common boundary.

Properties of 3-colourability problem

(1) It is easy to visualize

(2) It is NP- ~~complete~~ Complete

NOTE: The NP-completeness property implies that if one has zero knowledge verification of 3 colourability, then we can get a zero knowledge verification for any NP-problem by reducing it to 3colourability.

Zero-knowledge Proof of 3-colourability:

Visualize the vertices of the graph as small balls containing little coloured lights and joined by BARS whenever there is edge.

The light in each vertex can flash either red, green, blue

Picara has a device that:

(1) a device A which sets each vertex to flash ~~white~~ whichever of the three colours she chooses.

(2) a device B which, whenever a button is pushed, chooses a random permutation of the 3 colours and resets each vertex according to permutation.

~~Vivaldi~~ NOTE: Vivaldi has no control over the device B.

We further suppose that the lights inside the vertex balls are hidden from view. When someone grabs onto the bar connecting the two vertices, the lights in those 2 vertices becomes visible.

Now Picara has figured ~~out~~ a way for 3 colouring of the graph and uses the device A to set the vertices with the corresponding colours.

The procedure used to convince Vivales that she has been successful in doing this:

(1) Vivales is allowed to grab any of the edge bars revealing the colours of the 2 vertices at each end. Since the two vertices have different colours, it gives a little bit of evidence that Picara has valid colouring.

(2) Now Picara pushes the button B on to permute the colours.

(3) Vivales may then grab another edge bar.

(4) Picara & Vivales repeat steps #2 & #3 in alternation until Vivales has tested all the bars.

Conclusion:

(1) If Picara has not been able to 3-colour the graph, she won't be able to fool Vivales. eventually step 3 would reveal vertices with the same colour.

(3) Because of the random permutation of the colours, Virales learns nothing about the colouring.

finite

What is a group?

A group of finite no. of elements is called a finite group.

A group is a set G, combined with the operation * such that:

→ group contains an identity
→ group contains inverses
→ operation is associative
→ group is closed under the operation

Ex: $(\mathbb{Z}, +)$ is a group

(1) Closure property

$a, b \in \mathbb{Z}$ $\quad$ $3, -5 \in \mathbb{Z}$

$a + b \in \mathbb{Z}$ $\quad$ $3 - 5 = -2 \in \mathbb{Z}$

(2) Associative

$a + b \in \mathbb{Z}$, $\quad$ $a + (b + c) \in \mathbb{Z}$ $\quad$ $a + (b + c)$

$b + a \in \mathbb{Z}$ $\quad$ $(a + b) + c \in \mathbb{Z}$ $\quad$ $= (a + b) + c$

$2 + (3 - 1) = 2 + 2 = 4$

$(2 + 3) - 1 = 5 - 1 = 4$

(3) Existence of identity element

0 is the identity element

(4) Existence of inverse element

$a \in \mathbb{Z}$

$-a \in \mathbb{Z}$

$a + (-a) = 0$

Hence $(\mathbb{Z}, +)$ is a group.

Ex: $(\mathbb{Z}, *)$ is not a group

↳ only inverse of 1 & -1 exists

(2) Because of the random permutation of the colours, Vivales learns nothing about the colouring.

Zero knowledge proof of having found a discrete logarithm:

Let G = finite group containing N elements.
b = fixed element of G
y = element of G for which Picara has found a discrete logarithm to the base b. (she has solved the equation $b^x = y$ for positive integer x)

Let us suppose Vivales knows the order N of the group.
Now Picara wants to demonstrate to Vivales that she knows x without giving the clue what x is:

(1) Picara generates a random positive integer $e < N$ and sends Vivales $b' = b^e$

(2) Vivales flip a coin. If heads comes up, Picara must reveal e and Vivales checks in fact that $b' = b^e$

(3) If the coin comes up on tail, then Picara must reveal the least positive residue of $(x+e \bmod N)$, at which point Vivales check the fact that $yb' = b^{x+e}$

(4) Steps #1 to #3 are repeated until Vivales in convinced that Picara knows the value x of the discrete logarithm.

Conclusion

if Picara does not know the value of x, then she will not be able to respond to more than one possible result of the coin toss.

If she has performed step (1), as she was supposed to then she can respond to heads but not to tails. without knowing x.
On the other hand, if she anticipates tail and so in step (1) decides to send Vivales $b' = b^e/y$ (so that in step 3, she can simply send e instead of $x+e$), Now if head comes up, she does not know power of b that gives b'

Oblivious transfer

An oblivious transfer channel from Picara to Vivoles is a system for Picara to send Vivoles two encrypted packets of information subject to following conditions:

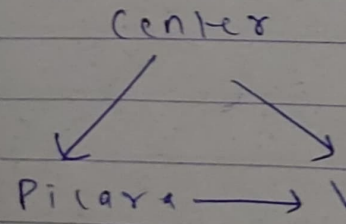
(1) Vivoles can decipher and read exactly one of the 2 packets.

(2) Picara does not know which of the 2 packets he can read

(3) both Picara & Vivoles are certain that conditions 1 & 2 hold.

---

* Example of Oblivious transfer:



Let us describe the procedure that Picara uses to convince Vivales that she can factor an integer $n = pq$ without giving information of what the factors might be:

(1) The center generates integer x and sends Picara and Vivales the least non-negative residue of $x^2 \bmod n$, let $y = x^2 \bmod n$

(2) Picara finds the four square roots of $y \bmod n$, $\pm x$ & $\pm x'$ she arbitrary chooses any of the square root x_0

3) Picara randomly picks integer r and sends Vivales the integer $s = r^2 \bmod n$ She sets $m_1 = r \bmod n$ and $m_2 = x_0 r \bmod n$ and sends these messages to Vivales by oblivious transfer.

Vivales is exactly able to read one of the 2 messages, He checks that its square modulo n is s (if his random $i = 1$) or ys (if $i = 2$)

Steps #1 to #4 are repeated. until Vivales is satisfied