POIS . Evaluation 1 - Q.

20171025
V. N. Lalitha Kameswari

Zero Knowledge Proof for DLP

Suppose Prover knows that $g^l = h$, for some public non identity elements g and h in some large public group of known size G (e.g. an elliptic curve group of prime order. $G = p$)

He has to convince Verifier that he knows l, without revealing value of l. He does as follows:

Schnorr's Protocol

1. Prover chooses v randomly mod G.
2. Prover computes $t = g^v$ and announces value to Verifier.
3. Verifier computes challengetext c, where $c = H(g, h, t)$, where H is a secure hash function and announces c to Prover.
4. Prover computes and announces $r = v - cl \bmod G$.
5. Verifier can now compute $t' = g^r h^c$ and verify whether $t = t'$

$\because t' = g^r h^c$

$= g^{(v - cl \bmod G)} h^c$

$= \dfrac{g^v}{g^{cl \bmod G}} \cdot h^c = \dfrac{g^v \cdot h^{c \bmod G}}{(g^l)^{c \bmod G}}$

$= \dfrac{g^v \cdot \cancel{h^{c \bmod G}}}{\cancel{h^{c \bmod G}}}$ $(\because g^l = h)$

$= t$

i.e if $t = t'$, then it means prover knows value of l.

This proof is a perfect zero knowledge proof because

① It obeys COMPLETENESS.
Given an honest prover and honest verifier, the protocol succeeds with close to 1 probability

② It obeys SOUNDNESS
i.e probability of a dishonest prover to complete the proof is negligible.
i.e in this case, probability of $t = t'$ without knowing l is negligible.

③ It also obeys ZERO KNOWLEDGE PROPERTY

Scanned with CamScanner

Designing a digital signature scheme based on the zero knowledge proof

Let's say this digital signature is for communication between A and B.

Step 1: We ~~ch~~ choose parameters

→ A and B agree on a group G of prime order q. Let g be the generator.
Here, we are making the assumption that discrete log problem is hard. i.e given $g^x \bmod q$, g and q, we can't find x in polynomial time.

→ A and B agree on a secure hash function $H : \{0,1\}^* \longrightarrow Z_q$

→ Let $M \in \{0,1\}^*$ be the set of all finite length messages.

→ Let $s, e, e_v \in Z_q$, the set of congruence classes modulo q.

→ Let $x, k \in Z_q$ (and are NON ZERO).

→ Let $y, r, r_v \in G$.

Step 2: Key Generation

→ Choose $x \in Z_q$, this is the private signing key.

→ The public verification key is $y = g^x$.

Step 3: Signing a message $m \in M$:

→ Choose a random $k \in Z_q$.

→ Let $r = g^k$.

→ Let $e = H(r \| m)$ (concatenation)

→ Let $s = k - xe$.

The signature pair is (s, e).

Step 4: Verifying

→ Let $r_v = g^s y^e$

→ Let $e_v = H(r_v \| m)$.

→ If $e_v = e$, then signature is verified.

Because, if $e_v = e$, then signed message is equal to verified message.

i.e. $r_v = g^s y^e = g^{k-xe} \cdot g^{xe} = g^k = r$

$\therefore e_v = H(r_v \| m) = H(r \| m) = e$.

Designing Collision Resistant Hash functions based on Hardness of DLP

Here, we propose a hash function h as

$$\boxed{h_i(x \| b) = g^x \cdot y^b}$$

$(y = g^x \bmod p)$

(h is the family of hash functions indexed by i)

This performs a one bit compression

(If we design for one bit, we can design for any number of bits using Merkle Damgard Transform discussed in class)

For this one bit hash function, if we can find an adversary A that can find collision for random i, then we can use A to compute Discrete logarithm efficiently. So, the proof is based on hardness of DLP

Proof If collision occurs,

We know that

$x \| b \neq x' \| b'$ and $h_i(x \| b) = h_i(x' \| b')$

If $b = b'$, since the hash will be a permutation, the discrete logarithm should also be unique.

→ If $b = b'$, then $x = x'$.

→ So, for input to be distinct, $b \neq b'$.

W.L.O.G, Assume
$b = 0$ and $b' = 1$

$$g^{x} \cdot y^{b} = g^{x'} \cdot y^{b'}$$

$$\Rightarrow g^{x} \bmod p = g^{x'} \cdot y \bmod p$$

$$\rightarrow y = g^{x - x'} \bmod p.$$

Since we know x, x', we can get $x - x'$.

This is against the hardness of DLP.

$\therefore$ h_i is collision resistant.

Scanned with CamScanner