Poisson

Evaluation - 1

Date :
Page No. :

Rishabh Singhal
2017213

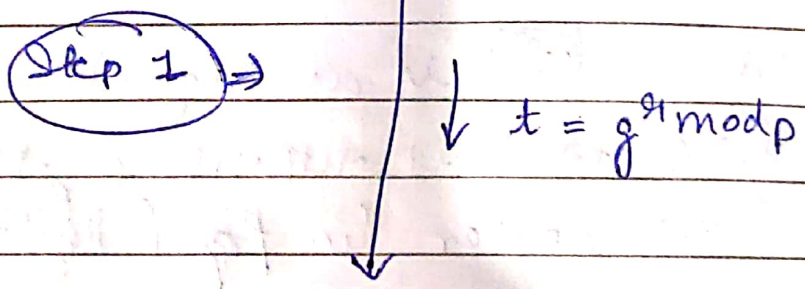
[Q] Zero-knowledge Proof for DLP ↓

(prover)

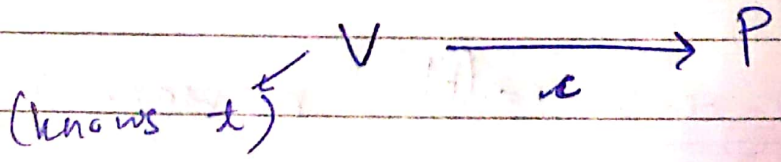
let P be verifier and wants to prove that he knows x such that $g^x = y \pmod p$

where g, y, p are public,

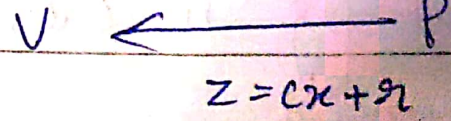
then P can generate random "r" $\in Z_p^*$



Step 2



Step 3



Date :
Page No. :

now, verifier checks if $g^z \overset{?}{=} y^c t$

and accepts if equal.

as $g^z = g^{cx+r} = (g^x)^c \times g^r = y^c g^r = y^c t$

but let's suppose, P does not knows the value of x,

then $cx' + r' = cx + r$

Chances of this to be correct is just $\frac{1}{p-1}$.

So, Verifier can repeat the process again & again & if at once P fails to provide (z), then it proves he doesn't know, otherwise he's able to proved that he knows (x) without telling him know the value of (x).

Digital Signature

Date :
Page No. :

☆ in this, for signing message,

we calculate $z = (x * \text{hash(message)} + r)$

where r is randomly generated,

and $\boxed{t = g^r}$ $g \rightarrow$ generator

and $(y = g^x)$ public key

For verifying,

if $g^z \overset{?}{=} y^{\text{hash}(m)} * t$

then (true) ☆

Proof,

as $g^z = g^{x*\text{hash}+r} = (g^x)^{\text{hash}(m)} \times g^r = \boxed{y^{\text{hash}(m)} \times t}$

here due to DLP it is difficult to obtain (x, r) from y & t

$\downarrow$ $\downarrow$

g^x g^t mod p

Date :
Page No. :

Collision-Resistant Hash function

⇒ Here this consists of 2 functions one for gen (Gen) & other hashing (H)

⇒ (Gen: (key generation algorithm):
on input 1^n, run $G(1^n)$ to obtain (G, p, g) & select $h \leftarrow G$
output $S = \langle G, p, g, h \rangle$

Here, G is an algorithm (polynomial time) that outputs a cyclic group G, whose order is p ($\|p\| = n$) & a generator g.
And then h is randomly selected from G (group).

⇒ Hash algorithm ⇒ (H) message ⇒ $(x_1, x_2) \in \mathbb{Z}_q \times \mathbb{Z}_q$

output $g^{x_1} h^{x_2} \in G$ ⇐ hash

hashing function
this algorithm is collision resistant as DLP is hard relative to G.