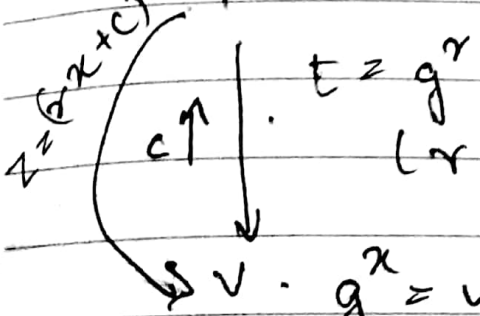
Evaluation I

ZKP for DLP



1. P chooses r, sends $t = g^r \bmod p$.
2. V sends C (random from $\mathbb{Z}_p^*$)
3. P sends $z = (cx + r)$.
4. V checks if $g^z = y^c \cdot t$

Accept/repeat if true, reject if false.

Completeness: $g^z = g^{cx+r} = g^{cx} \cdot r$

$= y^c \cdot t$.

If P knows x, V will always accept

Soundness: If P doesnot know x, pick.

x', r' such that.

~~Pr~~. $Pr(cx' + r' = (cx + r) \approx 1/p$.

zero-knowledge – Given y, V cannot calculate x. V can know x

if he can guess r and then $x = (z - r)/c$. To guess r, $t = g^r \bmod p$ but since DLP is hard to solve, getting r from t is hard.

Signature Scheme based on ZKP.

i) P chooses $r \in Z_p^*$ from random and sends $t = g^r \bmod p$.

ii) V sends a challenge $c \in Z_p^*$ from random

iii)

Signature Scheme based on ZKP

The users choose a Hash Function $H : \{0,1\}^* \rightarrow Z_p^*$

Key-Generation:

private key : $x \in Z_p^*$

public key : $y = g^x \bmod p$.

Sign: $r \in_R \mathbb{Z}_p^*$

$t = g^r \bmod p.$

$c = H(t \| M)$, M is the message

$z = cx + r.$

Send M, z and t

Verify:

$c = H(t \| M)$, M is the message

check if $y^c t = g^z$.

Hash functions using DLP.

1. $H: \mathbb{Z}_p^* \times \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*$

$H(x_1, x_2) = g^{x_1} h^{x_2} \bmod p$

where. $h \in \mathbb{Z}_p^*$

To extend this hash function to any given n bit string, we can use Merkle - Damgard Transform which has been proved to be collision resistant.