# Evaluation I

Q i) Design a zero - knowledge proof for DLP
ii) Using hash functions, show how to build a digital signature scheme
iii) How would you design collision resistant hash functions based on the hardness of DLP.

i) ZKP for DLP

The prover and verifier agree upon a group $\mathbb{Z}_p^*$ and a generator $g$. The prover proves knowledge of $x$ with the following interaction. Here $y = g^x \bmod p$.

i) Prover chooses $r \in_R \mathbb{Z}_p^*$. and sends $t = g^r \bmod p$
ii) Verifier sends the prover a challenge $c \in_R \mathbb{Z}_p^*$
iii) Prover sends $z = (cx + r)$
iv) Verifier checks if $g^z = y^c \cdot t$, accept / repeat if true. Else reject.

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

$= y^c \cdot t$

i.e. If the prover knows $x$, the verifier will always accept. (or repeat).

Soundness: If the prover does not know $x$, it has to guess a $z$ s.t. $g^z = y^c \cdot t$

However if it can guess such a $z$ with better than negl() probability, since it knows $c$ and $r$ it can find $x$. (and thus solve DLP with better than negl() probability).

zero-knowledge — Assuming the hardness of DLP, the verifier cannot recover $x$ from $y$. To recover $x$ from $z = cx + r$ the verifier needs to know $r$. However it only has $g^r = t$ available. Again due to the hardness of DLP it cannot recover $r$ with non-negl probability.

2) A signature scheme based on the above ZKP.

The users agree on a group $\mathbb{Z}_p^*$, generator $g$, and a Hash function $H: \{0,1\}^* \longrightarrow \mathbb{Z}_p^*$

Gen:

private key $x \in_R \mathbb{Z}_p^*$

public key $y = g^x$.

sign

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

$t = g^r$

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

$z = cx + r$

The message is sent along with the signature $(z, t)$

Verify

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

check if $y^c \cdot t = g^z$

3) ## Collision Resistant Hash Functions using DLP

Gen: For a group $G$ of order $p$ and a generator $g$. Let $h \in_R G$. $s = \langle G, p, g, h \rangle$

$$H : \mathbb{Z}_p \times \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$$
$$H^s(x_1, x_2) = g^{x_1} \cdot h^{x_2}$$

Now to find $H'^s : \{0,1\}^* \longrightarrow \mathbb{Z}_p$ we can use the Merkle-Damgard Transform.

consider $l = \log_2(p) + 1$.

i) set $B = \left\lceil \frac{L}{l-1} \right\rceil$. Pad $x$, the input string, with 0 till its length is a multiple of $l-1$.

ii) set $z_0 = p-1$.

iii) For $i = 1 \ldots B$ compute $z_i = H(z_{i-1}, x_i)$ where $x_i$ is the ith block.

iv) Output $z_B$.

Collision Resistance of $H$:

consider colliding inputs $x_1, x_2$ and $x_1', x_2'$

A collision with non negligible probability implies-

$$g^{x_1} \cdot h^{x_2} = g^{x_1'} \cdot h^{x_2'} \mod p$$

$$\Rightarrow g^{(x_1 - x_1')} = h^{(x_2' - x_2)} \mod p$$

Since $g$ is a generator $h = g^t$

$$\Rightarrow (x_1 - x_1') = t(x_2' - x_2) \mod p-1$$

Now this is a linear congruence which can be solved

in order to find $t$. However by finding $t$, we get the solution to the discrete log problem $h = g^t$.
$\therefore$ an adversary could find a collision with non-negligible probability and use it to solve DLP with non-negligible probability.
Assuming the hardness of DLP, finding a collision in $H$ must be as hard.

Collision Resistance of $H'$

This comes from the Merkle Damgard construction. For two inputs $x_1$ and $x_2$ to collide, they output the same value $z_B$. $\Rightarrow$ $\exists$ some index $i$ s.t. $z_{i-1}, x_i \neq z_{i-1}', x_i'$ and $z_i = z_i'$. Let $i^*$ be the rightmost such index. Then $z_{i-1}, x_i$ and $z_{i-1}', x_i'$ are distinct colliding inputs for $H$. But as we saw above the probability of collision in $H$ must be negligible.
$\Rightarrow$ Finding a collision in $H'$ is as hard as finding a collision in $H$. By the hardness of DLP, this probability must also be negligible.